Die Power von Behavioral Biometrics nutzen:

ein Game Changer bei der Betrugsprävention

arvato
BERTELSMANN
Financial Solutions

finance.arvato.com

Kundenbedürfnisse im Wandel: Vertrauen & Betrug im digitalen Zeitalter

Digital ist heute längst Normalität. Die Erwartungen der Kunden haben sich aufgrund der technologischen Entwicklungen verändert. Durch die „always-on"-Mentalität wird Komfort bei digitalen Transaktionen mehr denn je gefordert, was jedoch die Hürden für Betrug senkt. Kein Wunder also, dass Betrugsfälle zunehmen und immer ausgefeilter werden. Die negativen Auswirkungen auf das Verbrauchervertrauen und den Geschäftsumsatz sind erheblich.

Die häufigsten Online-Betrugsphänomene sind Bedrohungen wie Account Takeover, Konten- und Zahlungsbetrug sowie automatisierte Angriffe. Daraus entstehen große Herausforderungen und Risiken:

CUSTOMER FRICTION

Zusätzliche Authentifizierungs-methoden werden von Verbrauchern als störend wahrgenommen und somit schnell zur Conversion-Hürde.

OPERATIVE KOSTEN

Ineffiziente Untersuchungsprozesse und und manuelle Transaktions-prüfungen stellen einen erheblichen Mehraufwand dar.

FINANZIELLER VERLUST

Finanzielle Einbußen resultieren aus niedrigen Genehmigungsraten, Kaufabbrüchen, Betrugsfällen und False Positives.

REPUTATIONSSCHADEN

Kundenvertrauen und -loyalität können abnehmen, wenn man Opfer von Betrug wurde.

ONLINE-BETRUG VERHINDERN

Das Erkennen von Online-Betrug kann ein Balanceakt sein: Wie kann vertrauenswürdiges Verhalten von treuen oder potenziellen Kunden erkannt, während betrügerische Aktivitäten verhindert und gestoppt werden?

Mit Behavirol Biometrics Friction minimieren und Sicherheit maximieren

Intelligente Online-Authentifizierung:
Identifizieren Sie legitime Benutzer und bieten Sie ihnen eine reibungs- und mühelose Authentifizierungs- und Checkout-Erfahrung.

Betrugsprävention in Echtzeit:
Erhöhen Sie die Sicherheit, indem Sie Betrugsrisiken, Anomalien und verdächtige Aktivitätsmuster sofort erkennen und stoppen.

KOMFORTABLE TRANSAKTIONEN

DIE AUSWIRKUNGEN:

- ✓ Reibungslose Authentifizierung
- ✓ Verbesserte Customer Experience
- ✓ Bindung treuer Kunden

DIE ERGEBNISSE:

- ✓ Minimierung von False Positives
- ✓ Vermeidung von Transaktionsabbrüchen
- ✓ Erhöhte Conversion Rate

