

## System zur Betrugserkennung

Das ML FDS-System enthält ein Modul für maschinelles Lernen, das die zweite Verteidigungsline bildet und neue Betrugsarten direkt aus den verfügbaren Daten identifiziert. Dank dieses datenbasierten Ansatzes lernt das System ständig dazu und passt sich an die sich entwickelnde Betrugsssozialisierung an.

## Adressierbare Geschäftsanforderungen

Betrug und Fehlverhalten sind eine tägliche Herausforderung, mit der jedes Unternehmen heutzutage konfrontiert ist, sei es bei Finanztransaktionen, Versicherungen oder in anderen Bereichen. Die Erkennung von betrügerischem Verhalten basiert hauptsächlich auf vordefinierten Kriterien. Diese Herangehensweise leidet jedoch unter hohen Falsch-Positiv-Raten und, was noch wichtiger ist, sie ist nicht resistent gegen komplexe Betrugsmuster.

Das ML FDS-System identifiziert neue Betrugsarten direkt aus den Daten, wodurch es in der Lage ist, komplizierte Betrugsmuster zu erkennen und sie in Zukunft zu verhindern. Dank des datengesteuerten Ansatzes lernt das System ständig dazu und passt sich an die zunehmende Komplexität des Betrugs an.

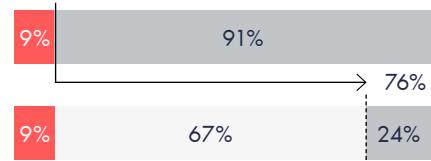
### VERTEILUNG DER VERHINDERNDEN BETRUGSVERLUSTE NACH QUELLE DER ERKENNUNG



Aus früheren Einsätzen geht hervor, dass die Betrugserkennungsgenauigkeit um **bis zu 76 %** gestiegen und die Zahl der gemeldeten Fehlalarme um **bis zu 60 %** gesunken ist.

- Regel / Blacklist
- Andere
- Maschinelles Lernen

#### Aktuell



## Ausgewählte Anwendungsfälle



### Versicherung

- Fehler und nicht übereinstimmende Datensätze bei der Identifizierung historischer Transaktionen.
- Management versteckter Risiken.
  - Nur auf relevante Fälle konzentrieren.
  - Reduzieren Sie falsch-positive Fälle.



### Buchhaltung

- Verarbeitung von Buchhaltungsberichten.
- Verarbeitung von Anwesenheitsberichten und Leistungsdaten.
- Finden Sie nützliche Erkenntnisse für Wirtschaftsprüfer.
- Decken Sie unerwünschtes Verhalten auf.



### Telco / Bankwesen

- Aufdeckung von Betrug und Fehlverhalten.
- Management versteckter Risiken.
- Reduzierung von Abonnementbetrug.
- Verhinderung von betrügerischem Verhalten.

# Die wichtigsten Vorteile

-  **Reduzierung der Erkennungszeit von Tage auf Minuten oder Sekunden.**
-  **Bis zu 60 % weniger Fehlalarme.**
-  **Fähigkeit zu lernen und sich anzupassen, ohne dass eine manuelle Verwaltung erforderlich ist.**
-  **Bis zu 76 % Genauigkeit bei der Betrugserkennung.**

## Wie es funktioniert

1.

### Unternehmens- und externe Daten

Vielfältige Datenströme aus verschiedenen Systemen werden als Eingabequelle für KI-Algorithmen verwendet, um betrügerische Ereignisse zu erkennen. Das System passt sich auf der Grundlage der Daten an, um neue Betrugarten aufzudecken.

2.

### Regelbasiertes System

Vordefinierte Regeln und schwarze Listen, die normalerweise vorhanden sind. Sie reichen nur für bekannte Muster aus und behandeln alle Probleme auf dieselbe Weise.

3.

### Maschinelles Lernen

Das System arbeitet in Synergie mit einem regelbasierten System als zusätzliche Sicherheitsebene: Maschinelles Lernen betrachtet Daten aus verschiedenen Blickwinkeln, erkennt komplizierte Betrugsmuster und verhindert sie in Zukunft.

4.

### Visualisierung und Integration

Das System wird in eine bestehende Umgebung integriert. Alle aufgedeckten Betrugsfälle werden den Benutzern zur weiteren Analyse und für Rückmeldungen gemeldet.

## Fallstudie: BETRUG BEI VERSICHERUNGANSPRÜCHEN



### GESCHÄFTSZIEL

Obwohl Versicherer über Prozesse, Tools und engagierte Mitarbeiter zur Betrugserkennung verfügen, sahen sie die Notwendigkeit, innovativ zu sein und die Effizienz der Betrugserkennung zu erhöhen, die Zahl der Falschmeldungen zu verringern und sich vor sich entwickelnden Betrugsaktivitäten zu schützen.

### ACTION

Wir nutzen historische Schadendaten, indem wir unser Framework für maschinelles Lernen zur Betrugserkennung anwendeten. Als Ergebnis erkannten KI-Modelle komplexe Muster in Schadenfällen, Policien und anderen Daten und ermöglichen so eine zuverlässige Betrugserkennung und gleichzeitige Erstellung von Whitelists.

### ERGEBNISSE

Die Blindspot-Betrugsbekämpfungslösung, die auf historische Schadendaten angewendet wurde, automatisierte den Betrugserkennungsprozess und ermöglichte es den Analysten, sich auf relevante Fälle zu konzentrieren, wodurch die Zahl der Falschmeldungen um 60 % gesenkt werden konnte.

60 % SENKUNG DER ZAHL DER „FEHLALARME“: ERHÖHUNG DER EFFIZIENZ DES BETRIEBS UND VERBESSERUNG DER KUNDENERFAHRUNG

## KI-Services In Höchster Qualität Von Blindspot Solutions

Blindspot Solutions ist ein professionelles Team von KI-Experten für die End-zu-End Implementierung von KI-Systemen in internationalen Firmen sowie Startups. Blindspot ist Ihr Partner für die Installation und den Umgang mit KI in jedem Anwendungsspektrum.



### BETRIEBSBERATUNG FÜR KÜNSTLICHE INTELLIGENZ

Gegründet 2014 in Prag  
Tschechische Republik



### ENTWICKLUNG PERSONALISIERTER KI-ANWENDUNGEN

Mitglied der  
Adastralia



### MACHINE LEARNING/ DATA SCIENCE TEAM

Kontaktieren Sie uns:  
[contact@blindspot.ai](mailto:contact@blindspot.ai)

Karolinská 706/3  
186 00 Prag, CZ