Cloudflare Page Shield

Zabezpiecz łańcuch dostaw Twojej aplikacji internetowej i chroń użytkowników końcowych przed atakami po stronie klienta.

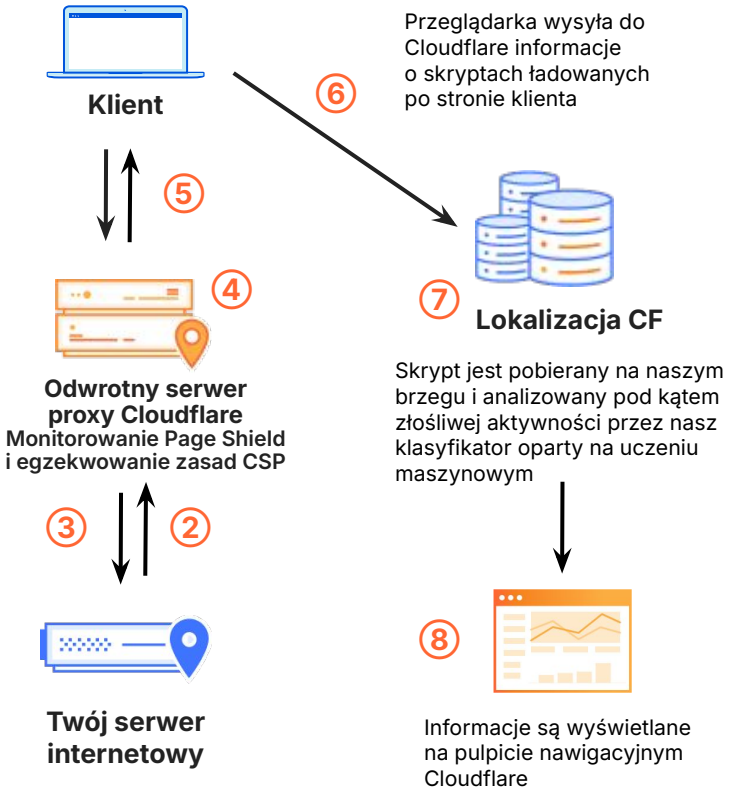
Wzmagające się ataki po stronie klienta

Niewidoczne punkty tworzone przez zależności zewnętrzne

Aby zapewnić lepsze doświadczenia internetowe, firmy rozbudowują funkcjonalności witryn o takie funkcje jak chatboty lub analizy uzyskiwane od innych firm zewnętrznych lub programistów. Atakujący starają się naruszać te zależności zewnętrzne, aby wykradać dane prywatne wprowadzane przez użytkowników końcowych podczas odwiedzania witryny, rozprzestrzeniać złośliwe oprogramowanie, kopać kryptowaluty lub przeprowadzać kolejne ataki.

Identyfikuj i ograniczaj skutki ataków w łańcuchu dostaw

Page Shield chroni użytkowników końcowych witryn internetowych przed atakami po stronie klienta wykorzystującymi luki w zabezpieczeniach związane z zależnościami JavaScript. Page Shield otrzymuje bezpośrednio od przeglądarki informacje o tym, jakie pliki i moduły JavaScript są ładowane, przeprowadza analizy w celu wykrycia złośliwych skryptów, zapewnia wgląd we wszystkie aktywne skrypty i połączenia wychodzące, a także ostrzega o złośliwych działaniach pliku JavaScript.



Rysunek 1: Architektura Cloudflare Page Shield

Inteligentne zapobieganie atakom

Uzyskaj pełny wgląd w łańcuch dostaw aplikacji internetowych i ograniczaj skutki ataków w łańcuchu dostaw poprzez ciągłe monitorowanie aktywnych skryptów, zmian w skryptach oraz nawiązywanych połączeń.

Automatyczne alerty dotyczące zagrożeń

Dostawaj natychmiastowe powiadomienia, gdy nowe skrypty zostaną wykryte, oznaczone jako złośliwe lub załadowane z nieznanych domen.

Spełniaj wymogi dotyczące zgodności z przepisami

Ogranicz ryzyko związane z dostawcami zewnętrznymi i spełniaj wymogi przepisów obowiązujących po stronie klienta, takich jak RODO, PCI DSS 4.0 i innych. Page Shield pomoże spełnić te wymagania bez dodatkowego wysiłku.

Funkcje umożliwiające przejęcie kontroli nad łańcuchem dostaw aplikacji internetowych oraz zabezpieczenie środowisk przeglądarek użytkowników końcowych

Page Shield	
Monitor skryptów	Wyświetla informacje o skryptach podmiotów zewnętrznych załadowanych na stronach w Twojej domenie.
Connection Monitor	Wyświetla informacje o połączeniach nawiązywanych przez skrypty na stronach w Twojej domenie.
Monitor plików cookie	Wyświetla informacje o plikach cookie wykrytych w ruchu HTTP.
Przypisanie stron	Umożliwia sprawdzenie, na której stronie skrypt pojawił się po raz pierwszy, jak również wyświetlenie listy najnowszych wystąpień tego skryptu na Twoich stronach.
Alerty o nowych zasobach i alerty dotyczące nowej domeny	Skonfiguruj i dostosuj powiadomienia o nowo wykrytych skryptach lub skryptach ładowanych z nieznanych domen.
Wykrywanie złośliwych skryptów i ostrzeganie o nich	Wykrywa złośliwe skrypty na Twoich stronach przy użyciu analizy zagrożeń i uczenia maszynowego.
Wykrywanie zmian kodu i ostrzeganie o nich	Wykrywanie wszelkich zmian w skryptach i połączeniach ładowanych na Twoje strony. Alerty można skonfigurować w taki sposób, aby były wysyłane z większą lub mniejszą częstotliwością.
Wykrywanie złośliwych połączeń i ostrzeganie o nich	Sprawdza, czy skrypt nawiązuje połączenie ze złośliwą domeną, taką jak domena typu „command-and-control” lub magazyn w chmurze, co wskazuje na eksfiltrację danych.
Zasady	Zasady definiują zasoby dozwolone w Twoich aplikacjach na mocy dyrektyw dotyczących zasad bezpieczeństwa treści (CSP). Zasady mogą rejestrować naruszenia oraz egzekwować pozytywny model bezpieczeństwa definiujący listę dozwolonych zasobów i blokujący zasoby nieujęte w zasadach.

Chcesz zobaczyć, jak działa Page Shield? Zarejestruj się na naszą bezpłatną ocenę ryzyka po stronie klienta już dziś.