Cloudflare WAF

Zapora WAF dla bezpieczeństwa nowoczesnych aplikacji

Wyzwania związane z bezpieczeństwem aplikacji

Aplikacje stanowią ważniejszy niż kiedykolwiek element działalności biznesowej, dlatego są nieustannie celem ataków — to z kolei prowadzi do powstania rozszerzonej powierzchni narażenia na atak.

Kwestie wymagające uwagi obejmują szeroki zakres obszarów: od ochrony przed pojawiającymi się lukami typu zero–day, wykrywania prób omijania zabezpieczeń i zmniejszania ryzyka ataków typu „credential stuffing" prowadzących do przejęcia konta aż po wykrywanie utraty danych, a nawet skanowanie w poszukiwaniu złośliwego oprogramowania przesyłanego do aplikacji.

Zagadnienia te wiążą się z koniecznością zagwarantowania, że ochrona aplikacji jest częścią szerszego, ujednoliconego systemu bezpieczeństwa, który zapewnia również ochronę interfejsów API, powstrzymuje boty i ogranicza zagrożenia po stronie klienta. Każde z tych działań musi być realizowane bez obciążania zespołów nadmiernymi problemami związanymi z zarządzaniem.

Cloudflare WAF

Zapora aplikacji internetowych (WAF) firmy Cloudflare jest podstawą naszego portfolio zaawansowanych zabezpieczeń aplikacji, które zapewniają im bezpieczeństwo i wydajność. Zapora Cloudflare WAF to jedyne rozwiązanie umożliwiające ochronę aplikacji bez względu na miejsce ich hostowania poprzez, między innymi, pełną widoczność zabezpieczeń, wielowarstwową ochronę przed atakami OWASP i nowymi zagrożeniami, wykrywanie prób omijania zabezpieczeń i nowych ataków z wykorzystaniem uczenia maszynowego, blokowanie przejęcia kont oraz wykrywanie utraty danych. Nasze zaawansowane funkcje bezpieczeństwa aplikacji, takie jak zabezpieczenie interfejsów API i powstrzymywanie ataków botów, są w pełni zintegrowane z WAF i korzystają z tego samego wydajnego silnika reguł, który jest dostarczany z jednego z wiodących na świecie rozwiązań connectivity cloud.

Widoczność ataków i proste wdrażanie

Oferujemy zróżnicowane analizy bezpieczeństwa w celu wizualizacji całego ruchu, zarówno ograniczanego, jak i nieograniczanego. Natychmiastowy wgląd w krajobraz zagrożeń zapewnia wymierny zwrot z inwestycji, umożliwiając zespołom zrozumienie działania ruchu związanego z atakami oraz zabezpieczeń, które powinny utworzyć zaraz po wdrożeniu.

Szybka ochrona przed pojawiającymi się atakami

Przy dziesiątkach tysięcy luk wykrywanych każdego roku nasza zapora WAF szybko dodaje nowe reguły zarządzane w celu blokowania nowo wykrytych luk w zabezpieczeniach (zero–day). Nasze reguły zarządzane blokują luki, bazując na ocenach WAF Attack Score ustalanych z użyciem uczenia maszynowego, w celu wykrywania prób obchodzenia zabezpieczeń.

Analiza zagrożeń napędzana ogromną siecią globalną

Skuteczność zabezpieczeń zaczyna się od najlepszych danych. Nasza rozległa sieć globalna pełni rolę proxy dla 20% Internetu, zapewniając nam niezrównany wgląd w krajobraz zagrożeń. Te dane stanowią bazę dla modeli uczenia maszynowego, które łączymy z tradycyjnymi detekcjami opartymi na sygnaturach, aby z dużą dokładnością wykrywać ataki i ograniczać ich skutki.

Wyzwania związane z bezpieczeństwem aplikacji

Cloudflare zapewnia skuteczniejszą ochronę.

Dostarczamy bardziej efektywną ochronę z użyciem zapory WAF dzięki zabezpieczeniom warstwowym:

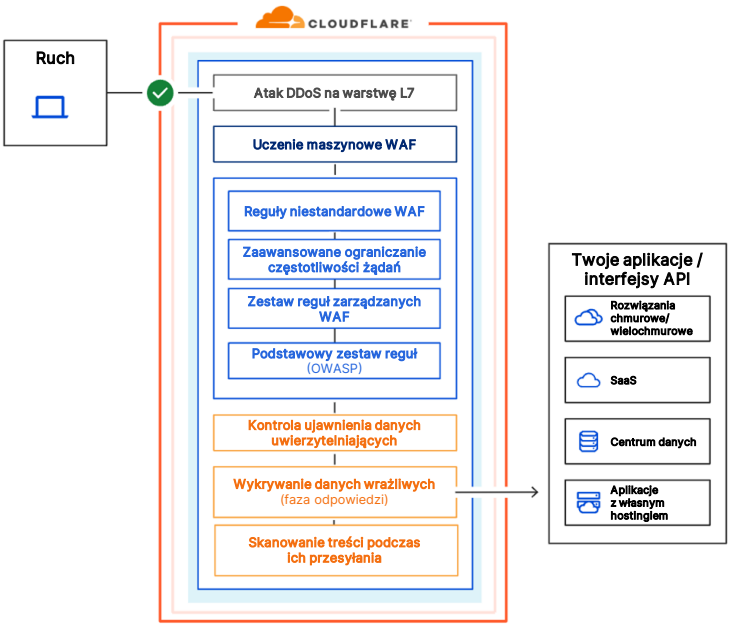
- Analiza danych dotyczących bezpieczeństwa
- Wiele zestawów reguł zarządzanych
- Reguły niestandardowe
- Wykrywanie oparte na uczeniu maszynowym
- Wykrywanie danych poufnych
- Sprawdzanie pod kątem skradzionych danych uwierzytelniających
- Zaawansowane ograniczanie częstotliwości żądań
- Skanowanie operacji przesyłania w poszukiwaniu złośliwego oprogramowania

