

Platforma SASE i SSE

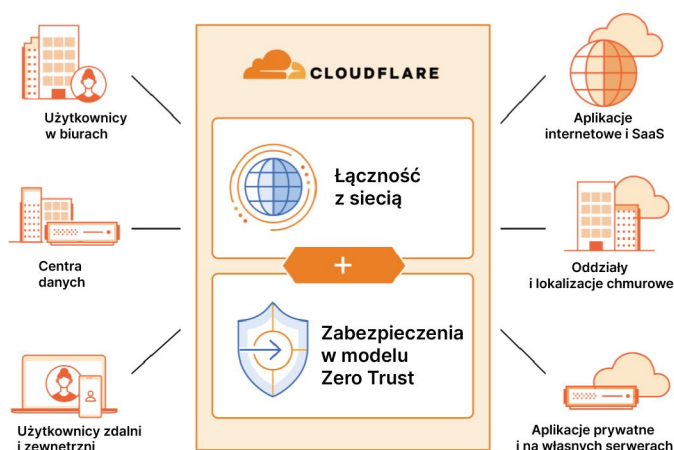
Rozszerz możliwości platformy connectivity cloud firmy Cloudflare — zmniejsz cyberzagrożenia i zmodernizuj swoją sieć dzięki komponowalnym sieciom w modelu Zero Trust

Połącz bezpieczeństwo i obsługę sieci już teraz

Aby zmniejszyć złożoność IT i odzyskać kontrolę, [88% liderów IT](#) już teraz konsoliduje i optymalizuje swój zestaw technologii. SASE, kluczowy trend architektoniczny, łączy bezpieczeństwo i sieć, aby zapewnić prosty, bezpieczny dostęp przy jednoczesnej poprawie elastyczności biznesowej.

Prosty i bezpieczny sposób zapewniania łączności wszystkich użytkowników ze wszystkimi zasobami bez stosowania VPN-u lub przekazywania ruchu MPLS

Chcesz przyspieszyć swoją drogę do modelu Zero Trust i poprawić przyspieszenie ruchu internetowego? Korzystaj z tej samej [platformy connectivity cloud](#), która łączy i chroni Twoje aplikacje internetowe, aby zapewnić łączność i ochronę aplikacji firmowych oraz funkcji przeglądania sieci. **Cloudflare One** to nasza platforma [Secure Access Service Edge \(SASE\)](#) od jednego dostawcy umożliwiająca komponowanie i wdrażanie rozwiązań łączących typu on-ramp i usług w dowolnej kolejności. Wiele z nich zaczyna od krawędzi usługi (SSE) modelu Zero Trust, aby ograniczyć powierzchnię narażenia na atak, powstrzymać phishing i oprogramowanie typu ransomware, zapobiegać ruchowi bocznemu oraz zabezpieczyć dane.



Najszybsza droga do architektury typu Zero Trust

Przestań domyślnie ufać użytkownikom, przydzielając im nadmierne uprawnienia dostępu, gdy tylko znajdą się w sieci firmowej. Zaczynij korzystać z serwera proxy, który wyraźnie weryfikuje tożsamość, stan urzędzenia i kontekst biznesowy, do uwierzytelniania i autoryzacji każdego żądania kierowanego do, pochodzącego od lub kierowanego pomiędzy jednostkami w sieci.



Poprawa wydajności operacyjnej

Prostsze zarządzanie zasadami, szybsze rozwiązywanie problemów i lepsze doświadczenia użytkowników pozwalają zredukować liczbę zgłoszeń IT związanych z łącznością sieciową o nawet **80%**.



Ograniczenie cyberzagrożeń

Wykorzystuj najszerszy zakres źródeł danych, obejmujący **20%** sieci, — dane z DNS, poczty e-mail, aplikacji i interfejsów API, — do analizy i blokowania zagrożeń w czasie rzeczywistym.