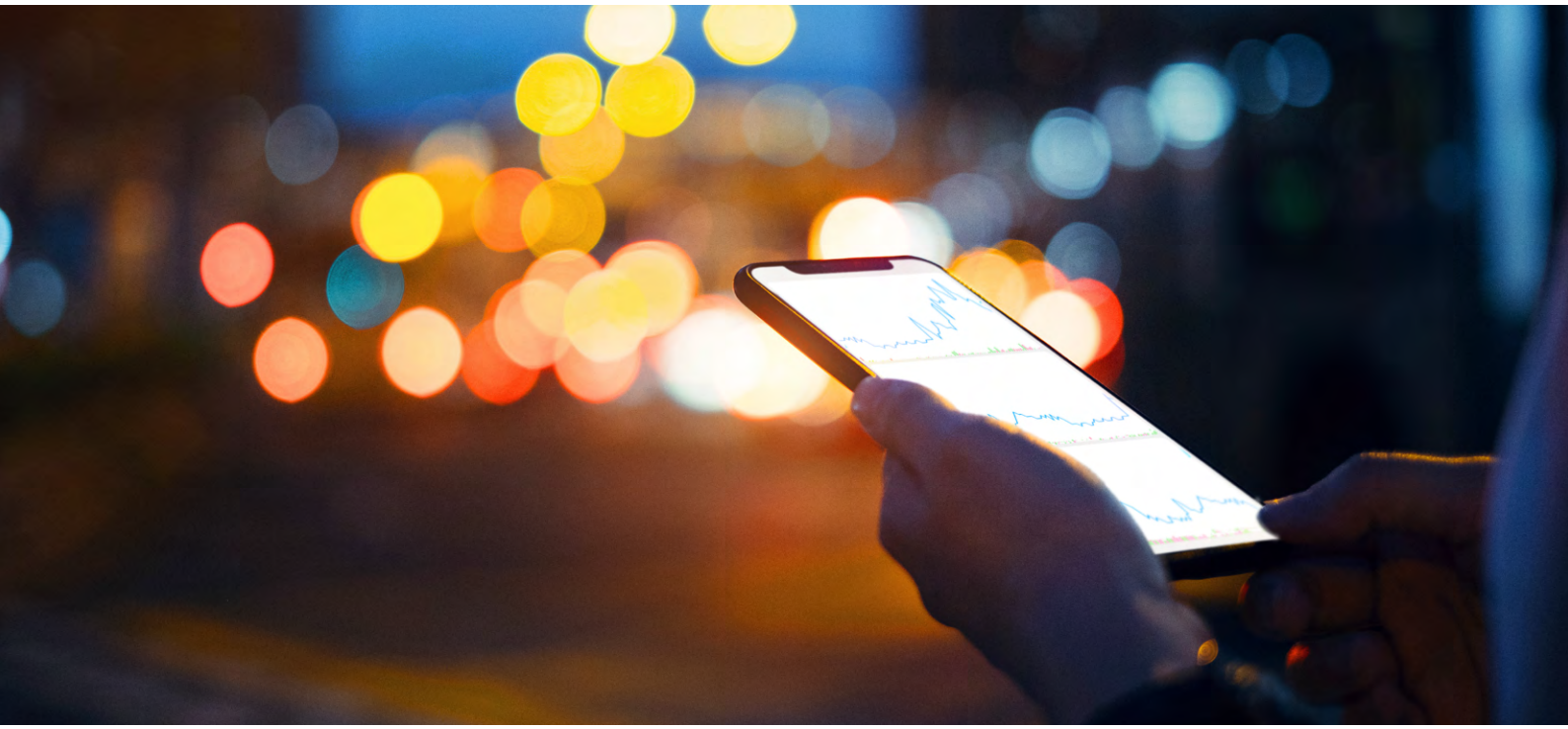
SCHUTZ VOR BETRUG

DIE AUSWIRKUNGEN:

- ✓ Kontinuierliche Authentifizierung
- ✓ Reduzierte Umsatzausfälle
- ✓ Reduzierung von durch Fraud entstandene Kosten
- ✓ Automatisierte Betrugserkennung

DIE ERGEBNISSE:

- ✓ Schutz in Echtzeit
- ✓ Minimierte operative Kosten
- ✓ Optimierte Prozesse



Optimierung der Customer Experience

Behandeln Sie Ihre Kunden nicht wie Kriminelle

In unserer digitalen Welt gibt es nicht die eine Lösung für alle. Unternehmen, die wachsen und ihren Umsatz steigern wollen, müssen zwischen legitimen und betrügerischen Online-Aktivitäten unterscheiden und ihre Kunden, Marken und Gewinne vor Risiken und Betrug schützen.

RISIKO

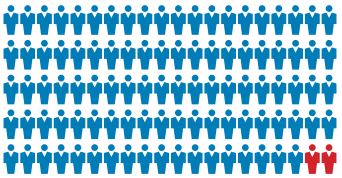
Schlechte Bonität
Kunden können nicht bezahlen

BETRUG

Betrugsabsicht
Kunden wollen nicht bezahlen

Da sich die Betrugsprävention auf die betrügerischen Nutzer konzentriert, neigen Unternehmen dazu, auch legitime Nutzer als Kriminelle, denn als vertrauenswürdige Kunden zu behandeln.