Cloudflare reaguje szybciej.

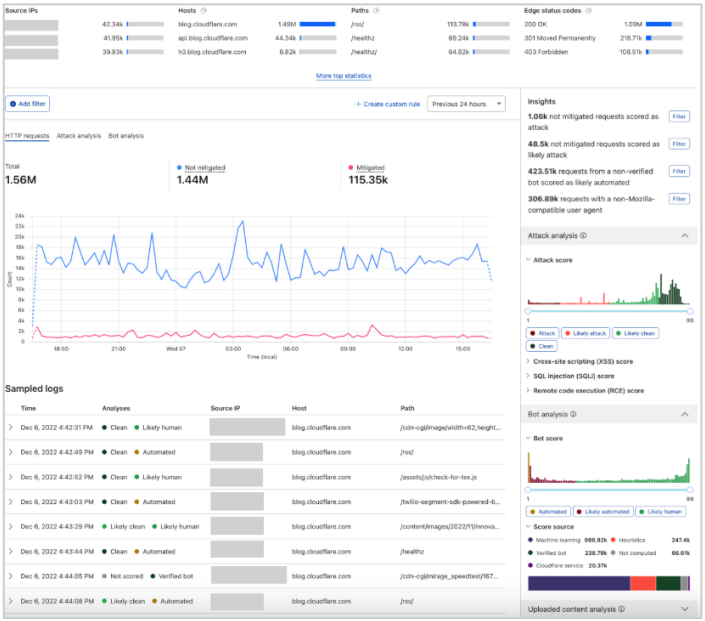
Zapewniamy szybszą ochronę przed lukami w zabezpieczeniach. W przypadku głównych luk w zabezpieczeniach, takich jak HTTP/2 Rapid Reset, Log4j i innych, wiele reguł zarządzanych wprowadziliśmy o jeden dzień szybciej niż inni dostawcy WAF.

Cloudflare w pełni integruje bezpieczeństwo aplikacji.

Nasza zapora WAF jest w pełni zintegrowana z resztą naszego portfolio zabezpieczeń aplikacji, w tym API Gateway i zarządzaniem ruchem botów, a wszystko to dostarczamy w ramach pojedynczego przejścia z rozwiązania Cloudflare connectivity cloud.



Analiza danych dotyczących bezpieczeństwa WAF



Zapora WAF na potrzeby bezpieczeństwa przedsiębiorstwa

Zintegrowana z SIEM, gotowa na SOC

Dzięki interfejsom API firmy Cloudflare i integracjom z dziennikiem nieprzetworzonym można w prosty sposób przeprowadzić integrację z SIEM lub zasilić Centrum bezpieczeństwa (SOC) informacjami dostarczanym przez Cloudflare.

Łatwiejsze DevSecOps

Nasza gotowa integracja z Terraform sprawia, że włączenie bezpieczeństwa aplikacji do procesu DevOps jest bezproblemowe.

Wsparcie Cloudforce One

Rozwiązania Cloudflare z zakresu bezpieczeństwa aplikacji korzystają z analizy zagrożeń uzyskiwanej od Cloudforce One, naszego zespołu ds. zagrożeń, w celu ich blokowania z użyciem nowych operacji wykrywania opartych na pojawiających się informacjach oraz taktykach, technikach i procedurach (TTP).

 | +44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/pl-pl/ REV:PMM-JAN-2025

