



KRÓTKI PRZEWODNIK · RYZYKO · OSZUSTWA TOŻSAMOŚCI

Nowy klient, fałszywa tożsamość? Sygnały sprawdzone, zanim dojdzie do zobowiązania.

Każdy, kto zakłada konto lub składa wniosek o umowę, zaczyna od podania, kim jest. Ten krótki przewodnik pokazuje, jak PaperOffice dostarcza adres e-mail, adres IP, urządzenie i dokument tożsamości jako sygnały, które można sprawdzić. Dla sklepów, platform, wynajmujących i sprzedawców na raty.

NAJWAŻNIEJSZE

Każda kontrola zwraca pola, na których może działać reguła: zalecenie dla e-maila, flagi VPN i Tor, identyfikator urządzenia oraz pola dokumentu tożsamości z miejscem źródłowym. Decyzję podejmuje zespół.

01 · NA CZYM POLEGA PROBLEM

Nazwisko się zgadza. Ale osoba za nim nie.

Nowy klient podpisuje umowę online, a smartfon trafia do niego na raty. Imię, nazwisko, adres i e-mail wyglądają wiarygodnie. Dopiero gdy płatności się urywają, wychodzi na jaw: dane należą do kogoś innego albo osoba w ogóle nie istnieje.

DLACZEGO TAK SIĘ DZIEJE

Skradzione i zmyślone dane

Oszuści używają prawdziwych nazwisk i adresów z wycieków danych albo mieszają je ze zmyślonymi szczegółami. Na formularzu oba wyglądają tak samo.

Ukrywanie w sieci

Jednorazowe adresy, VPN, Tor i wynajęte serwery ukrywają, kto składa zamówienie. Ta sama osoba może otworzyć wiele kont przy niewielkim wysiłku.

Dowody w pośpiechu

Przy ładzie kopia dowodu zostaje pobieżnie obejrzana i przepisana. Literówka lub brakujące pole łatwo mogą umknąć.

JAK TO ROZPOZNAĆ

- Adres e-mail pochodzi z jednorazowego serwisu albo jego domena nie ma serwera pocztowego.
- Rejestracja przychodzi przez VPN, Tor lub centrum danych, a nie przez zwykłe połączenie.
- Kraj adresu IP nie zgadza się z podanym adresem.
- To samo urządzenie pojawia się przy kilku rejestracjach pod różnymi nazwiskami.
- Dane na formularzu i w dokumencie tożsamości różnią się.

02 · ROZWIĄZANIE Z PAPEROFFICE

Od sygnału do decyzji.

PaperOffice dostarcza sygnały o e-mailu, sieci, urządzeniu i dokumencie przez REST API, SDK i w aplikacji. Dalszy krok zależy od reguły: przepuścić, zapytać ponownie, skierować do przeglądu lub odrzucić.

1

Oceń adres e-mail

POST /fakeemail/check sprawdza jednorazowe domeny, rekordy MX, SPF i DMARC i zwraca risk_score oraz zalecenie ACCEPT, REVIEW lub REJECT.

MODUŁ: WYKRYWANIE FAŁSZYWYCH ADRESÓW E-MAIL

2

Sprawdź sieć i lokalizację

/ip2location/full zwraca kraj, region i dostawcę oraz is_vpn, is_proxy, is_tor i is_datacenter. Pole type nazywa listę, na której trafiono.

MODUŁ: WYKRYWANIE VPN

3

Rozpoznaj urządzenie

SDK przeglądarki zwraca visitor_id dla każdego urządzenia. Przy kolejnym logowaniu /fingerprint/verify sprawdza, czy to to samo urządzenie, a risk.factors wymienia wszystko, co nietypowe.

MODUŁ: ODCISK URZĄDZENIA

4

Odczytaj dokument tożsamości

IDP Agent odczytuje imię i nazwisko, datę urodzenia, adres, numer dokumentu i datę ważności ze zdjęcia lub skanu, każdą wartość z jej miejscem w oryginale.

MODUŁ: IDP AGENT

5

Decyzja

Aplikacja łączy pola w regułę, np.: jednorazowy adres lub Tor oznacza przegląd przez człowieka. Decyzję podejmuje zespół.