98%
der Transaktionen
sind rechtmäßig *



Nur 2%
sind betrügerisch

*Quelle: Gartner

Ausgewogenheit zwischen Komfort und Sicherheit: das Beste aus zwei Welten

Ein reibungsloses Erlebnis ist für Endkunden während der gesamten Customer Journey über alle Kanäle hinweg entscheidend. Behavioral Biometrics ermöglicht komfortable Authentifizierungsprozesse und schützt zeitgleich Ihr Unternehmen und Ihre Endkunden vor Betrug.

Fokus auf die Customer Experience:
Das macht den Unterschied in der digitalen Welt

Bis 2022 werden digitale Unternehmen
MIT POSITIVEN KUNDENERLEBNISSEN
bei der Identitätsbestätigung
20% MEHR UMSATZ ERZIELEN.*

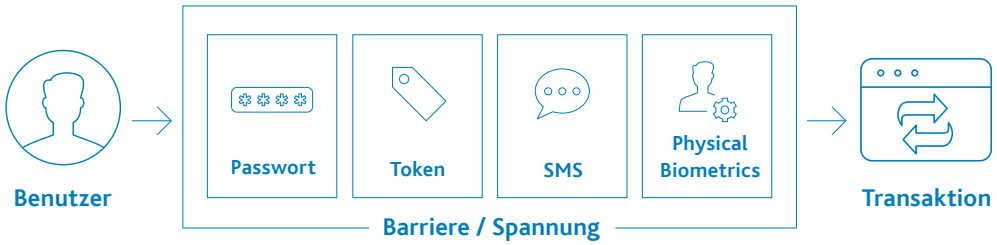
Fokus auf die Betrugsbekämpfung:
Besserer Schutz vor Bedrohungen

STÄRKERE SICHERHEITSMASSNAHMEN
zur Vermeidung von Betrug
MINIMIEREN DIE HÜRDEN FÜR KUNDEN,
die digitale Transaktionen durchführen möchten.

*Quelle: Gartner

Eine reibungslose Customer Journey

Obwohl die meisten digitalen Transaktionen rechtmäßig sind, stoßen Benutzer derzeit im Check-Out, in der Accountverwaltung und im Authentifizierungsprozess auf viele Hindernisse. Darüber hinaus können Datenschutzbestimmungen durch zusätzliche Sicherheitsmaßnahmen während der gesamten Customer Journey diese Hürden erhöhen, z.B. durch Multifaktor-Authentifizierung (MFA).



Wie Behavioral Biometrics funktioniert und was es für Ihr Unternehmen tun kann

Betrüger haben verschiedene Wege gefunden, den Schutz herkömmlicher Authentifizierungsmethoden zu überwinden, indem sie Sicherheitslücken ausnutzen und ausgefeilte automatisierte Betrugsangriffe starten:

TRADITIONELLE AUTHENTIFIZIERUNGSMASSNAHMEN	BETRÜGERISCHE GEGENMASSNAHMEN	BESCHREIBUNG
Benutzername & Passwort	Darknet	Handel mit gestohlenen Anmelde- und Zahlungsdaten in versteckten Online-Netzwerken
Captcha	Ausgefeilte BOTS	Simulation des menschlichen Verhaltens, um nahezu realistische Aktionen durchzuführen (z.B. Aggregatoren, Scrapers und Crawlers)
GEO-Position	Proxy	Verwendung von Vermittlungsservern, um die tatsächliche Geo-Positionierung des Benutzers zu verbergen
Device fingerprinting	Emulator	Verwendung von Computer-programmen zur Simulation von Geräten, die gefälschte Sensordaten an Apps senden
Multifaktor-Authentifizierung	Session takeover	Unbefugter Zugriff auf Benutzer- und Kontoinformationen zur Ausführung von Transaktionen

Wie effektiv sind Sie, wenn es darum geht, Ihre Benutzer zu authentifizieren und Betrug zu stoppen, um Ihr Online-Geschäft und Ihre Kunden zu schützen? Behavioral Biometrics erkennt Anomalien und verdächtiges Verhalten. Durch die frühzeitige Identifizierung von „legitimen Nutzern" bleibt nur eine kleine Gruppe von „verdächtigen Nutzern" übrig, die mit zusätzlichen Methoden validiert werden können.

