CLOUDFLARE

KRÓTKI OPIS PRODUKTU

Broker zabezpieczeń dostępu do chmury (CASB)

Kompleksowa widoczność i kontrola nad środowiskami SaaS, SI i chmurowymi — ochrona danych bez spowalniania innowacji.

Bezpieczeństwo SaaS stworzone z myślą o erze SI

Zabezpiecz swoje środowiska SaaS, SI i chmurowe bez zmniejszania produktywności. Dzięki rozwiązaniu Cloudflare CASB błyskawicznie wykrywaj błędne konfiguracje, szarą strefę IT oraz zagrożenia danych dotyczące pracowników hybrydowych.

- **Automatyzacja zgodności** — natychmiast wykrywaj i usuwaj luki w zabezpieczeniach, takie jak nieautoryzowane udostępnianie plików czy słabe uwierzytelnianie wieloskładnikowe, w Microsoft 365, Google Workspace i GitHub.
- **Powstrzymywanie szarej strefy SI/IT** — wykrywaj nieautoryzowane aplikacje i blokuj dostęp do niezatwierdzonych witryn przechowywania w chmurze lub udostępniania plików.
- **Bezpieczne korzystanie ze sztucznej inteligencji** — uzyskaj wgląd we wdrażanie narzędzi SI i egzekwuj ograniczenia dzierżawy na takich platformach jak ChatGPT i Gemini, aby zapewnić dostęp wyłącznie w ramach środowiska firmowego.
- **Zarządzanie ryzykiem dotyczącym podmiotów zewnętrznych** — identyfikuj i wycofuj ryzykowne integracje z podmiotami zewnętrznymi, które mają dostęp do danych firmowych.

Oparta na naszej globalnej sieci, sterowana przez interfejsy API i działająca inline ochrona Cloudflare CASB zapewnia szybkie i opłacalne bezpieczeństwo na dużą skalę.

EESTI RAUDTEE

Dostawca infrastruktury

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

Zapoznaj się ze studium przypadku

APPLIED

Dostawca oprogramowania ubezpieczeniowego

Zabezpieczono wdrożenie generatywnej SI poprzez blokowanie wprowadzania danych wrażliwych do takich narzędzi jak ChatGPT, bez zmniejszania produktywności pracowników.

Zapoznaj się ze studium przypadku

Dostawca usług telemedycznych

Zabezpieczono wrażliwe dane pacjentów (PHI/HIPAA) oraz przyspieszono dostęp dla szybko rosnącej liczby pracowników zdalnych dzięki rozwiązaniom DLP i CASB.

Czym wyróżnia się Cloudflare?

Natychmiastowe wdrożenie w trybie bez klienta

Połącz się z aplikacjami SaaS i SI, takimi jak Microsoft 365, GitHub, Slack i ChatGPT, w kilka minut przez interfejs API. Natychmiast skanuj w poszukiwaniu historycznych zagrożeń, błędnych konfiguracji i narażenia danych, bez instalowania klientów.

Ciągłe zarządzanie poziomem bezpieczeństwa danych w SaaS i chmurze

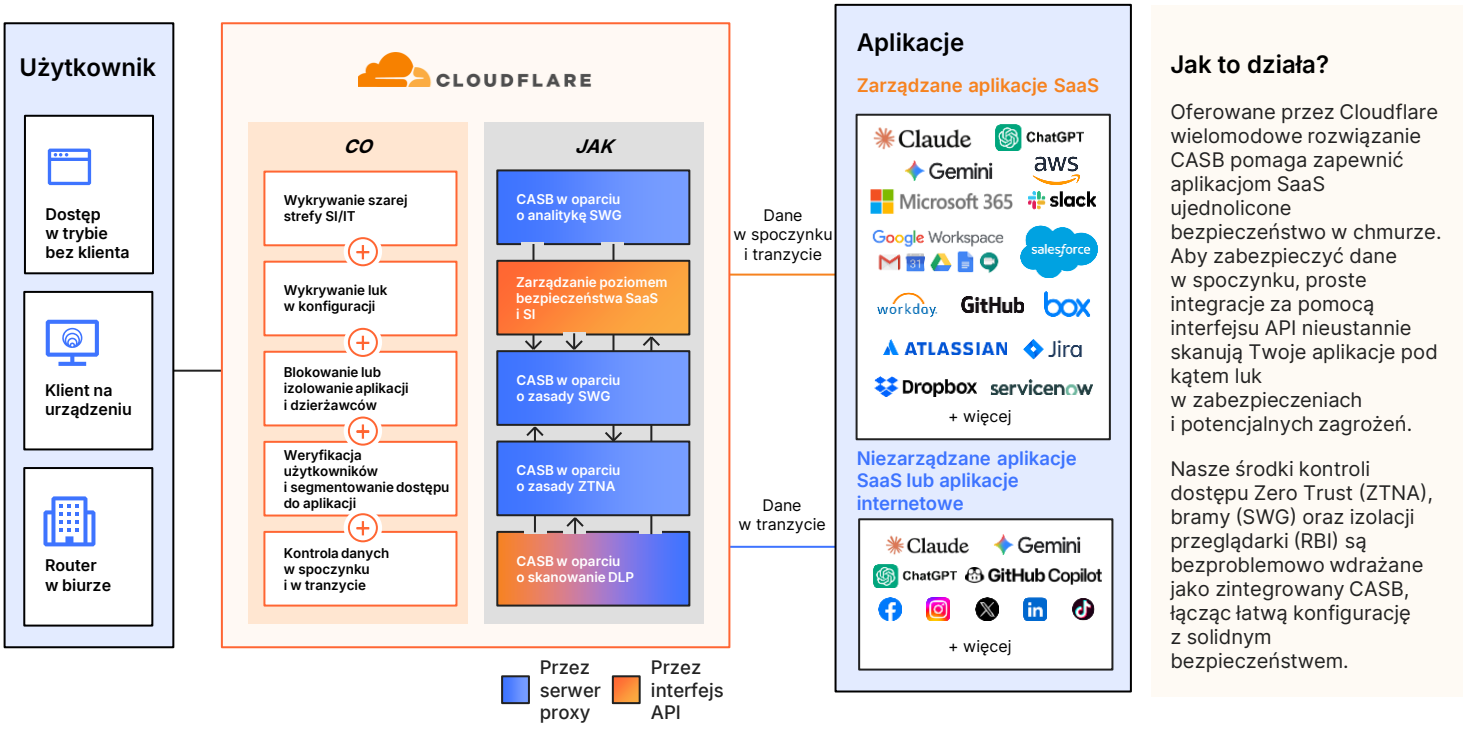
Identyfikuj odchylenia konfiguracji zabezpieczeń oraz niezabezpieczone ustawienia w ramach SaaS i pamięci masowej w chmurze. Wykrywaj i wycofuj krytyczne błędne konfiguracje, takie jak publiczne zasobniki S3 lub uprawnienia otwartych projektów, zanim doprowadzą do naruszenia bezpieczeństwa.

