

Harnessing the power of Behavioral Biometrics

A game changer in fraud prevention

Financial Solutions

Trick or treat: trust & fraud in the digital age



Digital is the new normal. Customer expectations have shifted because of technology, and 'always-online' behavior fuels the need for a fast and convenient journey to complete digital transactions. This development also leads to the increase in online fraud, which is becoming more and more sophisticated. The negative impact on consumer trust and business revenue is significant.

Online fraud includes threats such as account takeover, new account fraud, payment fraud and automated attacks. These cause significant challenges and risks:



CUSTOMER FRICTION

Intrusive authentication methods and additional security can be a hurdle for legitimate customers



OPERATIONAL COSTS

Inefficient processes, fraud case investigation and high rate of manual transaction reviews cause costly overhead



FINANCIAL LOSSES

Due to low approval rates, customer abandonment, fraud cases and false positives



REPUTATIONAL DAMAGE

Loss of customer trust and loyalty as a result of becoming a victim of fraudsters

PREVENTING ONLINE FRAUD

Detecting online fraud can be a delicate balancing act: how do you recognize trusted behavior from loyal and potential customers, while preventing and stopping fraudulent activity?



Minimize friction and maximize security with Behavioral Biometrics

Combining a seamless customer experience with stronger protection:

Smart online authentication:

Identify good users and provide them with smooth and hassle-free authentication and check-out experience.

Real-time fraud prevention:

Increase security by instantly recognizing, detecting and stopping fraud threats, anomalies and suspicious activity patterns.

CONVENIENT TRANSACTIONS



THE IMPACT

- ✓ Frictionless authentication
- ✓ Improved customer experience
- ✓ Stop pushing loyal customers away

THE RESULTS

- ✓ Minimized false positives
- ✓ Avoid transaction abandonment
- ✓ Increased conversion rate

