CLOUDFLARE

KRÓTKI OPIS ROZWIĄZANIA

Ochrona poufnych danych

Lepsza architektura sieci dla skuteczniejszej, wydajniejszej i sprawniejszej ochrony danych.

Ujednolicona ochrona danych w każdym miejscu

Obowiązek ochrony danych nie jest niczym nowym, ale przejście na architekturę chmury hybrydowej w połączeniu z szybkim wdrażaniem sztucznej inteligencji stwarza nowe wyzwania:

- **93% pracowników** przyznaje, że wprowadza informacje do narzędzi SI bez uzyskania zgody[1]
- **W 79% wszystkich krajów** obowiązują przepisy dotyczące prywatności danych[2]

Cloudflare zapewnia spójne mechanizmy kontroli w całym cyklu życia danych:

- **Bezpieczeństwo we wszystkich obszarach:** wdrażaj spójne środki kontroli w odniesieniu do Internetu, SaaS, poczty e-mail i ruchu chmurowego.
- **Blokowanie eksfiltracji SI:** analizuj prompty generatywnej SI w celu blokowania poufnych danych i zarządzania wykorzystaniem SI.
- **Zarządzanie ryzykiem związanym z danymi:** odkryj szarą strefę IT/SI i zarządzaj nią, a także skanuj aplikacje SaaS i chmurowe za pomocą CASB.

„Wzrost liczby tych wszystkich nieautoryzowanych narzędzi SI skłania nas do ponownego rozważenia naszego podejścia do bezpieczeństwa. Analizujemy teraz model SASE" – *Kierownik ds. bezpieczeństwa informacji,* ***AllSaints***

Dlaczego warto wybrać model SASE zamiast korporacyjnej ochrony przed wyciekiem danych (DLP)?

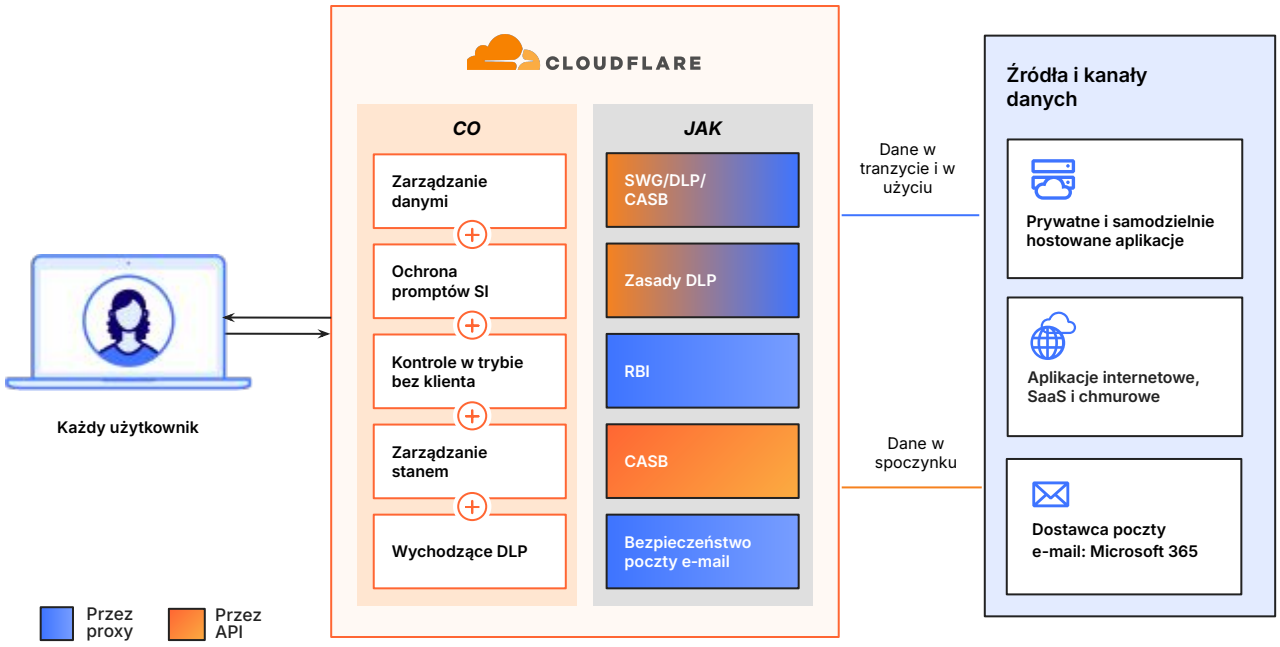
Platforma krawędzi usługi bezpiecznego dostępu (Secure Access Service Edge, SASE) firmy Cloudflare jest zaprojektowana tak, aby znajdować się pomiędzy Twoimi pracownikami a każdą aplikacją i źródłem danych. Dzięki temu SASE stanowi dla wielu osób idealny punkt początkowy dla bezpiecznej ochrony danych.