Szybszy rozwój firmy

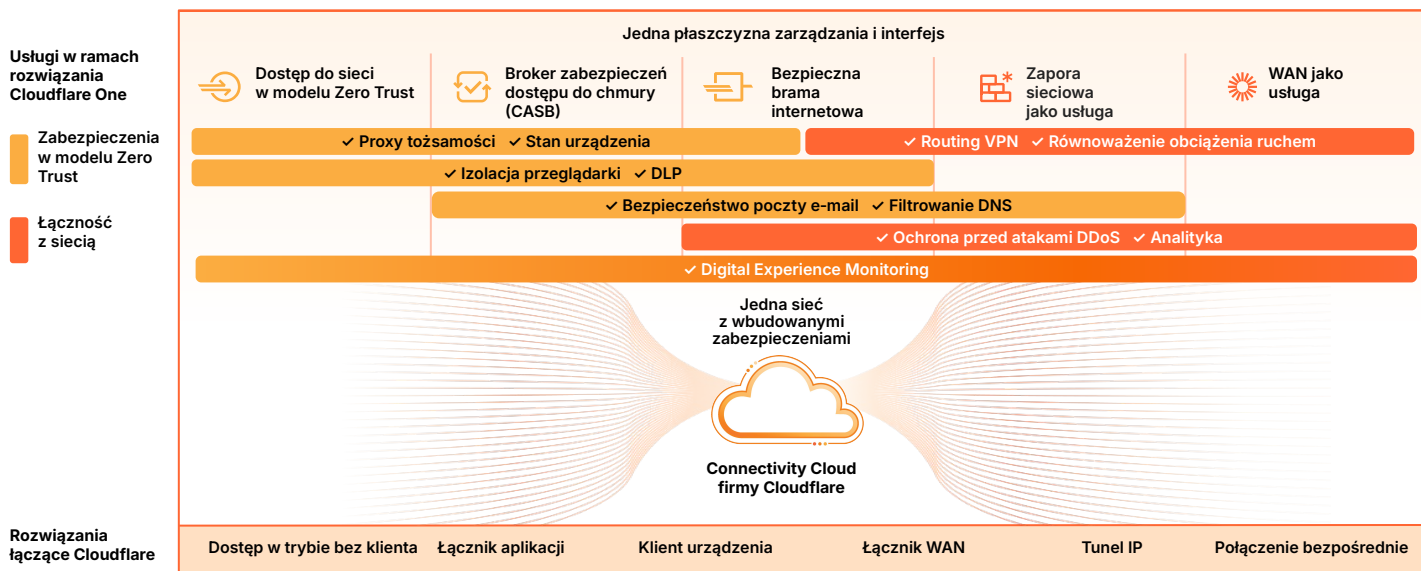
Szybsze osiągnięcie dojrzałości cyfrowej, zmniejszenia nakładów inwestycyjnych na sprzęt i konsolidacja rozwiązań punktowych dzięki komponowalnym, wbudowanym usługom bezpieczeństwa, które zapewniają całościowy wgląd w ruch sieciowy.

Everywhere Security

Wszystkie usługi działają w **ponad 330** miastach, więc cały ruch jest sprawdzany najbliżej źródła, co zapewnia spójną szybkość i skalę działania w każdym miejscu.



Jak działa rozwiązanie Cloudflare One?



Krótszy czas konfiguracji łączności typu „każdy z każdym” dzięki elastycznym rozwiązaniom łączącym typu on-ramp dla wszystkich zespołów

- **Zespoły ds. IT i bezpieczeństwa:** ochrona całego ruchu między użytkownikami a aplikacjami oraz zabezpieczenie ruchu dwukierunkowego i między lokalizacjami.
- **Zespoły ds. sieci:** uproszczenie łączności między lokalizacjami i obniżenie całkowitego kosztu eksploatacji dzięki nowoczesnej architekturze.
- **Zespoły DevOps:** zabezpieczenie nowoczesnych przepływów pracy między usługami i uproszczenie łączności równorzędnej / typu mesh.

Zintegrowane usługi wykraczające poza zakres rozwiązań SASE w ramach rozwiązania connectivity cloud

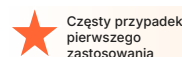
Cloudflare One łączy w sobie funkcje bezpieczeństwa i zwiększania wydajności, które zwykle nie są wbudowane w platformy SASE, co pozwala dodatkowo zmniejszyć złożoność infrastruktury IT. Na przykład:

- **Zabezpieczenia poczty e-mail w chmurze:** blokują zagrożenia przesyłane w wiadomościach e-mail.
- **Autorytatywny serwer DNS, równoważenie obciążenia ruchem i ochrona przed atakami DDoS:** nasze odwrotne serwery proxy i usługi sieciowe są wbudowane we wszystkie mechanizmy kontroli dostępu do aplikacji.

Priorytetowe zastosowania i od czego zacząć



Zapewnij bezpieczeństwo, automatyzację i większą elastyczność dzięki rozwiązaniom CrowdStrike, Microsoft i innym partnerom



Częsty przypadek pierwszego zastosowania



Przypadki kolejnych zastosowań