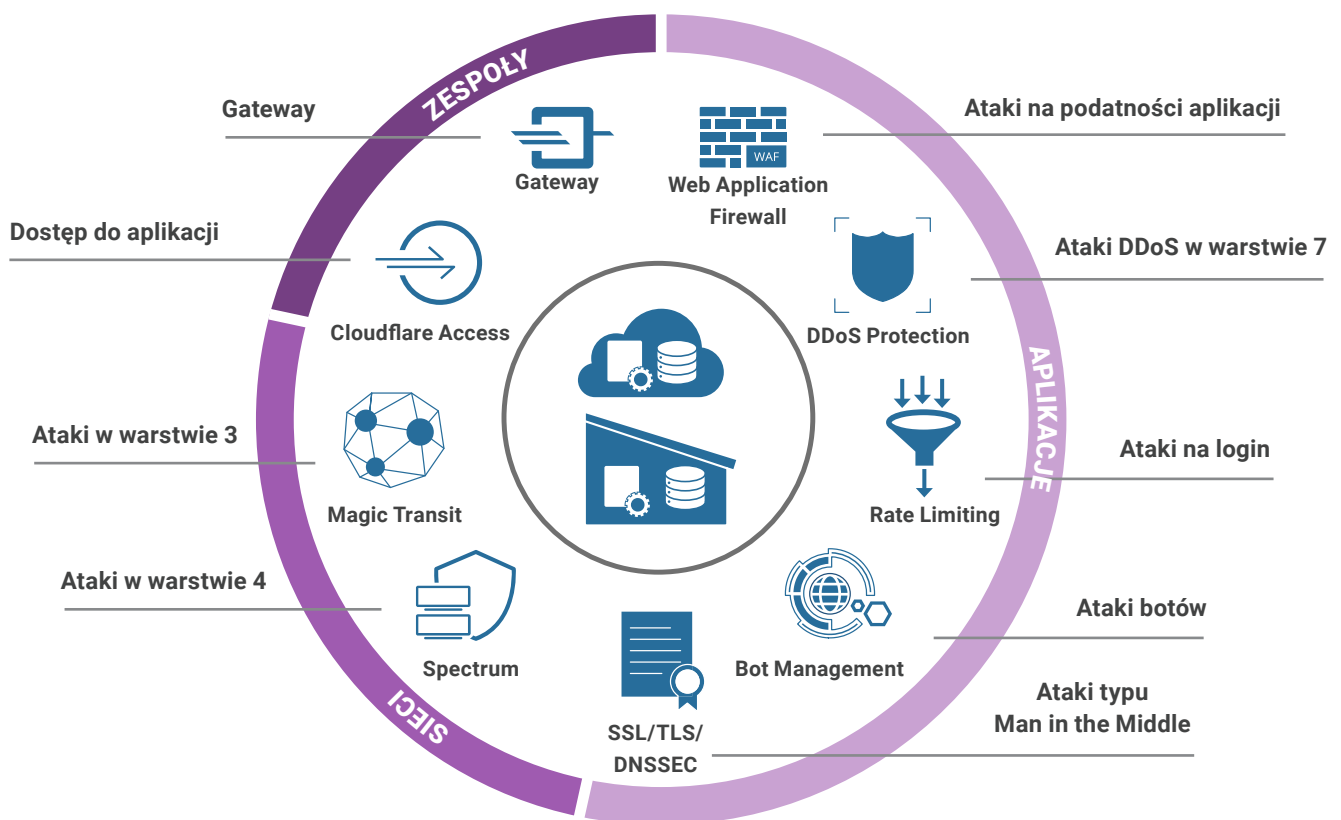


Usługi bezpieczeństwa Cloudflare

- Zabezpiecz aplikacje internetowe przed atakami, w tym blokadą usług czy złośliwymi botami, jak również krytycznymi podatnościami (OWASP Top 10) i atakami zero-day
- Zabezpiecz infrastrukturę sieciową w warstwie 3. i 4. przed atakami DDoS
- Zabezpiecz swoje urządzenia, sieci i wewnętrzne aplikacje



„Cloudflare WAF jest łatwy i intuicyjny w użyciu. Nasi inżynierowie potrzebowali jedynie chwili, aby się z nim zapoznać. Obecnie, rozszerzyliśmy wykorzystanie pakietu produktów Cloudflare. Integracja z każdym rozwiązaniem Cloudflare przebiegała sprawnie i bezproblemowo”.

