TD SYNNEX

Wykrywanie oszustw

Destination AI: Przypadek użycia

Wprowadzenie

Fraud Detection wykorzystuje zaawansowaną sztuczną inteligencję i techniki uczenia maszynowego do proaktywnego identyfikowania, badania i ograniczania nieuczciwych działań w branżach takich jak usługi finansowe, ubezpieczenia, handel detaliczny i handel elektroniczny. Analizując dane transakcyjne, zachowanie użytkowników i historyczne wzorce oszustw, systemy sztucznej inteligencji mogą wykrywać anomalie w czasie rzeczywistym i oznaczać podejrzane działania do dalszej analizy. Takie podejście nie tylko przyspiesza proces wykrywania, ale także zmniejsza zależność od tradycyjnych systemów opartych na regułach, które mają trudności z dostosowaniem się do ewoluujących taktyk oszustw. Organizacje korzystają z dynamicznego, opartego na danych systemu, który stale uczy się na podstawie nowych danych, zapewniając, że możliwości wykrywania oszustw pozostają odporne na pojawiające się zagrożenia. Wiodący dostawcy oferują wyspecjalizowane rozwiązania wspierające te inicjatywy. Na przykład IBM integruje obliczenia kognitywne z analizą oszustw; AWS zapewnia skalowalne usługi wykrywania oszustw w czasie rzeczywistym; Microsoft Azure oferuje zaawansowaną analizę bezpieczeństwa; Google Vertex AI wykorzystuje uczenie maszynowe na dużą skalę do wykrywania anomalii; a HPE Private Cloud AI zapewnia bezpieczne, zgodne z przepisami rozwiązania lokalne lub hybrydowe. Łącznie oferty te umożliwiają organizacjom ochronę zasobów, utrzymanie zaufania klientów i zapewnienie zgodności z przepisami w coraz bardziej złożonym środowisku cyfrowym.

Punkty bólu

Tradycyjne metody wykrywania oszustw często opierają się na statycznych regułach i ręcznych przeglądach, które mogą być powolne i nieefektywne. Organizacje stoją przed poważnymi wyzwaniami związanymi z przeszukiwaniem ogromnych ilości danych transakcyjnych w celu zidentyfikowania subtelnych anomalii wskazujących na nieuczciwe zachowanie. Te starsze systemy mają trudności z dostosowaniem się do szybko ewoluujących taktyk oszustw, co skutkuje opóźnionymi reakcjami i wyższymi stratami finansowymi. Ponadto wysoki wskaźnik fałszywych alarmów może przytłoczyć zespoły ds. bezpieczeństwa, odciągając zasoby od prawdziwych zagrożeń i powodując niedogodności dla legalnych klientów. Silosy danych i rozproszone systemy dodatkowo utrudniają budowanie kompleksowego obrazu potencjalnych nadużyć, komplikując szybkie wykrywanie i interwencję. Kwestie te łącznie zwiększają ryzyko, koszty operacyjne i podważają zaufanie klientów.

Korzyści z rozwiązania

Integracja rozwiązań do wykrywania oszustw opartych na sztucznej inteligencji oferuje transformacyjne korzyści poprzez automatyzację identyfikacji podejrzanych działań i umożliwienie interwencji w czasie rzeczywistym. Zaawansowane algorytmy uczenia

maszynowego analizują ogromne ilości danych transakcyjnych i behawioralnych w celu zidentyfikowania wzorców, które mogą wskazywać na oszustwo, znacznie skracając czas wykrywania i minimalizując straty finansowe. Ciągłe uczenie się na podstawie nowych danych poprawia dokładność w czasie, obniżając w ten sposób wskaźnik fałszywych alarmów i umożliwiając zespołom ds. bezpieczeństwa skupienie się na zagrożeniach o wysokim priorytecie. Ulepszona integracja danych zapewnia całościowy wgląd w transakcje, ułatwiając dokładniejszą ocenę ryzyka. Co więcej, zautomatyzowane systemy mogą działać na dużą skalę, zapewniając bezpieczeństwo nawet w środowiskach o największym natężeniu ruchu. Korzyści te przekładają się na lepszą wydajność operacyjną, zmniejszoną ekspozycję na ryzyko, zwiększoną zgodność z przepisami i większe zaufanie klientów do zdolności organizacji do ochrony poufnych informacji.