03 · W APLIKACJI

Klucze, SDK, agent: jak to skonfigurować.

Kontrole sygnałów działają przez REST API i SDK, dokument tożsamości przez IDP Agent w aplikacji. Nazwy zgadzają się z aplikacją.

1

Klucz API dla backendu

W **API i deweloper** > **Klucze API** użyj **Utwórz nowy klucz**, aby utworzyć **Klucz API**. Backend używa go do sprawdzania e-maila i IP. Klucz można w każdej chwili skopiować.

2

Klucz dla SDK przeglądarki

W **API i deweloper** > **Klucze API** użyj **Utwórz nowy klucz**, wybierz typ **Klucz do publikacji** i wpisz domeny strony. Strona ładuje następnie SDK do rozpoznawania urządzeń z tym kluczem.

3

Utwórz IDP Agent dla dowodów

Wybierz przykładowe zdjęcie, a następnie **Akcje** > **Agenci i przepływy pracy** > **IDP** i **Utwórz nowego agenta**. Wybierz szablon dla dokumentów tożsamości lub opisz pola własnymi słowami.

4

Sprawdź wartości z źródłem

W zakładce **Pola danych** każda wartość jest obok fragmentu z dokumentu tożsamości. Widok **IDP Review** pokazuje wszystkie dokumenty z otwartymi polami.

5

Przerób zadania przeglądu

Gdy brakuje wymaganego pola, zadanie tworzy się w wybranej kolejce przeglądu. W **Workflow AI** > **Zadania Human In The Loop** osoba widzi dokument i pola i kończy przegląd.

PORADA Z PRAKTYKI

Oceniaj kilka sygnałów razem VPN sam w sobie często ma niegroźne powody. Nabiera znaczenia razem z jednorazowym adresem albo z urządzeniem, które jest już powiązane z innymi kontami w systemie. Określ, kiedy przegląd wykonuje osoba.

04 · PRZYKŁAD

Sprzedawca telefonów, umowy na raty.



Sprzedawca telefonów komórkowych z sześcioma sklepami i sklepem internetowym sprzedaje smartfony z umowami i ratami. W sklepie zespół przepisuje dowód pole po polu, a online wystarcza formularz. Raz po raz płatności się urywają, a klientów nie da się dotrzeć.

PRZED

- W sklepie kopiuje się dowód i przepisuje go pole po polu do formularza umowy.
- Online przyjmuje się każdy adres e-mail, także jednorazowe.
- Wnioski przez VPN lub centra danych wyglądają jak wszystkie inne.
- Nikt nie zauważa, że jedno urządzenie złożyło już kilka wniosków.

Z PAPEROFFICE

- Formularz online sprawdza adres e-mail, a przy REVIEW wnioski trafiają do przeglądu.
- Kontrola IP zgłasza VPN, Tor i centrum danych, a wniosek porównuje kraj z adresem.
- Każdy wniosek zapisuje visitor_id, więc urządzenia użyte wielokrotnie się wyróżniają.
- W sklepie IDP Agent odczytuje dowód ze zdjęcia, a zespół sprawdza wartości z ich źródłem.

Przykład ilustracyjny, firma i proces są zmyślone. Warto sprawdzić z inspektorem ochrony danych, jakie dane o dowodach i urządzeniach są zbierane i jak długo są przechowywane.

05 · LISTA KONTROLNA

Dziesięć punktów dla przyjmowania klientów.

Te punkty warto przejść ze sprzedażą, IT i ochroną danych. Każdy z nich można sprawdzić we własnej firmie.

