Wykrywaj korzystanie z szarej strefy SI i IT przez pracowników

Rozszerz widoczność w zakresie nieautoryzowanych narzędzi SI i SaaS dzięki inspekcji ruchu oferowanej przez Cloudflare

Ujawnij to, co ukryte

Szara strefa IT nie jest nowym problemem, lecz gwałtowne upowszechnianie nieautoryzowanych narzędzi SI wywołuje współczesny kryzys:

- **20%** organizacji odnotowało w 2025 roku naruszenia bezpieczeństwa wynikające z incydentów związanych z szarą strefą SI[1]
- **85%** liderów IT przyznaje, że pracownicy zaczynają korzystać z narzędzi SI, zanim dział IT zdąży je ocenić[2]

Cloudflare przywraca organizacjom pełną widoczność, umożliwiając im kontrolę nad rozszerzającą się powierzchnią narażenia na atak:

- **Sprawdzaj status aplikacji** — klasyfikuj aplikacje SI i SaaS jako zatwierdzone, niezatwierdzone lub będące w trakcie oceny
- **Egzekwuj zasady w zależności od statusu aplikacji —** zezwalaj, blokuj, izoluj, stosuj mechanizmy wykrywania DLP w interakcjach, ograniczaj przesyłanie plików i więcej
- **Analizuj korzystanie z aplikacji** — monitoruj zbiorcze trendy i przeprowadzaj szczegółowe analizy
- **Oceniaj ryzyko dotyczące aplikacji** — weryfikuj ich wiarygodność na podstawie wskaźników zaufania aplikacji

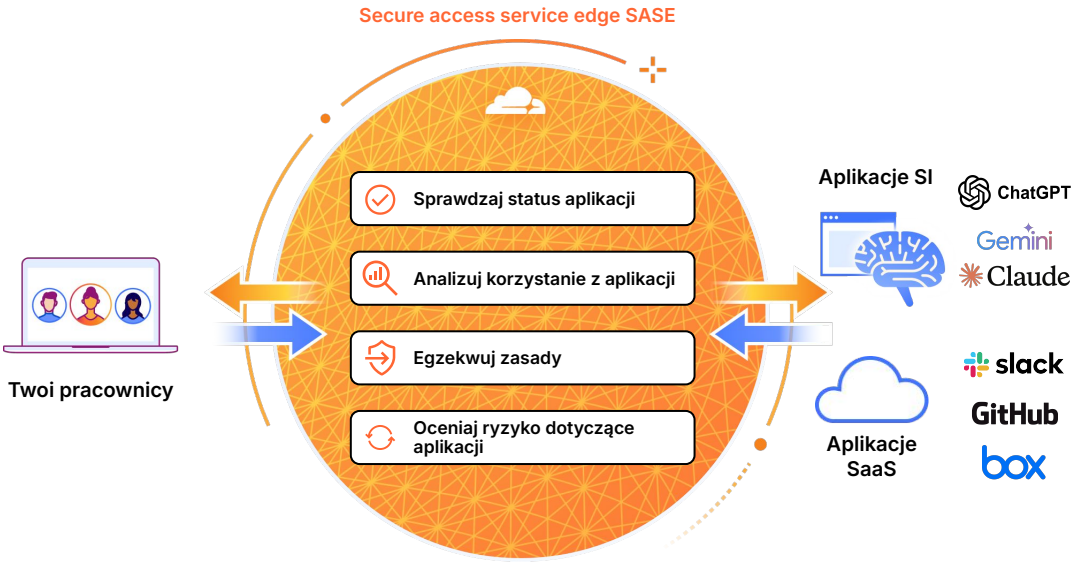
Unikalne zagrożenia związane z szarą strefą SI

Szara strefa SI różni się od tradycyjnej szarej strefy IT. Podczas gdy aplikacje SaaS służą głównie do przechowywania lub udostępniania plików, narzędzia SI przetwarzają i uczą się na podstawie wszelkich danych wprowadzanych przez pracowników.

Oznacza to, że dane wrażliwe, takie jak własność intelektualna, dane dotyczące klientów czy kod źródłowy, mogą zostać nieodwracalnie wchłonięte i wykorzystane do trenowania modelu, bez możliwości ich usunięcia.

Jak to działa?

