CLOUDFLARE

PRZEGLĄD PRODUKTU

Zabezpieczenia poczty e-mail Cloudflare

Zapewnianie autonomicznej, wielokanałowej ochrony na potrzeby bezpiecznej komunikacji w środowisku pracy

Ochrona przed ukierunkowanymi atakami phishingowymi

Bezproblemowe blokowanie i izolowanie zagrożeń niewidocznych dla innych rozwiązań

Ponieważ poczta e-mail jest najczęściej używaną i najczęściej wykorzystywaną aplikacją biznesową, ochrona użytkowników przed atakami phishingowymi, które mają na celu naruszenie ich zaufania, jest ważniejsza niż kiedykolwiek wcześniej. W miarę jak organizacje coraz częściej wdrażają usługi poczty e-mail w chmurze za pośrednictwem platform Microsoft 365 i Google Workspace, aby lepiej wspierać pracowników hybrydowych, podmioty zagrażające rozpoczęły bardziej ukierunkowane ataki o niskim wolumenie, które są w stanie ominąć tradycyjne bezpieczne bramki poczty e-mail (SEG), takie jak Proofpoint i Mimecast.

Właśnie dlatego natywne rozwiązanie chmurowe Cloudflare do zabezpieczania poczty e-mail zostało specjalnie zaprojektowane, aby wykorzystać prewencyjną analizę informacji dotyczących kampanii, analizę treści opartą na uczeniu maszynowym oraz ujednoliconą platformę zabezpieczeń opartą na modelu Zero Trust, aby powstrzymywać zagrożenia phishingowe, zanim dotrą do pracowników.

91%

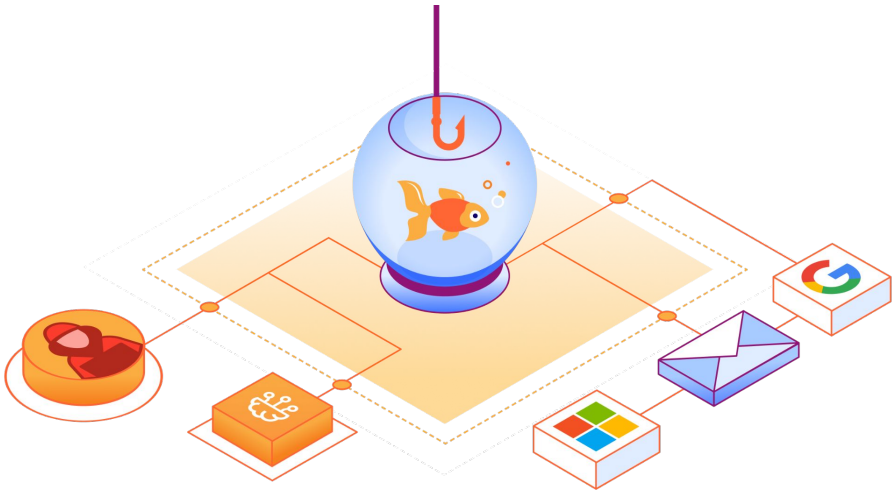
wszystkich cyberataków rozpoczyna się od phishingowej wiadomości e-mail[1]

50 mld

strat spowodowanych atakami BEC w ciągu ostatniej dekady[2]

81%

organizacji doświadczyło ataku wielokanałowego w ciągu ostatnich 12 miesięcy[3]



Powstrzymywanie naruszeń firmowej poczty e-mail (BEC)

Wykrywanie fałszywych i przejętych kont za pomocą warstwowej analizy kontekstowej opartej na uczeniu maszynowym.

Izolowanie ataków opóźnionych i wielokanałowych

Izolowanie użytkowników od złośliwych treści internetowych dostarczanych z wykorzystaniem nieznanych i zamaskowanych linków.

Blokowanie oprogramowania ransomware i złośliwych załączników

Zapobieganie próbom wymuszeń i złośliwemu kodowi, które mogą zagrozić Twojej organizacji.