- | | |
|---|--|
| ☐ Każda rejestracja sprawdza adres e-mail, zanim konto zostanie aktywowane. | ☐ Dla REVIEW i REJECT ustalono, co się dzieje: zapytanie ponowne, przegląd lub odrzucenie. |
| ☐ Backend wysyła adres IP klienta do API w parametrze ip. | ☐ VPN, Tor i centrum danych są oceniane osobno, z regułą dla każdego przypadku. |
| ☐ Kraj adresu IP jest porównywany z podanym adresem. | ☐ visitor_id jest zapisywany przy każdym koncie i każdym wniosku. |
| ☐ Gdy znane konto loguje się z nieznanego urządzenia, aplikacja prosi o drugi składnik uwierzytelnienia. | ☐ IDP Agent odczytuje dokumenty tożsamości, a wymagane pola są określone. |
| ☐ Dla żądań usunięcia udokumentowano ścieżkę przez POST /privacy/forget. | ☐ Cel, podstawa prawna i okres przechowywania danych o urządzeniach są uzgodnione z ochroną danych. |

06 · NAJCZĘŚCIEJ ZADAWANE PYTANIA

O co zespoły pytają przed startem.

Czy PaperOffice sprawdza dowody biometrycznie?

PaperOffice działa bez porównywania twarzy. IDP Agent odczytuje pola dokumentu tożsamości wraz z miejscem źródłowym, a pozostałe kontrole dostarczają sygnałów o e-mailu, sieci i urządzeniu. Czy tożsamość zostaje potwierdzona, decyduje zespół.

A osoby, które używają VPN z dobrych powodów?

VPN to sygnał, który reguła waży. Odpowiedź rozdziela VPN, proxy, Tor i centrum danych, a nazwę pasującej listy podaje w polu type. Adresy z list blokad pojawiają się także w is_vpn.

Jak kontrole trafiają do naszego portalu?

Przez REST API z backendu, przez SDK odcisku z **Klucz do publikacji** powiązany z domenami oraz przez MCP. Dokumenty tożsamości wgrywa się do Workspace, w którym działa IDP Agent.

Skąd bierze się wskaźnik ryzyka?

Z kontroli e-maila: risk_score od 0 do 100, risk_level od MINIMAL do CRITICAL oraz zalecenie ACCEPT, REVIEW lub REJECT. Kontrola urządzenia zwraca własne czynniki ryzyka, np. VPN lub niemożliwie szybką zmianę lokalizacji.

Czy można wykryć to samo urządzenie za kilkoma kontami?

Tak, jeśli visitor_id zapisuje się przy każdym koncie. Wtedy ten sam identyfikator pojawia się na kilku kontach. /fingerprint/similar znajduje urządzenia o podobnych cechach, /fingerprint/linked urządzenia z tej samej sieci.

Jak obsługiwać żądania usunięcia?

POST /privacy/forget usuwa profil urządzenia, powiązania, historię i alerty dla identyfikatora w organizacji. Znacznik blokady zapobiega ponownemu zapisaniu tego samego identyfikatora.

07 · JAK ZACZĄĆ

Sprawdź kolejną rejestrację na prawdziwych sygnałach.

Założ konto na app.paperoffice.ai, wygeneruj klucz API w [API i deweloper > Klucze API](#) i sprawdź pierwszy adres przez POST [/fakeemail/check](#). Rozliczenie: płatność za zużycie, szczegóły są na stronie cennika.

Dodaj sprawdzenie e-maila

Formularz rejestracji przesyła adres przez backend do [/fakeemail/check](#) i działa według pola recommendation.

Dodaj IP i urządzenie

[/ip2location/full](#) dla sieci i lokalizacji, SDK odcisku dla visitor_id. Zapisz oba razem z wnioskiem.

Odczytuj dokumenty

Utwórz IDP Agent z szablonem dokumentu tożsamości i pozwól mu działać automatycznie po przetworzeniu w Workspace dla wniosków.

KARTY TECHNICZNE NA TEN TEMAT

Wykrywanie fałszywych adresów e-mailpaperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf**Wykrywanie VPN**paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf**API lokalizacji IP**paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf**Odcisk urządzenia**paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf**IDP Agent**paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-pl.pdf

WIĘCEJ NA TEN TEMAT

Oszustwa tożsamościpaperoffice.ai/pl/solutions/ryzyko/ai-oszustwo-tozsamosci-wykrywanie-zapobieganie

WIĘCEJ NA TEN TEMAT

paperoffice.ai/pl/solutions/ryzyko/ai-oszustwo-tozsamosci-wykrywanie-zapobieganie

CENNIK

paperoffice.ai/en/pricing

KONTAKT

paperoffice.ai/pl/kontakt