CLOUDFLARE

KRÓTKI OPIS PRODUKTU

Ochrona przed wyciekiem danych

Chroń poufne dane i zapewnij zgodność z przepisami w aplikacjach internetowych, prywatnych, SaaS, chmurowych, SI i pocztowych.

Najbardziej zintegrowana ochrona przed wyciekiem danych (DLP) dla ery agentowej

Dzięki Cloudflare DLP możesz wykrywać i blokować eksfiltrację wrażliwych danych w całej sieci i wszystkich aplikacjach (SaaS, SI, chmurowych i prywatnych oraz poczcie e-mail) bez zakłócania i obniżania produktywności użytkowników.

Chroń swoją własność intelektualną, kod źródłowy, dane umożliwiające identyfikację osoby przekazywane przez klientów oraz inne informacje, aby:

- **Egzekwować zgodność**, korzystając ze wstępnie utworzonych profili danych finansowych, dokumentacji medycznej i numerów ubezpieczenia społecznego.
- **Zabezpieczać dane firmowe**, blokując przesyłanie wrażliwych danych do nieautoryzowanych witryn służących do przechowywania w chmurze lub udostępniania plików.
- **Zabezpieczać prompty SI** poprzez skanowanie i redagowanie danych wrażliwych lub kodu źródłowego w danych wejściowych narzędzi takich jak ChatGPT i GitHub.
- **Zyskać wgląd w ruch danych** w całym zespole pracowników hybrydowych.

Dzięki oparciu na krawędzi globalnej Cloudflare inspekcja jest wykonywana w odległości milisekund od użytkownika, co gwarantuje szybką i ekonomiczną ochronę na dużą skalę.

Dostawca infrastruktury

Zidentyfikowane luki w zabezpieczeniach SaaS — takie jak szerokie udostępnianie wrażliwych plików SharePoint — w celu ograniczenia skutków utraty danych.

Zapoznaj się ze studium przypadku

Wiodący bank cyfrowy

Skonsolidowane zabezpieczenia w ramach jednego pulpitu nawigacyjnego zapewniającego ścisłą zgodność danych i ochronę przed oprogramowaniem typu ransomware na platformie bankowości mobilnej.

Dostawca telemedycyny

Zabezpieczone wrażliwe dane pacjentów (PHI/HIPAA) i przyspieszony dostęp dla szybko rosnącej liczby pracowników zdalnych z wykorzystaniem DLP i CASB.

Czym wyróżnia się Cloudflare?

Uproszczone zabezpieczenia SaaS i SI

Zarządzaj wykorzystaniem SI przez pracowników, blokując podejrzane treści, a także ograniczaj ryzyko eksfiltracji poprzez identyfikowanie i korygowanie danych wrażliwych przechowywanych w środowiskach SaaS i chmurowych.

Ujednolicone zarządzanie zasadami

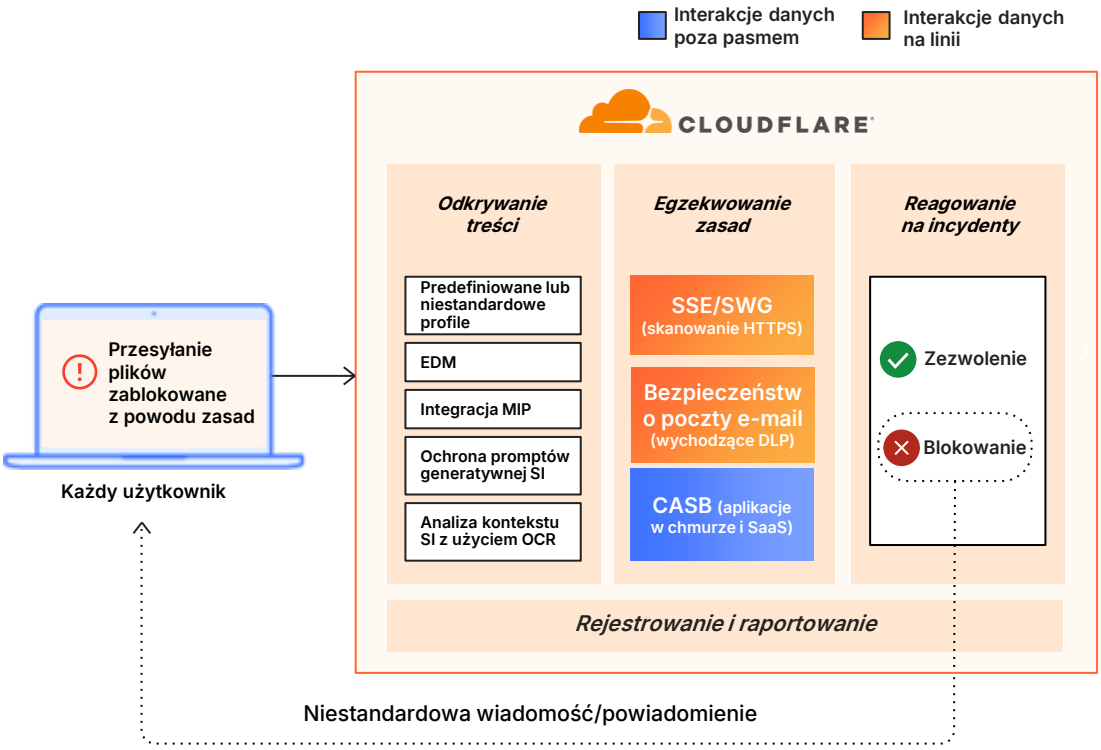
Skonfiguruj profile DLP, pozycje wykrywania oraz etykiety poufności Microsoft Purview, aby skonsolidować zabezpieczenia ruchu wychodzącego, dokumentów, plików PDF i obrazów.