Lepsza ochrona i prostota obsługi

Wdrożenie warstwowych zabezpieczeń zapewniających lepszą ochronę za ułamek kosztów

W miarę jak ataki phishingowe nadal się nasilają, Microsoft i Google kontynuują rozwijanie natywnej funkcjonalności zapewniającej podstawowe zabezpieczenia poczty elektronicznej i danych, takie jak uwierzytelnianie, archiwizacja i szyfrowanie po stronie klienta. Jednak cyberprzestępcy udoskonalili swoje taktyki, aby przeprowadzać bardziej ukierunkowane i trudniejsze do wykrycia ataki, które często omijają natywne mechanizmy bezpieczeństwa i skutkują wyższym wskaźnikiem sukcesu.

Dzięki zastosowaniu rozwiązania Cloudflare organizacje mogą automatycznie blokować lub izolować ukierunkowane ataki phishingowe, które wykorzystują złośliwe linki, załączniki i przejęte konta do kradzieży poufnych informacji i popełniania oszustw finansowych.

Wzmocnij swoje istniejące mechanizmy bezpieczeństwa poczty e-mail

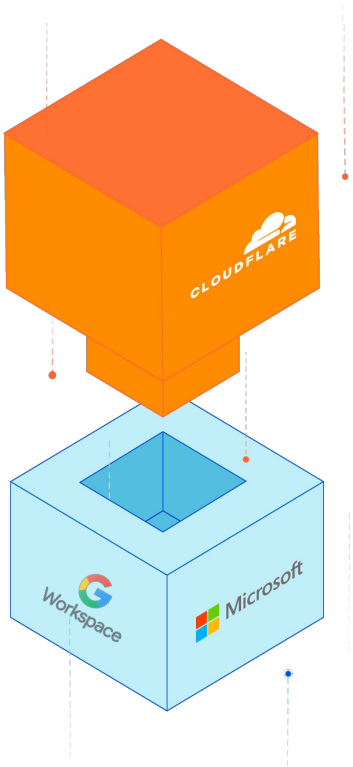
Natywne rozwiązanie chmurowe Cloudflare do zabezpieczania poczty e-mail może zostać wdrożone w ciągu kilku minut, aby ulepszyć istniejące wdrożenia SEG lub uzupełnić wbudowane funkcje poczty elektronicznej oferowane przez Microsoft i Google. Przy niewielkich lub zerowych wymaganiach dotyczących dostosowywania organizacje mogą uzyskać lepszą ochronę przed phishingiem, poświęcając mniej czasu i wysiłku na bieżące zarządzanie bezpieczeństwem.

„Od czasu wdrożenia rozwiązań Cloudflare [na platformie M365] odnotowaliśmy 50-procentową redukcję liczby złośliwych lub podejrzanych wiadomości e-mail, które codziennie otrzymują nasi użytkownicy. To uwalnia nam wiele godzin, które możemy przeznaczyć na realizację innych celów”.

Werner Enterprises
(firma z listy Fortune 1000)

Bezpieczeństwo poczty e-mail: ukierunkowana ochrona antyphishingowa i BEC

Dostawca poczty e-mail: podstawowe funkcje poczty e-mail i danych



Możliwość przeznaczenia czasu na inne cele dzięki zwiększonej automatyzacji

Zautomatyzowane, lekkie rozwiązanie Cloudflare oferuje płynną integrację z przepływami pracy Microsoft i Google, zapewniając jednocześnie intuicyjny interfejs użytkownika na potrzeby działań analitycznych.

Skuteczność wykrywania na poziomie 99,997%

Połączenie natywnych możliwości dostawcy poczty e-mail z ochroną antyphishingową i BEC Cloudflare zapewnia firmom kompleksową ochronę przy minimalnym poziomie ryzyka.

Osiąganie większych korzyści przy niższych kosztach

Zastąpienie przestarzałych, kosztownych i złożonych wdrożeń nieobciążającym rozwiązaniem Cloudflare może zmniejszyć koszty operacyjne, zbędne funkcje i nadmiarowe procesy dostosowawcze.

