

CASE STUDY

Kunde: Nr. 5 Online-Marktplatz

Lösung: Behavioral Biometrics

Mehr Sicherheit durch Behavioral Biometrics

Nr. 5 Online-Marktplatz kämpft erfolgreich gegen Account Takeover (ATO) durch Behavioral Biometrics an

→ Wie unser Kunde es geschafft hat, bis zu 2.000 ATO pro Tag zu vermeiden, seine Verluste aufgrund von Betrug um 1,2 Mio € zu verringern und seine Conversions trotz höchster Sicherheit zu steigern.

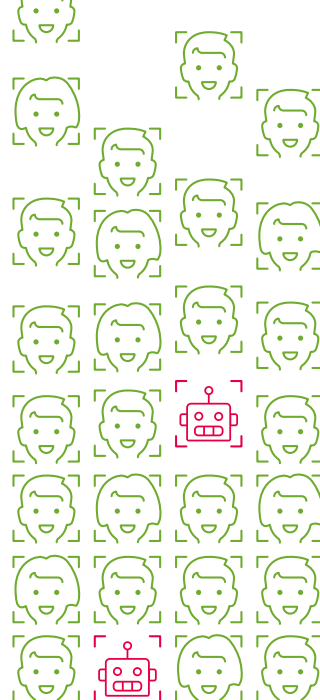


BETRÜGER ODER KUNDE?

01

Unser Kunde

Seit 2018 dürfen wir einen der Top-5-Online-Marktplätze zu unseren Kunden zählen. Das Unternehmen betreibt eine native iOS und Android App mit über 9 Mio. App-Downloads und eine webbasierte Plattform. Mit dem stetigen Wachstum des Unternehmens stiegen jedoch auch die Account-Takeover-Fälle exponentiell. Um den Reputationschaden und die Kosten aus Betrugsfällen einzudämmen, musste eine Lösung gefunden werden.



02

Die Ausgangssituation

Der Kunde hatte mit unzähligen Account Take Over (ATO) pro Tag zu kämpfen, die durch aufwändige, manuelle Prozesse überprüft werden mussten und stark vom Regelset abhängig waren. Das Standard-Vorgehen der Betrüger: sich Zugang zu den Accounts legitimer User verschaffen, Bestellungen aufgeben und an eine gewünschte Lieferadresse, meist Packstation, senden lassen. Die Folge: Eine überdurchschnittlich hohe Rate an Chargebacks, die den Handlungsbedarf des Online-Händlers verschärfte.

Kurz:

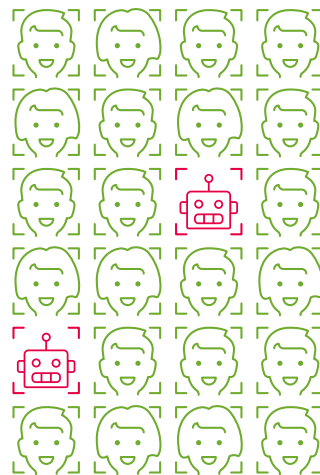
- ↳ Reputation
- ↳ Effektive Betriebsprozesse

- Rückbuchungen
- Manuelle Prüfungen
- Chargeback-Handling

03

Die Herausforderung

- **Sicherheit ohne Nebenwirkungen:** Hohe Sicherheitsstandards etablieren, ohne die Customer Journey und somit die Conversions zu beeinträchtigen.
- **Erkennen statt Kontrollieren:** Nutzer mit betrügerischen Absichten, Bots oder Emulatoren bereits beim Versuch eines Betrugs identifizieren, um Folgeschäden zu vermeiden.
- **Sicherheit ohne Performance-Verlust:** Implementieren einer skalierbaren Fraud-Lösung mit minimalen technischen Footprint, um die Site Performance hoch zu halten.



Jetzt Business Insight anfordern:
„Die Power von Behavioral Biometrics nutzen“

04

Unsere Lösung

Erkennung von Fraud, bevor er entsteht. Der Einsatz von Behavioral Biometrics hilft dabei, betrügerische Aktivitäten frühzeitig zu erkennen.

- Erkennung von legitimen Nutzern über verhaltensbiometrische Daten und Geräteanomalien mit Hilfe von Machine Learning.
- Bilden eines Trust-Scores in Echtzeit, um legitime von betrügerischen, nicht menschlichen Usern zu unterscheiden und Bestellungen zu stoppen.
- Unsichtbare, kontinuierliche Analyse der Nutzerdaten und Kontoaktivitäten innerhalb einer Website oder App.

05

Das Ergebnis

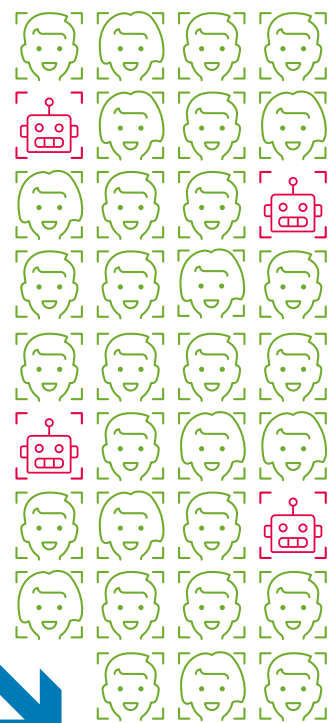
- Reduzierung der Verluste durch Betrug von über 1.200.000 €
- Vermeidung von über 2.000 ATO pro Tag
- Verbesserte Customer Experience der treuen Kunden durch weniger Sicherheitshürden
- Reduzierung interner Kosten durch die Automatisierung von manuellen Prüfprozessen
- Erfolgreiche Bewältigung der stetig steigenden Transaktionen

06

Statement des Head of Risk

Nr. 5 Online-Marktplatz

Die Lösung hat unsere ersten Anforderungen erfolgreich erfüllt und schon kurz nach der unkomplizierten Implementierung konnten wir einen deutlichen Rückgang der Betrugsrate, Rückbuchungen und Rückerstattungsanträge feststellen. Wir sind sehr froh, eine Lösung gefunden zu haben, die ATOs schon vor Transaktionen erkennt, ohne sich negativ auf die Customer Experience und somit auch unweigerlich auf die Conversion auszuwirken.



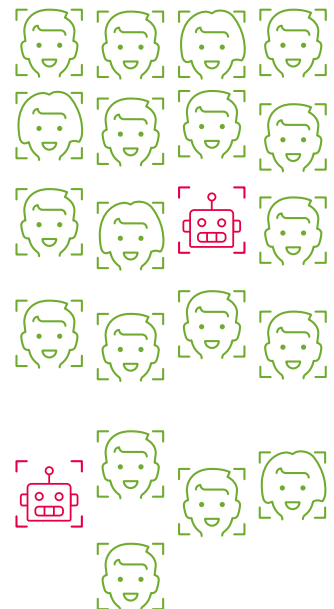
Reduzierung

- **Finanzielle Verluste**
- **Betrugsrate**
- **Interne Kosten**



Steigerung

- **Customer Experience**
- **Legitime Transaktionen**



Jetzt Business Insight anfordern:
„Die Power von Behavioral Biometrics nutzen“