

Zabezpieczanie rozproszonych miejsc pracy

Spójna ochrona wszystkich żądań na jednej ujednoliconej płaszczyźnie zarządzania, z dowolnej lokalizacji biurowej

Przeniesienie zabezpieczenia do chmury

Ogranicz złożoność i zagrożenia dotyczące biur dzięki rozwiązaniom Cloudflare

Ze względu na to, że pracownicy wykonują swoje zadania zarówno w biurach, jak i zdalnie, wiele organizacji ponownie ocenia swoje aktualne metody zabezpieczania biur — niezależnie od tego, czy polegają na urządzeniach w centrach danych, czy zezwalają na bezpośredni, niezabezpieczony dostęp do Internetu.

Nowym priorytetem jest zapewnienie spójnej ochrony i doświadczenia użytkownikom, zarówno w sieci, jak i poza nią. Najczęściej oznacza to odejście od różnych narzędzi, takich jak sieci VPN, serwery proxy i zapory sieciowe, na rzecz jednej platformy zabezpieczeń dostarczanej w chmurze.

Cloudflare dostrzega, że organizacje modernizują zabezpieczenia biurowe w dwóch typowych przypadkach użycia.

Zalecany przypadek użycia:

Zabezpieczenie dostępu do aplikacji z wykorzystaniem modelu Zero Trust w celu zastąpienia sieci VPN

Egzekwuj szczegółowe, ukierunkowane na tożsamość zasady dostępu dla każdej aplikacji, zamiast pozwalać na ruch boczny w sieci firmowej.



- **Krok 1:** Integracja z dostawcami tożsamości
- **Krok 2:** Zapewnienie ochrony każdej aplikacji internetowej za pośrednictwem przeglądarki
- **Krok 3:** Zabezpieczenie środowisk SSH, VNC i RDP za pośrednictwem przeglądarki



Połącz dostęp z oddziałów i dostęp zdalny w ramach jednego wdrożenia, aby zapewnić spójne zasady oraz zminimalizować liczbę wymaganych dostawców. Wdróż dostęp ZTNA, aby rozszerzyć lub zastąpić przestarzałe sieci VPN w celu ograniczenia inwestycji w starsze technologie¹.

Gartner

Zalecany przypadek użycia:

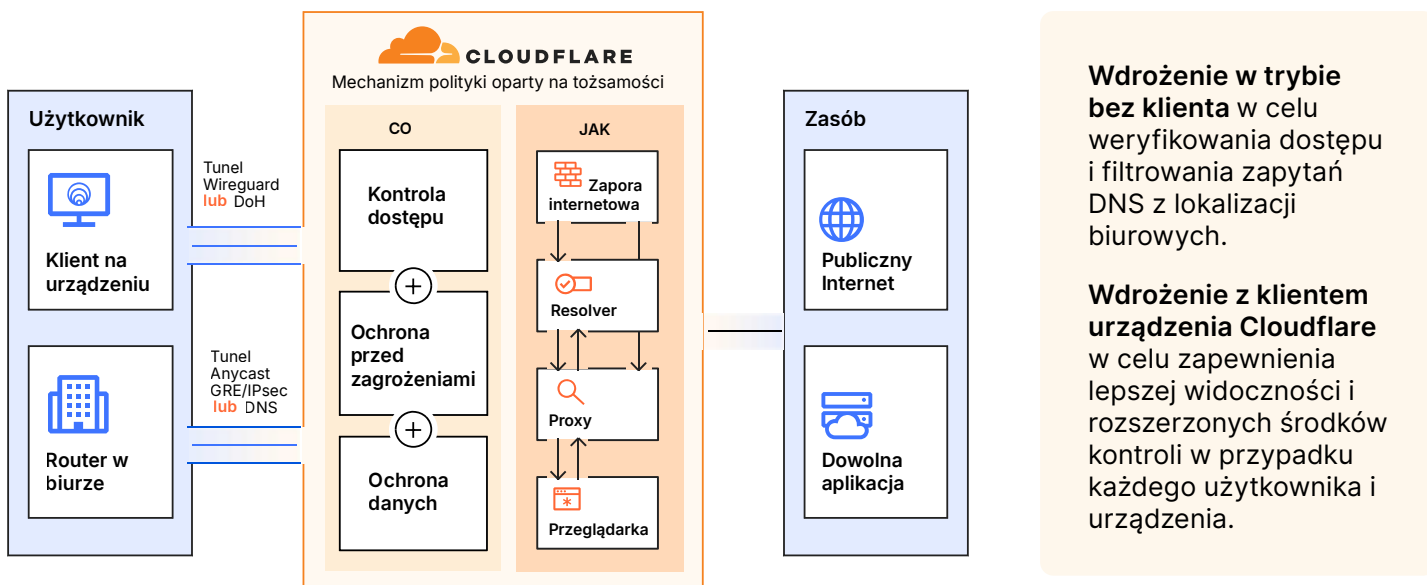
Filtrowanie dostępu do Internet w celu zapewnienia spójnych zabezpieczeń i skrócenia czasu do osiągnięcia korzyści