Powstrzymywanie zaawansowanych ataków BEC

50 miliardów USD zgłoszonych strat z tendencją wzrostową

Biorąc pod uwagę, że ataki BEC są odpowiedzialne za oszałamiającą kwotę strat w ciągu ostatniej dekady, zaskakujące jest, że niektóre organizacje nadal nie traktują priorytetowo tak skutecznej formy oszustwa finansowego. Chociaż ataki BEC stanowią znacznie mniejszy odsetek zagrożeń phishingowych, często pozostają niewykryte przez SEG i dostawców poczty e-mail w chmurze, powodując większe straty finansowe. Tego rodzaju ukierunkowane ataki są trudne do wykrycia, ponieważ wykorzystują podszyte lub przejęte konta i kontekst konwersacji do maskowania się jako pracownik lub zaufany dostawca.

Rozszerzenie zasad Zero Trust na pocztę e-mail

Wykorzystując przejęte konto e-mail pracownika lub dostawcy, atakujący mogą ominąć tradycyjne mechanizmy kontroli bezpieczeństwa, które próbują jedynie potwierdzić legalność konta nadawcy. Rozwiązanie Cloudflare idzie o krok dalej, analizując szeroki wachlarz atrybutów behawioralnych, wzorców pisania, wskaźników opinii i historii konwersacji w celu określenia autentyczności nadawcy. Modele zagrożeń Cloudflare oparte na uczeniu maszynowym i rozbudowany system analizy informacji nt. sieci zapewniają najskuteczniejszą broń przeciwko zainfekowanym kontom, które są wykorzystywane do wyłudzania fałszywych płatności.

Rysunek 1. Analiza wiadomości

Wykrywanie ataków BEC za pomocą analizy kontekstowej opartej na uczeniu maszynowym

Dokładna identyfikacja ataków BEC wymaga czegoś więcej niż tylko strukturalnej analizy wiadomości. Skuteczne wykrywanie obejmuje również szczegółowe zrozumienie różnic w stylu i intencjach konwersacji. Rozbudowana telemetria sieciowa Cloudflare (ponad 3 bln żądań DNS dziennie) oraz rozwijające się modele uczenia maszynowego napędzają silnik analizy małych wzorców, który poddaje dekonstrukcji każdy aspekt wiadomości e-mail, aby ocenić wzorce pisania, sentyment, kontekst historyczny oraz szeroki zakres innych zmiennych pomagających zweryfikować autentyczność nadawcy.