Wpływ na KPI

Kluczowe wskaźniki wydajności, na które pozytywny wpływ może mieć wykrywanie oszustw oparte na sztucznej inteligencji, obejmują:

- Współczynnik oszustw: Mierzalne zmniejszenie liczby udanych transakcji oszukańczych.
- Czas reakcji: Szybsze wykrywanie i rozwiązywanie potencjalnych przypadków oszustw.
- Współczynnik fałszywych alarmów: Zwiększona dokładność, redukcja niepotrzebnych alertów i ręcznych przeglądów.
- Straty finansowe: Niższe straty finansowe dzięki szybkiej interwencji i zapobieganiu.
- Zaufanie klientów: Zwiększona satysfakcja i zaufanie wynikające z solidnych środków bezpieczeństwa.

Wdrożenie przypadku użycia

Wdrożenie wykrywania oszustw opartego na sztucznej inteligencji wymaga kompleksowego, wieloetapowego podejścia, które integruje innowacje techniczne ze strategią operacyjną.

Planowanie i dostosowanie do interesariuszy

Zdefiniowanie celów: Ustal jasne cele, takie jak zmniejszenie liczby incydentów związanych z oszustwami, zminimalizowanie czasu reakcji i obniżenie liczby fałszywych alarmów. Przyporządkuj te cele do mierzalnych wskaźników KPI.

Zebranie wielofunkcyjnego zespołu: Uwzględnij przedstawicieli IT, bezpieczeństwa, zarządzania ryzykiem, zgodności i operacji, aby upewnić się, że wszystkie wymagania zostały spełnione.

Ocena dostawców i narzędzi: Ocena dostępnych rozwiązań od dostawców takich jak IBM, AWS, Microsoft Azure, Google Vertex AI i HPE Private Cloud AI, zapewnienie zgodności z istniejącymi systemami i standardami regulacyjnymi.

Alokacja zasobów i infrastruktura

Integracja danych: Konsolidacja danych z systemów transakcyjnych, platform CRM i źródeł zewnętrznych w ujednoliconym, bezpiecznym repozytorium do kompleksowej analizy.

Planowanie budżetu: Przydziel zasoby na licencjonowanie oprogramowania AI, potencjalne aktualizacje sprzętu lub infrastruktury chmurowej oraz szkolenia personelu. Oceń zwrot z inwestycji, porównując przewidywane zmniejszenie strat związanych z oszustwami z kosztami wdrożenia.

Bezpieczeństwo i zgodność: Wdrożenie rygorystycznych zasad zarządzania danymi i zapewnienie zgodności rozwiązania z przepisami, takimi jak PCI-DSS, RODO i innymi standardami branżowymi.

Projekt pilotażowy i dowód koncepcji

Wybierz segment docelowy: Wybierz konkretną jednostkę biznesową lub typ transakcji o wysokim ryzyku oszustwa dla początkowego programu pilotażowego.

Konfiguracja narzędzi AI: Zintegruj wybrane rozwiązanie do wykrywania oszustw z istniejącymi systemami, konfigurując źródła danych w czasie rzeczywistym i mechanizmy ostrzegania.

Podstawowe wskaźniki: Dokumentowanie bieżących wskaźników oszustw, czasów reakcji i wskaźników fałszywie dodatnich, które posłużą jako punkty odniesienia do pomiaru sukcesu programu pilotażowego.

Wykonanie i przyjęcie

Wdrażanie i szkolenia: Przeprowadzaj kompleksowe sesje szkoleniowe dla zespołów ds. bezpieczeństwa i operacji, aby zapewnić efektywne wykorzystanie alertów generowanych przez sztuczną inteligencję i funkcji systemu.