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



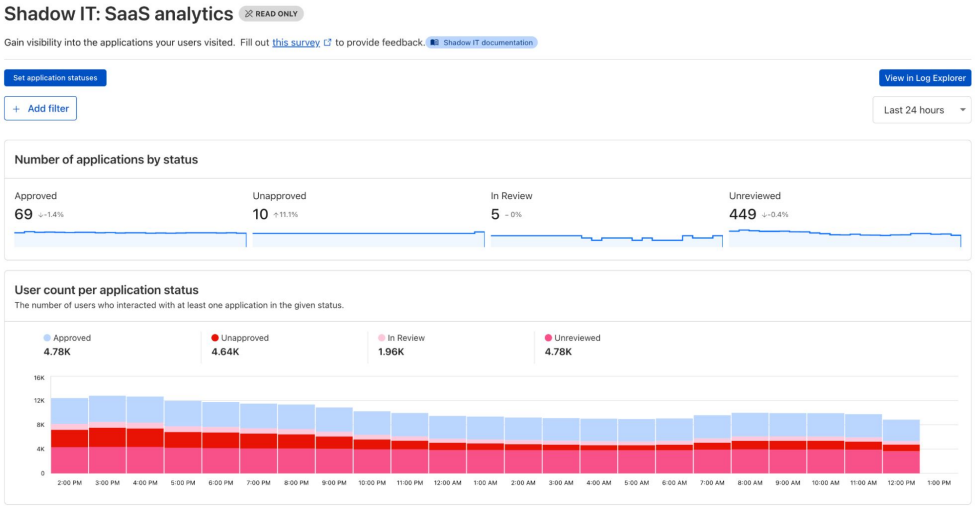
Dodatkowo można zintegrować brokera CASB Cloudflare za pośrednictwem interfejsu API, aby skanować pod kątem błędnych konfiguracji, aktywności użytkowników oraz danych wrażliwych. Zarządzaj poziomem bezpieczeństwa w aplikacjach SI (ChatGPT, Claude, Google Gemini) i innych aplikacjach SaaS. Użyj rozwiązania CASB w połączeniu z dostawcą tożsamości, aby monitorować przypadki uwierzytelniania użytkowników w nieautoryzowanych aplikacjach zewnętrznych.

Przykładowe pulpity nawigacyjne

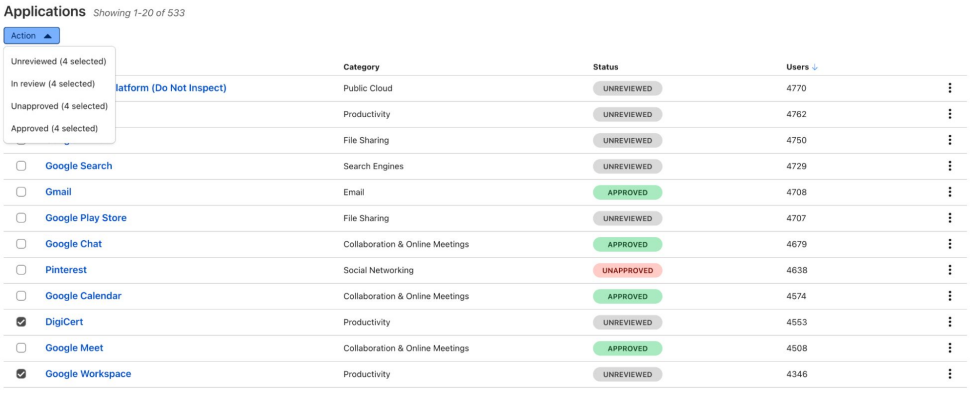
Filtruj ten ogólny podgląd wykorzystania aplikacji na podstawie:

- aplikacji i jej typu,
- statusu zatwierdzenia,
- ochrony dzięki ZTNA,
- liczby użytkowników.

Aby uzyskać więcej informacji, kliknij nazwę dowolnej aplikacji SI, aby wyświetlić szczegółowe dane o korzystających z niej użytkownikach lub grupach, częstotliwości użycia, lokalizacji i ilości przesyłanych danych.



Rysunek 1: Pulpit analityczny dla szarej strefy IT



Rysunek 2: Oznaczanie statusów aplikacji

Porządkuj aplikacje i definiuj zasady dostępu w zależności od statusu zatwierdzenia:

- Zatwierdzone (autoryzowane)
- Niezatwierdzone (nieautoryzowane)
- W trakcie przeglądu
- Nieocenione

Potrzebujesz więcej wskazówek technicznych? Dzięki tej ścieżce edukacyjnej dowiedz się, jak tworzyć zasady.

Chcesz dowiedzieć się więcej o tym, jak zabezpieczyć wdrażanie SI w Twojej organizacji?

Zapoznaj się z kolejnymi zastosowaniami

Umów się na warsztaty

1. Raport IBM Cost of a Data Breach 2025: źródło
2. Badanie Manage Engine z 2025 roku: źródło