GRUNDSÄTZE VON BEHAVIORAL BIOMETRICS

Behavioral Biometrics bietet eine zusätzliche Sicherheitsebene, indem sie eine reibungslose, kontinuierliche Benutzerauthentifizierung ermöglicht, die praktisch nicht zu fälschen ist. Die Grundsätze dieser Lösung sind:

- ✔ Rückschlüsse aus Verhaltensmustern der Benutzer mithilfe von Machine Learning
- ✔ kontinuierliche Überwachung der Verhaltensdaten für mehr Genauigkeit
- ✔ Hintergrundanalyse von Daten (für den Benutzer unsichtbar)
- ✔ Dynamisch verbesserte Sicherheitsebene durch Echtzeit-Analysen der technischen Daten

Differenzierungsmerkmale von Behavioral Biometrics

Die statische Authentifizierung durch physische Biometrie, wie z.B. Gesichtserkennung, Iriserkennung, Fingerabruck, kann anfällig für Sicherheitslücken und Risiken sein. Passive Biometrics-Lösungen bieten eine intelligentere und sicherere Lösung. Sie liefern eine kontinuierliche Authentifizierung, die eine reibungslose Benutzervalidierung ermöglicht. Dies basiert auf dem einzigartigen und messbaren Verhalten der menschlichen Interaktion mit dem Endgerät wie beispielsweise Klicken, Swipen, Zoom-Muster, Fingerdruck, Tippgeschwindigkeit und Gerätehaltung.

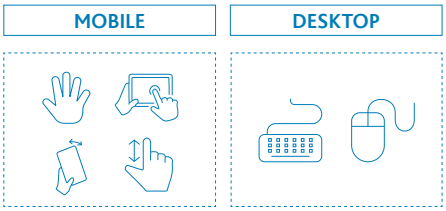
AKTIVE PHYSICAL BIOMETRICS

EINZELNE IDENTIFIKATIONSPUNKTE

- ✔ Erfordert spezielle Hardware und aktive Benutzerinteraktion
- ✔ Daten können gestohlen, gefälscht oder kopiert werden

VS.

PASSIVE BEHAVIORAL BIOMETRICS



MULTI-PARAMETER TOUCHPOINTS

- ✔ Nahtlose Identifizierung ohne zusätzliche Maßnahmen
- ✔ Daten können nicht gestohlen, gefälscht oder kopiert werden

Die Technologie erstellt ein einzigartiges Profil für jeden Benutzer, indem sie hunderte von Parametern aus menschlichen Interaktionen mit dem Gerät, Geräteattributen und Kontoaktivitäten sammelt und analysiert. Dieser Vorgang läuft im Hintergrund innerhalb einer Website oder App ab.

Lösungskomponenten

PASSIVE BIOMETRICS

- ✔ Analyse von hunderten Parametern aus der menschlichen Interaktion mit dem Gerät, den Geräteattributen und den Kontoaktivitäten.
- ✔ Feststellung, ob sich der mit dem Gerät interagierende Benutzer normal verhält und dem legitimen Profil entspricht

VERHALTENSAUFFÄLLIGE ANOMALIEN

- ✔ Analyse eines allgemeinen, guten Nutzerverhaltens im Vergleich zu betrügerischen Aktivitäten z.B. durch einen Gast Check-Out ohne Nutzerprofil
- ✔ Identifizierung von betrügerischen Aktivitäten und Anomalien

BOT-ERKENNUNG

- ✔ Erkennung von nichtmenschlichem Verhalten und automatisierten Angriffen
- ✔ Erkennung ausgefeilter Betrugsversuche, die traditionelle Erkennungswerkzeuge, mit Hilfe von virtueller und automatisierter Betrugstechniken durch Bots umgehen

ANALYSE DES GERÄTS

- ✔ Analyse des Geräts durch Crowd Intelligence und ausschließlicher Nutzung technischer Daten (keine PII-Daten; DSGVO-konform)
- ✔ Feststellung, ob es sich um ein echtes Gerät oder einen Emulator handelt.

Trust Score für die Benutzerauthentifizierung

Durch einen Trust Score, der auf dem Online-Verhalten des Benutzers und der Interaktion mit dem Gerät basiert, unterscheidet Behavioral Biometrics legitime von betrügerischen Benutzern und nicht-menschlichen Aktivitäten.