Niezależnie od tego, czy pracownicy uzyskują dostęp do danych w aplikacjach SaaS, pobierają poufne pliki, czy korzystają z narzędzi generatywnej SI, platforma SASE firmy Cloudflare zapewnia spójne środki kontroli bezpieczeństwa we wszystkich interakcjach z danymi.

Jak to działa?

Platforma SASE firmy Cloudflare działa w trybie inline między pracownikami a zasobami organizacji, zapewniając spójną widoczność oraz środki kontroli.

Oparta na sztucznej inteligencji ochrona danych z udziałem platformy SASE firmy Cloudflare w obszarze ruchu internetowego, SaaS, poczty e-mail i chmury



Wbudowana ochrona danych w czasie rzeczywistym

- **Szczegółowa ochrona DLP:** zatrzymaj ujawnianie poufnych danych dzięki kontekstowym mechanizmom wykrywania danych umożliwiających identyfikację osób, kodu źródłowego, danych dotyczących klientów i innych treści.
- **Ochrona DLP wychodzącej poczty e-mail:** automatycznie oznaczaj poufne dane w wychodzących wiadomościach e-mail, aby zapobiec przypadkowym wyciekom danych.
- **Ochrona promptów:** wykrywaj i blokuj ryzykowne prompty i odpowiedzi SI na podstawie intencji (np. próby złamania zabezpieczeń, nadużycia kodu czy żądania danych umożliwiających identyfikację osoby).

Bezpieczny dostęp i kontrole z klientem

- **Bezpieczny dostęp do aplikacji:** egzekwuj zasady dostępu do sieci w modelu Zero Trust (ZTNA), takie jak szczegółowe skanowanie DLP dla połączeń agentowej SI, we wszystkich aplikacjach korporacyjnych.
- **Kontrole stanu bezpieczeństwa urządzeń:** steruj dostępem na podstawie szczegółowych kontroli stanu bezpieczeństwa, na przykład szyfrowania dysków lub włączonej ochrony DLP w punkcie końcowym.
- **Kontrole bez klienta:** zastosuj mechanizmy kontroli danych oparte na przeglądarce, aby zabezpieczyć zasady dostępu stron trzecich i modelu BYOD dla pracowników.

Szara strefa IT i zagrożenia dla stanu bezpieczeństwa

- **Wykrywanie szarej strefy IT i SI:** odkrywaj obszary szarej strefy IT i SI w całym swoim środowisku oraz zarządzaj nimi. Kwantyfikuj ryzyko dzięki ocenom zaufania do aplikacji i wskaźnikom transferu danych, aby szybko minimalizować zagrożenia.
- **Zarządzanie stanem:** skanuj aplikacje SaaS i środowiska chmury pod kątem zagrożeń dla stanu bezpieczeństwa. Podejmij konkretne kroki w celu usunięcia ustaleń dotyczących bezpieczeństwa.
- **Kontrola dzierżawcy:** blokuj osobistych dzierżawców aplikacji SaaS, aby zapobiegać eksfiltracji danych.