FRAUD PROTECTION

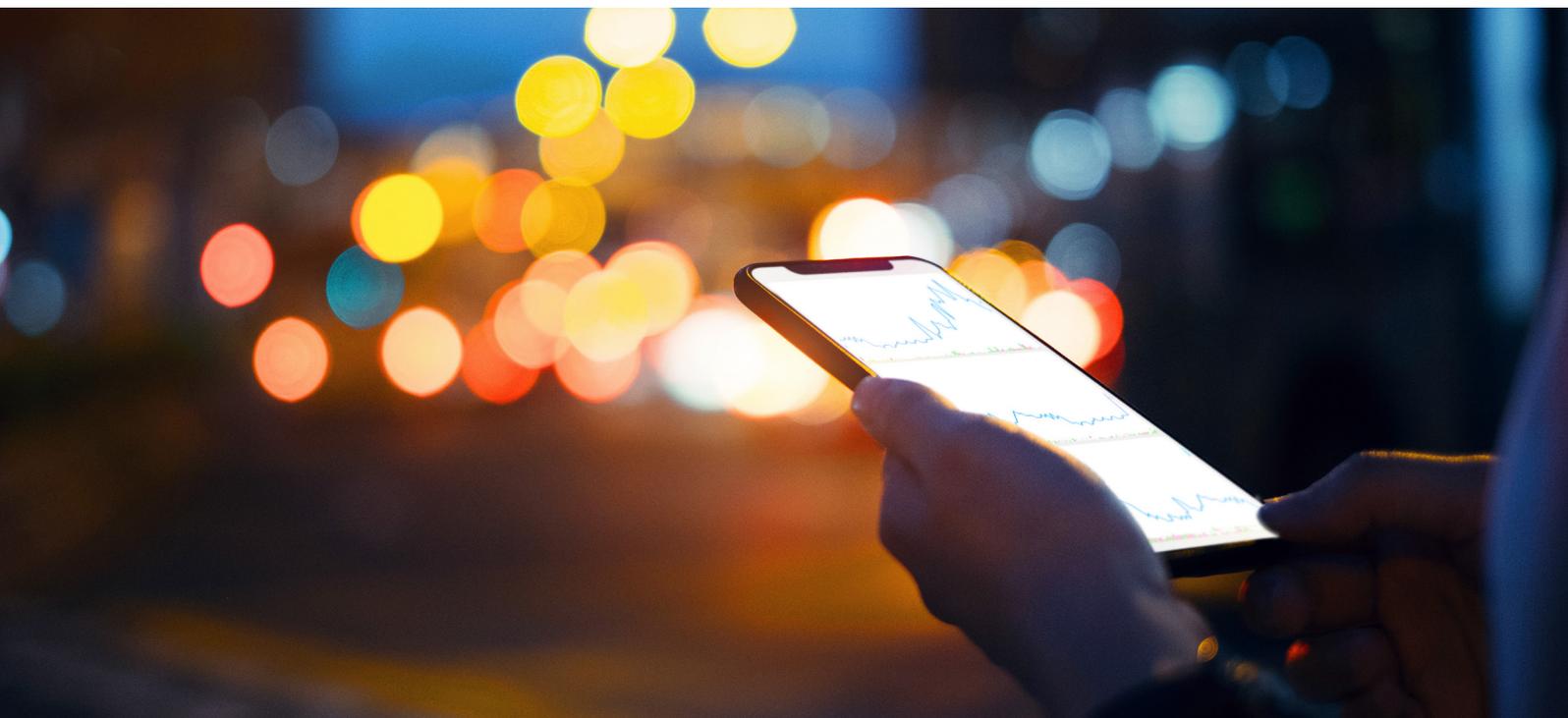


THE IMPACT

- ✓ Continuous authentication
- ✓ Reduced fraud losses
- ✓ Automated fraud detection

THE RESULTS

- ✓ Protection in real-time
- ✓ Minimized operational costs
- ✓ Optimized processes



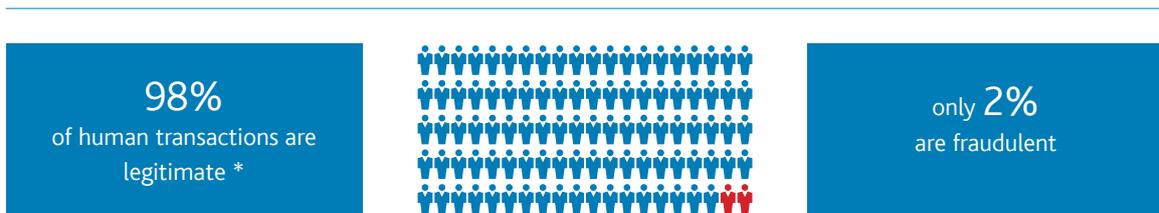
Optimizing the customer experience

Don't treat your customers as criminals

In our digital world, one size doesn't fit all. Companies willing to increase revenue and to grow have to differentiate between good and bad online activity and protect their customers, brand and profits against risk and fraud.



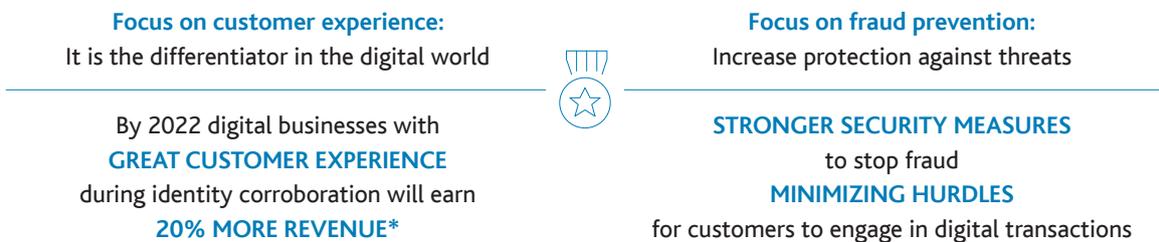
Because fraud prevention focuses on the fraudulent users, companies tend to treat legitimate users as criminals rather than trusted customers.



*Source: Gartner

Balancing convenience and security: the best of both worlds

A seamless experience is crucial for users throughout the multichannel user journey and the authentication process. Behavioral Biometrics makes this possible, while protecting your business and your customers against fraud.



*Source: Gartner

A frictionless customer journey

Even though most digital transactions are legitimate, users currently encounter many barriers in the check-out, account administration and authentication process. In addition, data protection regulations may increase these hurdles with supplementary security measures throughout the customer journey, e.g. with multi-factor authentication (MFA) requests.



How Behavioral Biometrics works and what it can do for you

Fraudsters have found different ways to overcome the protection of traditional authentication methods by taking advantage of security gaps and sophisticating automated fraud attacks:

TRADITIONAL AUTHENTICATION MEASURE	COUNTERACTING FRAUD METHODS	DESCRIPTION
Username + password	Darknet	Trade of stolen login and payment data in online hidden networks
Captcha	Sophisticated BOTS	Simulation of human behavior to perform fairly realistic actions (e.g. aggregators, scrapers and crawlers)
Geo location	Proxy	Use of intermediary servers to hide the true geolocation of the user
Device fingerprinting	Emulators	Using computer programs to simulate devices sending fake sensor data to apps
Multi factor authentication	Session takeover	Unauthorized access to user & account information to execute transactions

How effective are you when it comes to authenticate your users and stop fraud to protect your online business and your customers? Behavioral Biometrics detects anomalies and suspicious behavior. The early identification of 'good users' leaves only a small group of 'suspected users' to validate with additional methods.