Spójna kontrola nad szarą strefą IT

Nie przełączaj się między konsolami. Używaj danych CASB do wykrywania niezatwierdzonych aplikacji, a następnie natychmiast uruchamiaj zasady Zero Trust, aby blokować lub izolować ten ruch za pośrednictwem Cloudflare Gateway, zarządzając wszystkim z jednego panelu sterowania.

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

Kompleksowe bezpieczeństwo dla SaaS, SI i szarej strefy IT



Jak to działa?

Oferowane przez Cloudflare wielomodowe rozwiązanie CASB pomaga zapewnić aplikacjom SaaS ujednolicone bezpieczeństwo w chmurze. Aby zabezpieczyć dane w spoczynku, proste integracje za pomocą interfejsu API nieustannie skanują Twoje aplikacje pod kątem luk w zabezpieczeniach i potencjalnych zagrożeń.

Nasze środki kontroli dostępu Zero Trust (ZTNA), bramy (SWG) oraz izolacji przeglądarki (RBI) są bezproblemowo wdrażane jako zintegrowany CASB, łącząc łatwą konfigurację z solidnym bezpieczeństwem.

Ochrona danych poza pasmem i poziom bezpieczeństwa SaaS (oparte na interfejsie API)	
Zarządzanie poziomem bezpieczeństwa SaaS (SSPM)	Skanuj aplikacje SaaS oraz pamięć masową w chmurze za pośrednictwem interfejsu API, aby wykrywać błędne konfiguracje i ryzykowne integracje podmiotów zewnętrznych (np. publiczne zasobniki S3, nieautoryzowane aplikacje OAuth lub naruszenia MFA).
Ochrona danych SaaS (DLP)	Wykrywaj pliki wrażliwe (PCI, dane umożliwiające identyfikację osoby, sekrety) dzięki skanowaniu danych w spoczynku, a następnie automatycznie usuwaj naruszenia (np. cofaj publiczny dostęp do plików), aby egzekwować zgodność.
Wbudowana ochrona danych (oparta na serwerach proxy)	
Wykrywanie szarych stref SI i IT	Natychmiastowa widoczność nieautoryzowanego użycia aplikacji. Automatycznie kategoryzuj oraz blokuj lub izoluj ryzykowne aplikacje (np. niezatwierdzone konwertery PDF lub narzędzia SI) na podstawie wskaźników zaufania.
Wbudowana ochrona DLP i OCR	Wykrywaj dane wrażliwe w ruchu dzięki funkcji dokładnego dopasowania danych (EDM) oraz zaawansowanym klasyfikatorom. Wykorzystaj funkcję OCR (Optical Character Recognition), aby rozszerzyć te zabezpieczenia na obrazy i blokować wycieki danych.
Ochrona promptów generatywnej SI	Zapobiegaj wklejaniu danych wrażliwych, takich jak kod źródłowy czy dane umożliwiające identyfikację klienta, do publicznych modeli LLM. Kontroluj żądania HTTPS wysyłane do takich narzędzi jak ChatGPT czy Gemini, aby egzekwować bezpieczne korzystanie ze sztucznej inteligencji.
Kontrola dzierżawców	Egzekwuj wyłącznie firmowy dostęp do takich aplikacji jak Microsoft 365, Google Workspace czy Slack, aby blokować logowanie na konta prywatne na urządzeniach firmowych.
Ujednolicone zarządzanie	
Jeden klient	Nie jest wymagany oddzielny klient CASB. Ujednolicony klient obsługuje ZTNA, SWG i CASB z kontrolą z jednym skanowaniem.
Ocena ryzyka dotyczącego użytkowników	Wykrywaj użytkowników z przejętymi kontami poprzez korelowanie wyników CASB z anomaliami behawioralnymi w celu przypisania dynamicznych ocen ryzyka.
Logpush	Kompleksowe rejestrowanie obejmuje wszystkie żądania, użytkowników i urządzenia. Natychmiast eksportuj dzienniki CASB do Splunk, Datadog lub S3 na potrzeby analizy SIEM.

 | +44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/pl-pl/ REV:BDES-8793.2026JAN15