Iteracyjne pętle sprzężenia zwrotnego: Ustanowienie regularnych sesji informacji zwrotnych w celu udoskonalenia algorytmów wykrywania i dostosowania progów w oparciu o rzeczywiste dane dotyczące wydajności.

Wdrożenie na pełną skalę: Stopniowe rozszerzanie wdrożenia na wszystkie odpowiednie jednostki biznesowe, zapewniając płynną integrację i minimalne zakłócenia w bieżących operacjach.

Monitorowanie i zarządzanie zmianami

Ciągłe monitorowanie: Wykorzystaj pulpity nawigacyjne w czasie rzeczywistym do śledzenia kluczowych wskaźników KPI i wydajności systemu, szybko rozwiązując wszelkie pojawiające się problemy.

Zarządzanie ryzykiem: Opracowanie protokołów w celu ograniczenia ryzyka, takiego jak naruszenia danych lub nadmierne poleganie na automatycznych alertach, zapewniając w razie potrzeby stały nadzór człowieka.

Skalowanie i integracja: Zintegrowanie systemu wykrywania oszustw z szerszymi ramami bezpieczeństwa i zarządzania ryzykiem, zapewniając interoperacyjność z innymi systemami IT i zgodności.

Konserwacja i ciągłe doskonalenie

Aktualizacje modeli: Regularne ponowne trenowanie modeli AI przy użyciu nowych danych, aby dotrzymać kroku zmieniającym się wzorcom oszustw i utrzymać wysoką dokładność wykrywania.

Dokumentacja: Prowadzenie szczegółowej dokumentacji metodologii wykrywania, konfiguracji systemu i dostosowań procesów w celu wspierania ciągłego doskonalenia.

Zaangażowanie społeczności i ekosystemu: Współpracuj ze społecznościami dostawców, forami branżowymi i organami regulacyjnymi, aby być na bieżąco z pojawiającymi się trendami i najlepszymi praktykami w zakresie wykrywania oszustw.

Przegląd oferty dostawców

- IBM: Oferuje kompleksowe rozwiązania do wykrywania oszustw, które integrują obliczenia kognitywne z zaawansowaną analityką w celu niezawodnej identyfikacji zagrożeń.
- AWS: Zapewnia skalowalne usługi wykrywania oszustw w czasie rzeczywistym, wykorzystując moc infrastruktury chmury.
- Microsoft Azure: Zapewnia zaawansowaną analitykę bezpieczeństwa i wykrywanie anomalii za pomocą pakietu narzędzi bezpieczeństwa.
- Google Vertex AI: wykorzystuje uczenie maszynowe na dużą skalę do analizy obszernych zbiorów danych w celu wykrywania nieuczciwych wzorców.
- HPE Private Cloud AI: Obsługuje bezpieczne, lokalne lub hybrydowe rozwiązania dostosowane do organizacji o ścisłych wymaganiach w zakresie zgodności i suwerenności danych.

Podsumowanie

Wykrywanie oszustw oparte na sztucznej inteligencji stanowi krytyczny postęp w ochronie organizacji przed stratami finansowymi, karami regulacyjnymi i utratą reputacji. Wykorzystując zaawansowane algorytmy uczenia maszynowego i analizę danych w czasie rzeczywistym, organizacje mogą szybko identyfikować i ograniczać nieuczciwe działania, znacznie zwiększając ogólne bezpieczeństwo. Ustrukturyzowany proces wdrażania - obejmujący jasne określenie celów, solidną integrację danych, testy pilotażowe i ciągłe monitorowanie - zapewnia, że rozwiązanie zapewnia wymierną poprawę w zapobieganiu oszustwom. Wykorzystanie ofert dostawców od liderów branży zapewnia skalowalną, bezpieczną i zgodną z przepisami strukturę, która jest niezbędna w dzisiejszym dynamicznym środowisku zagrożeń. Wdrożenie tych technologii nie tylko zabezpiecza zasoby, ale także wzmacnia zaufanie klientów i zapewnia organizacji trwały sukces.