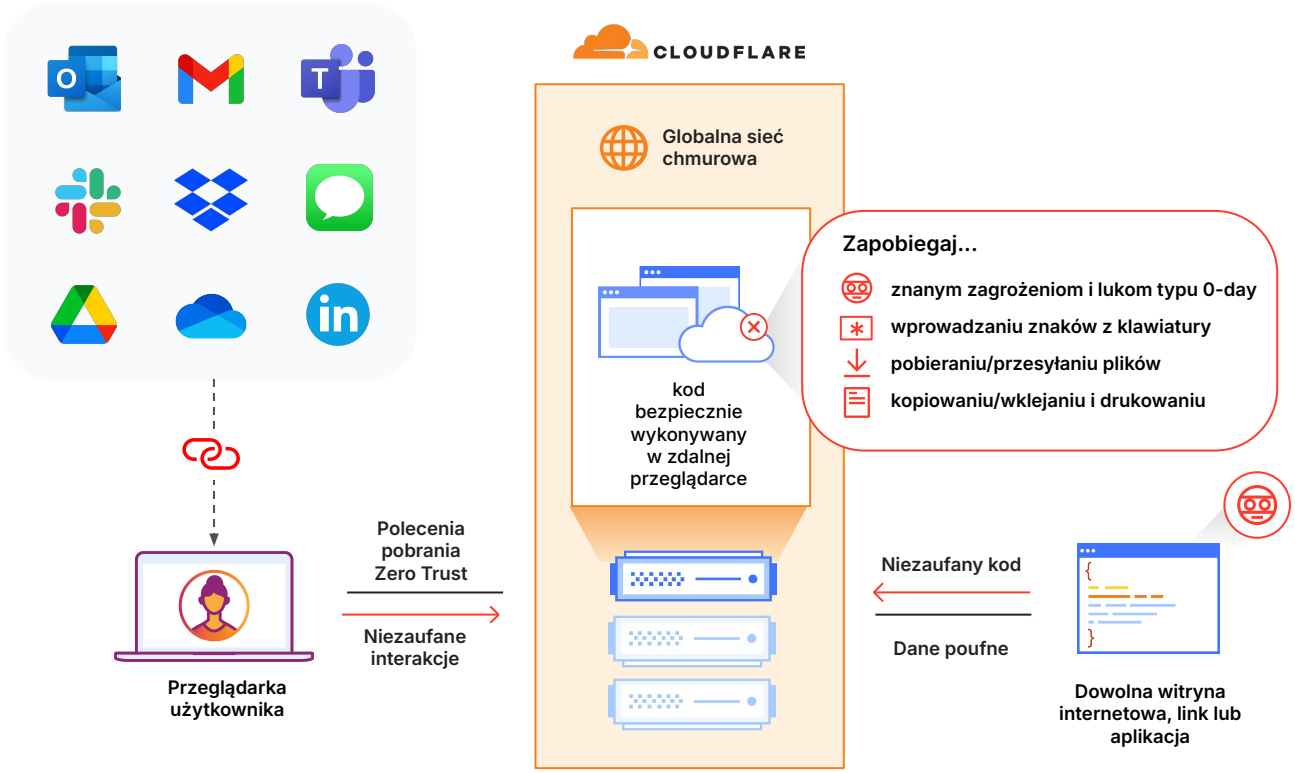
Izoluj ataki oparte na linkach

Ataki oparte na linkach stały się sprawdzoną metodą kradzieży poświadczeń, ładowania złośliwego oprogramowania / oprogramowania typu ransomware oraz wykradania danych wrażliwych. Wykorzystanie kombinacji wiadomości e-mail, czatu, SMS-ów, mediów społecznościowych i innych aplikacji do dostarczania tych linków dodatkowo komplikuje proces zapewnienia ochrony zarówno pracownikom, jak i danym przed ukierunkowanymi atakami phishingowymi.

Cloudflare rozwiązuje problem ataków phishingowych opartych na linkach poprzez zdalne renderowanie całego kodu internetowego w naszej globalnej sieci chmurowej zamiast na urządzeniu lokalnym użytkownika. To minimalizuje ryzyko związane ze złośliwym oprogramowaniem i atakami typu zero-day na przeglądarki, a jednocześnie zapewnia szczegółową kontrolę nad działaniami użytkownika (np. uniemożliwienie wprowadzania danych z klawiatury), aby zapobiec wyłudzaniu poświadczeń i wyciekom danych.

Eliminuj ryzyko phishingu bez spowalniania pracy zespołu

Dzięki integracji zaawansowanych funkcji izolacji przeglądarki nowej generacji, opartych na naszej unikalnej technologii Network Vector Rendering (NVR), Cloudflare jest w stanie dostarczyć bezproblemowe, bezpieczne i skalowalne rozwiązanie do izolowania potencjalnie złośliwych linków. W przeciwieństwie do technik obciążających przepustowość, NVR przesyła na urządzenie bezpieczne polecenia pobrania. Pomaga to wyeliminować ryzyko związane ze złośliwymi treściami internetowymi bez wpływu na doświadczenie użytkownika końcowego. Dzięki NVR i sieci Cloudflare o małych opóźnieniach organizacje mogą izolować zagrożenia wielokanałowe, zapewniając jednocześnie niezakłóconą produktywność swoich pracowników.



Szybkie sprawdzanie i reagowanie

Intuicyjne, niewymagające dużego zaangażowania zarządzanie bezpieczeństwem

Dzięki większej automatyzacji i minimalnej konfiguracji potrzebnej do uzyskania optymalnych wyników, rozwiązanie Cloudflare znacznie skraca czas i wysiłek wymagany do bieżącego zarządzania bezpieczeństwem poczty e-mail. Zespoły ds. bezpieczeństwa mogą natychmiast uzyskać pełny wgląd we wszystkie najważniejsze wskaźniki i trendy na pulpicie nawigacyjnym, z możliwością kliknięcia bardziej szczegółowych informacji na temat oflagowanych wiadomości. Zagłębianie się w trendy umożliwia szybkie wykrywanie częstych typów ataków; ustalenie, które osoby z kadry kierowniczej są celami ataków; zapobieganie opóźnionym atakom i ochronę innych krytycznych punktów danych.