Chroń użytkowników biurowych najpierw za pomocą filtrowania DNS, a następnie przeprowadzaj bardziej kompleksowe inspekcje we wszystkich lokalizacjach. Koniec z dosyłaniem ruchu przez lokalne urządzenia zabezpieczające w centrach danych.



- **Krok 1:** Skierowanie ruchu DNS do globalnej sieci Cloudflare
- **Krok 2:** Skonfigurowanie usługi filtrowania DNS opartego na lokalizacji w celu ochrony przed oprogramowaniem typu ransomware, phishingiem i innymi zagrożeniami internetowymi
- **Krok 3:** Kontrola przepływu danych poprzez wymuszenie reguł HTTP, sieci i izolacji przeglądarki z nieograniczoną inspekcją protokołu TLS 1.3.

Jak to działa



Rysunek 1: Weryfikowanie, filtrowanie, izolowanie i sprawdzanie ruchu biurowego w jednym przejściu dzięki modelowi [Cloudflare Zero Trust](#)

Elastyczne rozwiązania typu on-ramp z dowolnego źródła

Zacznij od zastosowania rozwiązań Cloudflare do rozpoznawania nazw DNS za pośrednictwem routerów sieciowych. Stopniowo wysyłaj ruch z warstwy L3 do naszej sieci globalnej za pomocą tuneli GRE lub IPsec — lub korzystaj z istniejącej metody routingu SD-WAN.

Innym sposobem może być wdrożenie klienta Cloudflare na potrzeby filtrowania i inspekcji DNS oraz HTTP na urządzeniach zarządzanych.

Szybkie egzekwowanie zasad z możliwością skalowania globalnego

Wszystkie funkcje bezpieczeństwa, wydajności i niezawodności opracowano z myślą o uruchamianiu na każdym serwerze w każdym centrum danych w ponad 275 lokalizacjach i ponad 100 krajach.

Skalowanie naszej sieci oznacza, że zabezpieczenia są zawsze egzekwowane w pobliżu biur i użytkowników końcowych, gdziekolwiek się znajdują, z dużą szybkością za sprawą kontroli z jednym skanowaniem.

Inne przypadki użycia do zbadania w ciągu kolejnych sześciu do dwunastu miesięcy



Odzyskiwanie kontroli nad aplikacjami SaaS

Odkryj zagrożenia związane z szarą strefą IT, z której pracownicy korzystają w biurach i w domu, a następnie ogranicz ich negatywne skutki.

Zapobiegaj wyciekom danych i naruszeniom zgodności z przepisami dzięki zasadom CASB dostępnym z jednego pulpitu nawigacyjnego Cloudflare. [Dowiedz się, jak to działa.](#)



Przenoszenie ruchu MPLS

Zastąp prywatne połączenia MPLS, które są drogie, przestarzałe i wolne.

Uprość przestarzałą architekturę WAN, wykorzystując globalną sieć Cloudflare do zarządzania ruchem między oddziałami, centrami danych i usługami w chmurze publicznej. [Dowiedz się, jak to działa.](#)

1. Gartner Hype Cycle for Network Security, 2021 | GARTNER i HYPE CYCLE są zarejestrowanymi znakami towarowymi i usługowymi firmy Gartner, Inc. i/lub jej spółek zależnych w Stanach Zjednoczonych i na całym świecie, używanymi w niniejszym dokumencie za stosowaną zgodą. Wszelkie prawa zastrzeżone.