Magic Transit

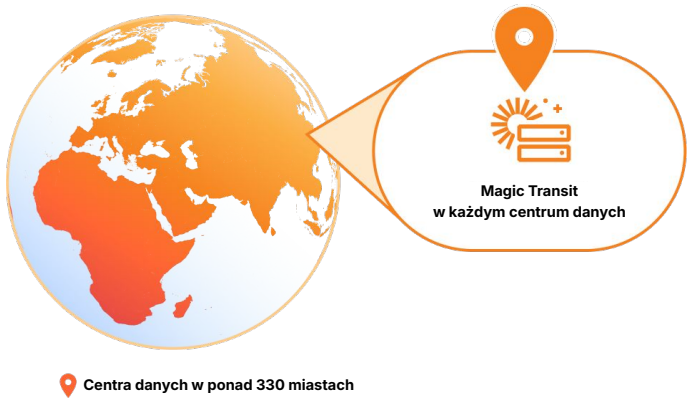
Cloudflare Magic Transit chroni Twoją infrastrukturę sieciową, centra danych oraz usługi chmury publicznej przed atakami DDoS

Ochrona przed atakami DDoS dla sieci lokalnych, hostowanych w chmurze i hybrydowych

Szybka, niezawodna ochrona przed atakami DDoS

Pytanie nie brzmi już „czy", ale „kiedy" Twoja organizacja stanie się celem ataku DDoS. Ochrona infrastruktury sieciowej przed atakami DDoS wymaga połączenia analizy zagrożeń, szybkości działania i przepustowości. Ataki wolumetryczne mogą z łatwością przytłoczyć starsze rozwiązania. Większość innych opartych na chmurze rozwiązań do ochrony przed atakiem DDoS przesyła ruch przez sieć dosyłową do centrów filtrowania ruchu (scrubbing center), co powoduje znaczne opóźnienia i odbywa się kosztem wydajności.

- Prawie natychmiastowa minimalizacja skutków ataku (TTM)
- Ochrona przed atakami DDoS z każdego pojedynczego centrum danych
- Łatwe wdrażanie w ciągu kilku minut
- Pojedynczy punkt zarządzania



Rysunek 1. Ochrona DDoS w każdym centrum danych Cloudflare

Wiodąca w branży ochrona przed atakami DDoS

Rozwiązanie Magic Transit zostało wyróżnione tytułem Customers' Choice w raporcie Gartner® Peer Insights™ „Voice of the Customer": DDoS Mitigation Solutions.

Korzyści

Nowoczesna architektura

Bezkonkurencyjna przepustowość sieci na poziomie **449 Tb/s** w **ponad 330 lokalizacjach**. Nie łączymy sieci dosyłowej z centrami filtrowania ruchu (scrubbing center), a wielu klientów zgłasza poprawę wydajności po przejściu na Cloudflare.

Kompleksowa ochrona

Cloudflare **blokuje średnio 234 mld cyberzagrożeń każdego dnia**. Wspólna analiza zagrożeń zapewnia lepszą ochronę przed złożonymi, nowatorskimi i wyrafinowanymi atakami. Magic Transit oferuje zautomatyzowaną ochronę, która blokuje skutki większości ataków w **mniej niż trzy sekundy**.

Łatwość użycia

Rozpocznij wdrażanie w ciągu kilku minut, korzystając z własnego adresu IP (BYOIP) lub adresu IP dzierżawionego od Cloudflare. Skonfiguruj raz na zawsze dzięki naszej „zawsze włączonej" ochronie. Wszystkie ustawienia można konfigurować z poziomu jednej konsoli lub interfejsu API na potrzeby analiz, alertów i logów.