Wszystkie analizy, dane telemetryczne, obserwacje zagrożeń i wskaźniki naruszeń bezpieczeństwa (IOC) są dostępne za pośrednictwem rozbudowanego interfejsu API w celu łatwej integracji z istniejącymi przepływami pracy analityków i narzędziami do orkiestracji.

„Często opowiadam współpracownikom o tym, że rozwiązanie Cloudflare jest proste i łatwe w obsłudze jako rozwiązanie SaaS oparte na chmurze i że bardzo jestem zadowolony z jego wysokiego poziomu dokładności”.

Japan Airlines

Zarządzane wykrywanie i reagowanie (PhishGuard)

Zarządzana usługa bezpieczeństwa poczty e-mail Cloudflare, PhishGuard, uzupełnia istniejący zespół SOC, dzięki czemu zwalnia cykle sprawdzania zabezpieczeń i zapewnia cenne informacje o zagrożeniach. Usługa PhishGuard może pomóc zneutralizować kampanie phishingowe, pomagając w sprawdzaniu, ocenie zagrożeń wewnętrznych, aktywnym eliminowaniu oszustw i spełnianiu złożonych wymagań dotyczących procesów naprawczych. Usługa PhishGuard rozszerza zasoby bezpieczeństwa i wiedzę specjalistyczną, aby aktywnie powiadamiać o potencjalnych oszustwach i zagrożeniach wewnętrznych, wyszukując jednocześnie zagrożenia oparte na wiadomościach e-mail.

Funkcje i zalety usługi PhishGuard:

- Zarządzanie zgłoszeniami phishingu i reagowanie na incydenty w celu szybszego ich rozwiązywania
- Proaktywne powiadomienia o atakach BEC i oszustwach, dzięki którym organizacje mogą szybko reagować na wczesnym etapie cyklu życia ataku
- Dedykowane zasoby do monitorowania w czasie rzeczywistym, okresowych przeglądów kont i bieżącej oceny zagrożeń
- Niestandardowe sygnatury blokujące oparte na analizie zagrożeń w środowisku zarządzanym

Ponad 1100

zaoszczędzonych godzin rocznie dzięki automatyzacji weryfikacji ręcznej

Zautomatyzowane rozwiązanie Cloudflare eliminuje ręczne, czasochłonne zadania, aby poprawić czas reakcji i odblokować dodatkowe cykle.

50%

mniej dostarczanych złośliwych lub podejrzanych wiadomości e-mail (na platformie M365)

Nałożenie warstwy Cloudflare na Microsoft 365 umożliwia organizacjom przechwytywanie ukierunkowanych ataków i zmniejszenie ogólnej liczby złośliwych wiadomości e-mail.

40

godzin spędzonych w ciągu siedmiu lat na konfigurowaniu zabezpieczeń poczty e-mail

Nieobciążające zabezpieczenia poczty e-mail Cloudflare wymagają niewielkiej wstępnej konfiguracji i minimalnego dostosowywania, zapewniając wysoką skuteczność wykrywania natychmiast po wdrożeniu.