Ein Trust Score wird in Echtzeit erstellt und errechnet eine Wahrscheinlichkeit, dass der Benutzer nicht nur eine Person ist, sondern auch ob der Benutzer der eigentliche Eigentümer des authentifizierten Kontos ist. Dies ermöglicht Echtzeit-Entscheidungen innerhalb der jeweiligen Nutzersession und verringert das Betrugsrisiko.

Behavioral Biometrics erkennt Geräteanomalien und Abweichungen von der normalen Online-Aktivität.

MENSCHLICHE AKTIVITÄT

LEGITIM		BETRÜGERISCH
RECHTMÄSSIGER NUTZER	VS.	BETRÜGER

MENSCHLICHES VERHALTEN		NICHT-MENSCHLICHES VERHALTEN
REALE PERSON	VS.	BOT

AKTIVITÄT DES GERÄTS

REALITÄT		SIMULATION
PHYSISCHES GERÄT	VS.	EMULATOR

VORTEILE

- ✔ Unterbindung der Kontoübernahme (ATO) in Echtzeit
- ✔ Identifizierung legitimer Benutzer (KYC)
- ✔ Verbesserung der Customer Experience
- ✔ Reduzierung von False Positives
- ✔ Reduzierung von Kosten
- ✔ Einhaltung von DSGVO-Standards

Wie der Trust Score generiert wird

Basierend auf dem analysierten Benutzerverhalten und den Gerätedaten liefert Behavioral Biometrics einen Trust Score in drei Schritten:

1. DATENPUNKTANALYSE ZUR ERSTELLUNG EINES BENUTZERPROFILS

Alle Verhaltens- und Gerätedaten werden erfasst und miteinander verknüpft.

Hunderte von Einzelinformationen werden zu einem einzigartigen Benutzerprofil kombiniert, das viel schwieriger zu kopieren ist als ein Passwort oder eine PIN.

Im Laufe der Zeit sammelt die Behavioral Biometrics-Lösung immer mehr Daten, um das Benutzerprofil zu verfeinern, was zu einer noch stärkeren und personalisierteren Benutzerauthentifizierung führt.

2. ERKENNUNG VON ANOMALIEN DURCH MACHINE LEARNING

Predictive Modeling erfolgt durch die automatisierte Entwicklung und Anwendung von selbstlernenden Algorithmen. Sie erkennt Abweichungen von der normalen Online-Aktivität.

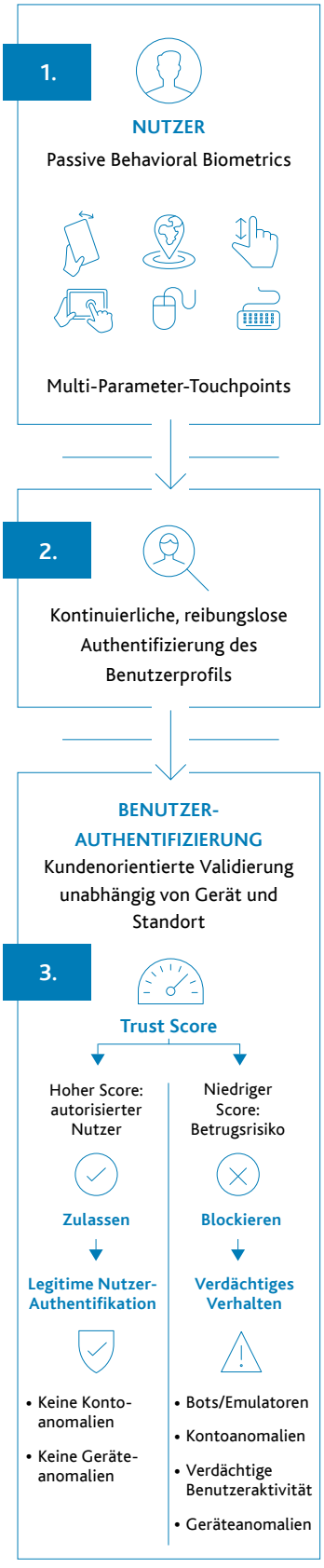
Geräteeigenschaften	Interaktion mit dem Gerät	Nutzerverhalten
Geräte-ID, Geo-Positionierung	Touchscreen & Sensor-Daten & Tastatur und Maus	Navigationsmuster und Benutzerentscheidungen

3. TRUST SCORE GENERIERUNG

Ein Trust Score wird in Echtzeit erstellt und spiegelt ein fein kalibriertes Sicherheitslevel wider, dass der Benutzer nicht nur eine Person, sondern auch die richtige Person ist.