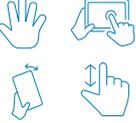
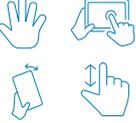
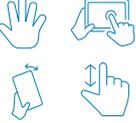
BEHAVIORAL BIOMETRICS: KEY PRINCIPLES

Behavioral Biometrics provides an additional layer of security by offering seamless, continuous user authentication virtually impossible to imitate. Key principles of this solution:

- ✓ Powered with machine learning capabilities learning from the patterns from the users' behavior
- ✓ Continuous behavior data monitoring and improved accuracy
- ✓ Analysis of data points in the background (invisible to the user)
- ✓ Security layer dynamically improved through real-time analysis of technical data

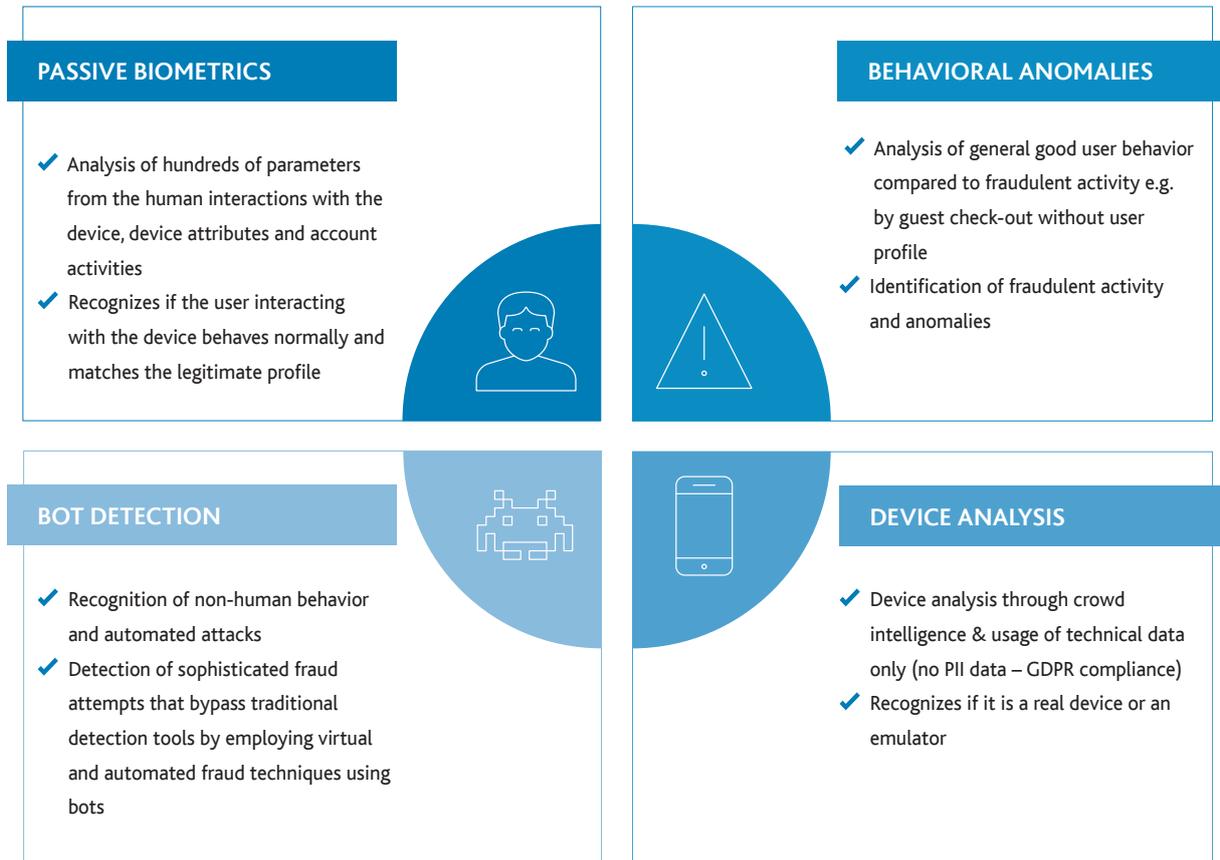
Behavioral Biometrics differentiators

The static authentication delivered by active physical biometrics can be vulnerable to security gaps and risks. Passive biometrics offers a smarter and safer solution. It allows continuous authentication providing the mechanism for frictionless user validation based on the unique and measurable behavior from the human interaction with a device such as clicking, swiping, zooming patterns, finger pressure, typing speed and device holding.