PAUL SHOPE
Security Engineer, SoFi



„Cloudflare Access pomaga 23andMe uzyskać bezpieczny dostęp do wewnętrznych aplikacji z dowolnego urządzenia, w dowolnym czasie, bez konieczności korzystania z VPN”.

ARNOLD DE LEON
SRE Manager



„Korzystając z uczenia maszynowego na dziesiątkach milionów stron internetowych, Cloudflare jest w stanie natychmiast zidentyfikować nieautoryzowane boty, które korzystają z naszej witryny w nieupoważniony sposób. Blokuje boty, nie utrudniając przy tym korzystania ze strony realnym użytkownikom”.

TONY BRUESS
Product Engineer

Usługi bezpieczeństwa Cloudflare

Web Application Firewall (WAF)

WAF klasy korporacyjnej wykrywa i blokuje typowe podatności w warstwie aplikacji, egzekwując m.in. zestawy reguł OWASP TOP 10.

DDoS

Oparte na chmurze rozwiązanie DDoS Cloudflare zapewnia ciągłą ochronę przed zaawansowanymi atakami DDoS.

Rate Limiting

Rate Limiting pozwala chronić krytyczne zasoby, uzupełniając ogólną ochronę Cloudflare DDoS o precyzyjną kontrolę w celu blokowania lub oznaczania odwiedzających z podejrzanymi statystykami żądań.

Bot Management

Bot Management ogranicza zaawansowane ataki botów i blokuje podejrzanе żądania bez użycia Javascript lub narzędzi innych firm.

SSL/TLS

Szyfrowanie Transport Security Layer (TLS) umożliwia połączenie HTTPS między odwiedzającymi a serwerem źródłowym, zapobiegając atakom typu man-in-the-middle, sniffingowi pakietów itp., bez wyświetlania ostrzeżeń o zaufaniu w przeglądarce internetowej.

DNSSEC

Cloudflare DNSSEC chroni integralność witryny, a także zapewnia odwiedzającym połączenie z serwerami internetowymi bez wycieku informacji.

Magic Transit

Magic Transit to produkt Cloudflare do ochrony infrastruktury sieciowej przed atakami DDoS. Jest on dostępny w trybach ciągłego połączenia i połączenia na żądanie. Magic Transit posiada wbudowaną zaporę IP i oferuje korzyści związane z większą wydajnością

Spectrum

Spectrum to produkt typu reverse-proxy, który zapewnia ochronę przed atakami DDoS i przyspieszenie ruchu dla aplikacji TCP/UDP.

Access

Cloudflare Access zastępuje korporacyjnych klientów VPN, umieszczając globalną sieć graniczną Cloudflare przed wewnętrznymi aplikacjami.

Gateway

Gateway wykorzystuje globalną sieć Cloudflare w celu zapewnienia zespołom kompleksowego bezpieczeństwa w sieci, bez obniżania wydajności.

Zalety Cloudflare



Skala

Globalna sieć, która obejmuje ponad 200 miast i ponad 25 milionów obiektów internetowych, umożliwia Cloudflare korzystanie z unikalnych informacji o zagrożeniach, aby zapewniać ochronę przed zaawansowanymi atakami.



Łatwość użytkowania

Łatwość wdrożenia, adaptacji i zarządzania jest podstawowym założeniem projektowym każdego produktu Cloudflare. Tworzymy proste i intuicyjne projekty, których celem jest rozwiązywanie złożonych problemów związanych z bezpieczeństwem.



Zintegrowane bezpieczeństwo i wydajność

Cloudflare eliminuje konieczność poświęcania wydajności na rzecz bezpieczeństwa. Rozwiązania Cloudflare są zaprojektowane tak, aby integrować się i współpracować bezproblemowo z innymi produktami z zakresu bezpieczeństwa i wydajności.