Dies ermöglicht Entscheidungen in Echtzeit innerhalb einer Nutzer-Session und verringert das Betrugsrisiko.

Das Trust Scoring ermöglicht Echtzeitalarmierung, automatisierte Betrugserkennung und Identifizierung legitimer Benutzer. Die Annahme von Transaktionen vertrauenswürdiger Kunden oder die Blockierung von Aktivitäten verdächtiger Benutzer erfolgt dann automatisiert und gestaltet Prozesse effizienter, was wiederum zu einer optimierten Customer Journey führt.



Vorteil und Mehrwert: Baustein für ein zukunftssicheres Unternehmen

Behavioral Biometrics hilft bei der genauen Unterscheidung zwischen legitimen Kunden und Cyberkriminellen in Echtzeit: Maximierung von Sicherheit und Vertrauen, Minimierung von Friction und Risiko. Behavioral Biometrics wurde entwickelt, um Sie bei der Betrugsbekämpfung zu unterstützen, ihr Endkundenerlebnis zu optimieren, Entscheidungsprozesse zu vereinfachen und den Umsatz zu steigern.

Die richtige Anwendung von Behavioral Biometrics wird in einer schnelllebigen, digital gesteuerten Welt einen entscheidenden Wettbewerbsvorteil für Unternehmen schaffen.

1. **Kontinuierliche & reibungslose Online-Authentifizierung**
   Die Lösung läuft ab dem ersten Moment des Surfens im Hintergrund innerhalb der Website oder der App. Sie authentifiziert kontinuierlich das Verhalten des Benutzers gegenüber dem eindeutigen Benutzerprofil. Behavioral Biometrics führt zu einer reibungslosen Erfahrung und macht mehrere Stufen von Authentifizierungsanfragen überflüssig.

2. **Benutzervalidierung und Betrugserkennung unabhängig von der Hardware & Standort**
   Automatisierte Erkennung von Betrugsangriffen und Validierung von Benutzern auf der Grundlage von Verhaltensanalysen. Der Prozess wird kontinuierlich während der gesamten Interaktion des Benutzers mit der Anwendung durchgeführt. Jede Abweichung von dem, was als „normales Verhalten" eines bestimmten Benutzers mit einem bestimmten Gerät und einem bestimmten Konto definiert ist, wird als Anomalie gekennzeichnet.

3. **Technische Datenanalyse – keine Erhebung oder Speicherung personenbezogener Daten**
   Behavioral Biometrics basiert darauf, dass anstelle von personenbezogenen Daten nur technische Daten verwendet werden und die Datenschutzbestimmungen wie DSGVO eingehalten werden. Dies spiegelt den Gesamtansatz wider, High-End-Datenanalyse mit den erforderlichen rechtlichen Rahmenbedingungen zu kombinieren.

Die Anwendung von Behavioral Biometrics steigert das Vertrauen in Ihre Endkunden, stoppt Betrug und unterstützt das Wachstum Ihres Unternehmens.

Intelligente Benutzeridentifikation: unsichtbar für den Benutzer, was eine reibungslose Customer Journey ermöglicht.

Fortschrittliche Betrugsprävention: zusätzliche Sicherheitsebene, basierend auf Machine Learning

Gesteigerter Umsatz: Erkennung von betrügerischen Aktivitäten in Echtzeit, um Verluste zu reduzieren.

Wettbewerbsfähige Dienstleistungen: Bereitstellung wettbewerbsfähiger Dienstleistungen und Einhaltung von Vorschriften wie der DSGVO

Möchten Sie mehr über Behavioral Biometrics erfahren? Kontaktieren Sie uns jetzt und sichern Sie sich entscheidende Wettbewerbsvorteile!

Arvato Financial Solutions | Sales Team Fraud Management
Phone: +49 7221 5040 - 1600 | E-Mail: fraud-management@finance.arvato.com | finance.arvato.com