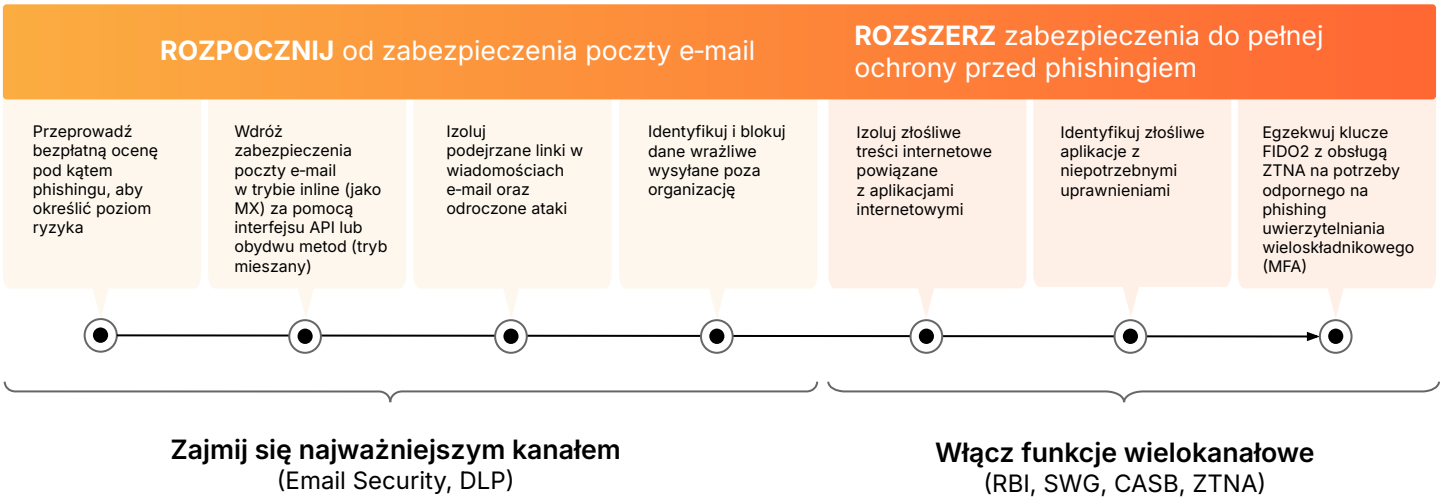
KORZYŚCI

Pełna ochrona wielokanałowa

W miarę jak kampanie phishingowe szybko wykraczają poza pocztę e-mail, dla organizacji staje się teraz pilniejsze niż kiedykolwiek wdrożenie rozwiązania phishingowego, które zapewni szybki i prosty sposób na osiągnięcie pełnej ochrony wielokanałowej.

Dzięki ujednoliconej platformie bezpieczeństwa Cloudflare organizacje mogą najpierw wdrożyć wiodące w branży zabezpieczenia poczty e-mail, aby szybko zneutralizować najważniejszy kanał ataków phishingowych, a następnie w prosty sposób włączyć usługi Zero Trust w celu rozszerzenia ochrony na wszystkie kanały, skutecznie powstrzymując zarówno znane, jak i nowe zagrożenia phishingowe.

- **Ochrona niewymagająca dużego zaangażowania, o wysokiej skuteczności:** Zminimalizuj ryzyko phishingu dzięki wiodącej w branży skuteczności wykrywania, która wymaga minimalnej konfiguracji.
- **Większa konsolidacja, niższy koszt:** Zmniejsz wydatki dzięki jednej, w pełni zintegrowanej platformie, która rozwiązuje wszystkie przypadki użycia dotyczące phishingu.
- **Szybkie wdrożenie, łatwe zarządzanie:** Zapewnij natychmiastową ochronę, jednocześnie ograniczając czas i wysiłek potrzebny do bieżącego zarządzania.



Ocena i porównanie

Oceń swoje obecne zabezpieczenia poczty e-mail i sprawdź, które zagrożenia pozostają niezauważone

Przeprowadź bezpłatne skanowanie wsteczne w ciągu kilku minut, aby sprawdzić, które zagrożenia phishingowe przedostały się przez filtry w ciągu ostatnich 14 dni, lub poproś o ocenę ryzyka phishingu (PRA), aby monitorować skrzynki odbiorcze pod kątem phishingu w momencie dostarczenia wiadomości. Dokonaj oceny w porównaniu z innymi dostawcami, bez potrzeby jakiejkolwiek konfiguracji, aby sprawdzić, które rozwiązanie do zabezpieczenia poczty e-mail oferuje najszybszą i najłatwiejszą ochronę.

Uruchom skanowanie wsteczne | Poproś o ocenę PRA

1. Badanie Deloitte z 2020 r.: źródło
2. Badanie FBI IC3 PSA z 2023 r.: źródło
3. Badanie Forrester Opportunity Snapshot z 2023 r.: źródło