Adaptacyjna kontrola danych

Przekazuj opinie dla każdego wykrycia, aby uściślić dokładność wykrywania analizy kontekstu SI. Rozwiązanie DLP dostosowuje się do Twoich charakterystycznych wzorców danych i ruchu sieciowego, aby zredukować liczbę fałszywych alarmów.

Chcesz dowiedzieć się więcej o tym produkcie? Zapoznaj się z naszą architekturą referencyjną lub porozmawiaj z ekspertem.

Ochrona danych we wszystkich kanałach roboczych



Jak to działa?

Cloudflare DLP zapewnia zautomatyzowaną, kontekstową inspekcję ruchu HTTPS i poczty e-mail.

Rozwiązanie wbudowane natywnie w ramach modelu Zero Trust firmy Cloudflare eliminuje luki w zabezpieczeniach, konsolidując ochronę danych w ramach jednej, ujednoliconej platformy dla zapewnienia bezproblemowej widoczności i kontroli we wszystkich kanałach.

Przykładowe możliwości DLP	
Profile DLP	Wdrażaj wstępnie zdefiniowane profile dla danych identyfikacyjnych, medycznych i finansowych oraz poświadczeń lub twórz niestandardowe profile, aby zabezpieczać zastrzeżone zasoby, takie jak wewnętrzne nazwy projektów lub niepublikowana własność intelektualna.
Microsoft Information Protection (MIP)	Pozyskuj etykiety poufności MIP, aby automatycznie egzekwować zasady (np. blokowanie danych poufnych) bez ponownego tagowania plików.
Dokładne dopasowanie danych (EDM)	Prześlij skróty zestawów danych (np. bazy danych konkretnego klienta) w celu wykrywania dokładnych wartości, a nie ogólnych wzorców. Blokuj konkretne rekordy, jednocześnie znacząco ograniczając liczbę wyników fałszywie dodatnich.
Odcisk palca dokumentu	Zabezpiecz poufne dokumenty, tworząc i przechowując unikalne „odciski cyfrowe" (skróty/wzorce), które są następnie porównywane z ruchem sieciowym w celu identyfikacji i zablokowania podobnych dokumentów.
Ochrona promptów generatywnej SI	Zapobiegaj wklejaniu danych wrażliwych (kodu źródłowego, danych umożliwiających identyfikację osoby klienta) do publicznych modeli LLM. Kontroluj żądania HTTPS wysyłane do narzędzi takich jak ChatGPT czy Gemini, aby egzekwować bezpieczne korzystanie ze sztucznej inteligencji.
Analiza kontekstu SI i ocena pewności	Wykorzystaj uczenie maszynowe do analizowania słów kluczowych związanych z kontekstem i bliskością. Ustaw progi ufności, aby automatycznie blokować dopasowania o wysokim ryzyku, jednocześnie rejestrując zdarzenia o niższym poziomie ufności w celu dostrojenia systemu.
Optyczne rozpoznawanie znaków (OCR)	Automatycznie skanuj i wyodrębniaj tekst z plików obrazów (PNG, JPG/JPEG), aby uniemożliwić użytkownikom omijanie zabezpieczeń poprzez tworzenie zrzutów ekranu z poufnych dokumentów.
Szkolenie i edukacja użytkowników	Wyświetlaj konfigurowalne, działające w czasie rzeczywistym powiadomienia, które natychmiast informują użytkowników o naruszeniach polityki bezpieczeństwa.
Ujednolicona analiza danych śledczych i rejestrowanie	Połącz szczegółowe rejestrowanie zdarzeń z bezpieczną inspekcją ładunku. Analizuj konkretne fragmenty danych i kontekst użytkownika, aby natychmiast weryfikować incydenty i dostosowywać zasady.