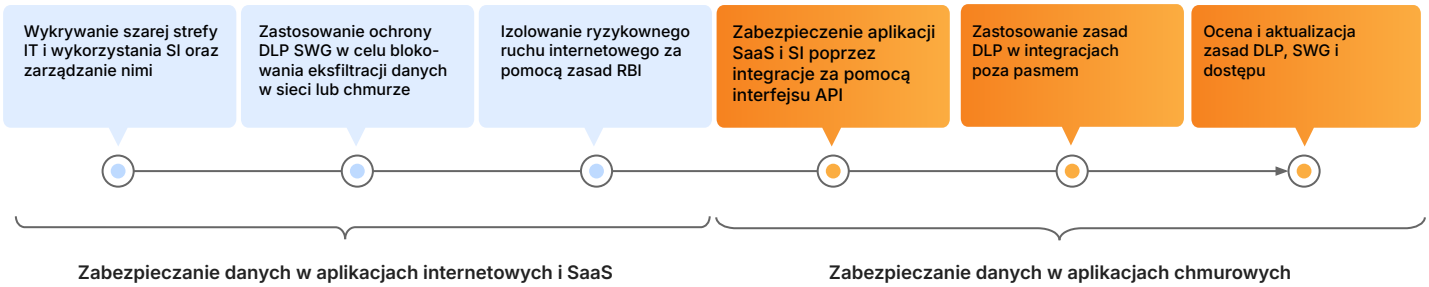
Integracje i raportowanie

- **Integracje CASB:** wykonaj bezproblemową integracją z wiodącymi platformami SaaS i SI (w tym Microsoft 365, Google Workspace i ChatGPT) w celu realizacji skanowania CASB opartego na interfejsie API.
- **Integracja z Microsoft MIP:** korzystaj z ciągłej synchronizacji z etykietami Microsoft Information Protection (MIP) dla spójnych zasad DLP.
- **Obserwowalność i analiza**: bezpiecznie zapisuj dane w preferowanym systemie SIEM na potrzeby audytu lub analizuj dzienniki natychmiast za pomocą pulpitu nawigacyjnego lub interfejsu API.

Przykładowy proces ochrony danych osobowych

Zacznij od wykrywania szarej strefy IT i wykorzystania sztucznej inteligencji, aby uzyskać widoczność powierzchni narażenia na atak. Skonfiguruj podstawowe zasady ochrony przed wyciekiem danych (DLP) w SWG, aby blokować wycieki danych o wysokim ryzyku z niezarządzanych aplikacji w chmurze, oraz przeprowadź wdrożenie zdalnej izolacji przeglądarki (RBI) dla niezatwierdzonego ruchu internetowego.

Następnie wdróż CASB, aby zabezpieczyć zatwierdzone aplikacje SaaS i SI poprzez zapobieganie błędom konfiguracji i egzekwowanie wewnętrznych zasad udostępniania. Udoskonal i zintegruj szczegółowe zasady ochrony DLP oraz dostępu w SWG, poczcie e-mail i CASB, aby zyskać zautomatyzowane, ujednolicone środowisko działań prewencyjnych obejmujące wszystkie główne wektory danych.



Przykładowe zastosowania na początek

- **Blokowanie w czasie rzeczywistym eksfiltracji danych umożliwiających identyfikację osoby (PII) oraz chronionych informacji medycznych** we wszystkich niezatwierdzonych kanałach komunikacji i przechowywania.
- **Ochrona kodu źródłowego i własności intelektualnej** przed kradzieżą wewnętrzną i nieautoryzowanym rozpowszechnianiem.
- **Egzekwowanie zasad ochrony promptów** dla aplikacji generatywnej SI w celu zapobiegania ujawnianiu poufnych danych i zanieczyszczaniu modeli.
- **Zapobieganie błędnym konfiguracjom** i wprowadzanie szczegółowych mechanizmów kontroli dostępu we wszystkich aplikacjach SaaS i SI.

Wyniki dotyczące klientów

EESTI RAUDTEE

Dostawca infrastruktury
Zapoznaj się ze studium przypadku

Ograniczenie utraty danych i luk w zabezpieczeniach SaaS

poprzez identyfikację wycieków danych i błędnych konfiguracji.

APPLIED

Technologie ubezpieczeniowe
Zapoznaj się ze studium przypadku

Izolowanie publicznych narzędzi generatywnej SI, takich jak ChatGPT,

w celu blokowania kopiowania i wklejania poufnych danych.

Flo

Wiodąca aplikacja zdrowotna
Zapoznaj się ze studium przypadku

Ochrona danych pacjentów

i osiągnięcie zgodności dzięki zabezpieczeniom poczty e-mail i modelowi Zero Trust.

CREDIT SAISON INDIA

Pożyczkodawca NBFC
Zapoznaj się ze studium przypadku

Ochrona danych umożliwiających identyfikację osoby i osiągnięcie zgodności

w celu zapobiegania niechcianemu wyciekowi danych.

Chcesz porozmawiać o swoich potrzebach w zakresie ochrony danych?

Umów się na warsztaty

1. Badanie Manage Engine z 2025 r.: źródło
2. Konferencja Narodów Zjednoczonych w zakresie Handlu i Rozwoju w 2025 r.: źródło

 | +44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/pl-pl/