Bezpieczeństwo aplikacji internetowych	
Warstwowa ochrona z użyciem wielu zestawów reguł WAF	Zatrzymuje złośliwe payloady w dowolnym komponencie żądania za pomocą wielu zestawów reguł: 1. Reguły zarządzane przez Cloudflare 2. Podstawowy zestaw reguł OWASP 3. Niestandardowe reguły powstrzymywania ataków Nowe reguły zarządzane są testowane na ogromnym wolumenie ruchu w celu zapewnienia jak najmniejszej liczby wyników fałszywie dodatnich.
Zaktualizowane zasady zabezpieczeń zero–day	Zasady stale aktualizowane przez zespoły Cloudflare ds. bezpieczeństwa w celu zapewnienia ochrony przed nowymi atakami i wykorzystaniem luk w zabezpieczeniach typu zero–day, zanim zostaną udostępnione poprawki.
Wykrywanie oparte na uczeniu maszynowym	Skuteczniejsze powstrzymywanie prób obejścia zabezpieczeń dzięki modelom uczenia maszynowego uzupełniającym warstwowe zestawy reguł. Dla reguł są dostępne cztery różne oceny ataków: ogólna ocena WAF Attack Score, ocena ataków XSS, ocena ataków SQLi oraz ocena ataków RCE.
Zestawy reguł specyficzne dla platformy dla głównych platform CMS i e–commerce	Gotowa ochrona bez dodatkowych opłat dla platform takich jak WordPress, Joomla, Plone, Drupal, Magneto, IIS itp.
Niestandardowa konfiguracja reguł	Tworzenie pozytywnego lub negatywnego modelu bezpieczeństwa poprzez wykonywanie działań BLOCK, MANAGED CHALLENGE, JS CHALLENGE, SKIP, LOG, LEGACY CAPTCHA i CUSTOM RESPONSES podczas wdrażania reguł lub zestawów reguł.
Zaawansowane ograniczanie częstotliwości żądań	Zapobieganie nadużyciom oraz atakom DDoS i brute force ukierunkowanym na aplikacje i interfejsy API poprzez ograniczanie częstotliwości żądań dla określonych adresów IP lub na podstawie atrybutu nagłówka (np. klucz, cookie, token), numeru ASN lub kraju.
Wykrywanie danych poufnych	Wykrywanie odpowiedzi zawierających dane poufne, takie jak informacje umożliwiające identyfikację osoby, dane finansowe, numery kart kredytowych lub dane tajne, takie jak klucze interfejsu API.
Kontrola ujawnienia danych uwierzytelniających	Wykrywanie ataków credential stuffing z użyciem skradzionych danych uwierzytelniających przed przejęciem kont użytkowników końcowych.
Skanowanie przesyłanych treści	Skanowanie treści WAF umożliwia analizowanie przesyłanych plików w poszukiwaniu złośliwego oprogramowania. Uzyskane sygnały można połączyć z innymi parametrami żądania, tworząc reguły niestandardowe.
SSL/TLS	Pełne przeniesienie i konfiguracja ruchu SSL dla aplikacji.
Mniej wyników fałszywie dodatnich	Nowe reguły są testowane na ogromnym wolumenie ruchu w celu zapewnienia jak najmniejszej liczby wyników fałszywie dodatnich.
Obsługa gRPC i Websocket	Serwer proxy i bezpieczny ruch dla punktów końcowych gRPC i Websocket.
Konfigurowalne strony blokowania	Dostosowanie stron blokowania z użyciem szczegółowych informacji dla odwiedzających.
Pełna integracja z szerszym pakietem produktów Cloudflare	Większa wydajność aplikacji, ruch kierowany geograficznie oraz przetwarzanie brzegowe.

Widoczność, raportowanie i programowalność	
Analiza danych dotyczących bezpieczeństwa	Wizualizacja wszystkich potencjalnych ataków ocenianych na podstawie uczenia maszynowego.
Rejestrowanie w czasie rzeczywistym i dostęp do plików dziennika nieprzetworzonego	Widoczność ułatwiająca dostrojenie zapory WAF i możliwość przeprowadzenia dogłębnej analizy obejmującej wszystkie żądania WAF.
Rejestrowanie payloadu	Rejestrowanie i szyfrowanie złośliwych payloadów w celu analizy incydentów.
Integracje SIEM	Przesyłanie lub pobieranie dzienników bezpośrednio do istniejącego SIEM.
Integracja z usługą Terraform	Włączenie bezpieczeństwa aplikacji do przepływów pracy CI/CD.
Zarządzanie	
Zarządzanie z jednej konsoli	Usprawnione zarządzanie w ramach jednej konsoli na potrzeby globalnego wdrażania bezpieczeństwa i wydajności aplikacji oraz zarządzania tymi obszarami.
Zarządzanie na poziomie konta	Oszczędność czasu związanego z zarządzaniem zaporą WAF dzięki możliwości konfiguracji WAF na poziomie pojedynczego konta dla wszystkich domen.
Wysoka dostępność dzięki umowom SLA	Gwarancja 100-procentowej dostępności z uwzględnieniem kar finansowych w razie naruszenia umów SLA.
Brak wymogów odnośnie sprzętu, oprogramowania i dostosowywania	Wdrażanie poprzez prostą zmianę DNS.
Certyfikat PCI	Cloudflare posiada certyfikat dostawcy usług poziomu 1.
Autoryzacja FedRAMP	Nasz pakiet Cloudflare dla instytucji rządowych, w tym rozwiązania z zakresu bezpieczeństwa aplikacji, ma autoryzację FedRAMP.

Chcesz zobaczyć więcej? Zarejestruj się na naszą serię prezentacji na żywo dotyczących bezpieczeństwa aplikacji.

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