ACTIVE PHYSICAL BIOMETRICS	VS.	PASSIVE BEHAVIORAL BIOMETRICS				
<div style="text-align: center;">  </div> <p style="text-align: center;">SINGLE IDENTIFICATION POINTS</p> <ul style="list-style-type: none"> ✓ Requires special hardware and active user interaction ✓ Data can be stolen, spoofed or copied 		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th data-bbox="898 1585 1107 1615">MOBILE</th> <th data-bbox="1123 1585 1337 1615">DESKTOP</th> </tr> </thead> <tbody> <tr> <td data-bbox="898 1630 1107 1787" style="text-align: center;">  </td> <td data-bbox="1123 1630 1337 1787" style="text-align: center;">  </td> </tr> </tbody> </table> <p style="text-align: center;">MULTI-PARAMETER TOUCHPOINTS</p> <ul style="list-style-type: none"> ✓ Seamless identification without extra actions needed ✓ Data can't be stolen, spoofed or copied 	MOBILE	DESKTOP		
MOBILE	DESKTOP					
						

The technology creates a unique profile for each user by collecting and analyzing hundreds of parameters from human interactions with the device, device attributes and account activities. It runs in the background within the website or app.

Solution components

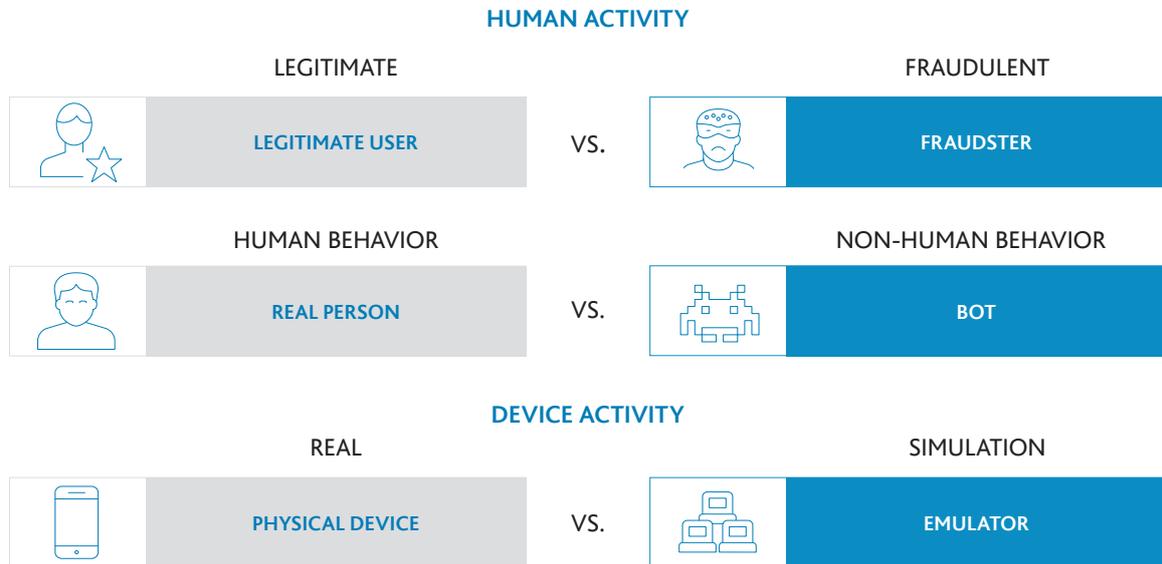


Confidence scoring for user validation

Through a Trust Score, Behavioral Biometrics recognizes good vs. bad users and non-human traffic based on the online behavior of the user and the interaction with the device.

A Trust Score is established in real-time and represents the level of confidence that the user is not only a person, but also the probability of the user being the real owner of the account authenticating in the system. This enables real-time decision-making within sessions and decreases the risk of fraud.

Behavioral Biometrics recognizes device anomalies and deviations from normal online activity



KEY BENEFITS	
✓ Stop account takeover (ATO) inreal-time	✓ Minimize false positives
✓ Identify good users (KYC)	✓ Reduce costs
✓ Improve customer experience	✓ Regulation compliance



How the Trust Score is generated

Based on the analyzed user behavior and device data, Behavioral Biometrics delivers a Trust Score in three steps:



1. DATA POINTS ANALYSIS TO CREATE A USER PROFILE

All behavioral and device data are collected and linked.

Hundreds of metrics are combined into a unique user profile that is much harder to copy than a password or PIN.

Over time, the Behavioral Biometrics solution collects more and more data to refine the user profile leading to an even stronger and more personalized user authentication.



2. RECOGNIZING ANOMALIES WITH MACHINE LEARNING

Predictive modeling takes place through the automated development and application of self-learning algorithms. It detects deviations from normal online activity.

Device attributes



Device-ID,
geolocation

Device interaction



Touchscreen & sensors data
+ keyboard & mouse

User behavior



Navigation patterns and
user choices

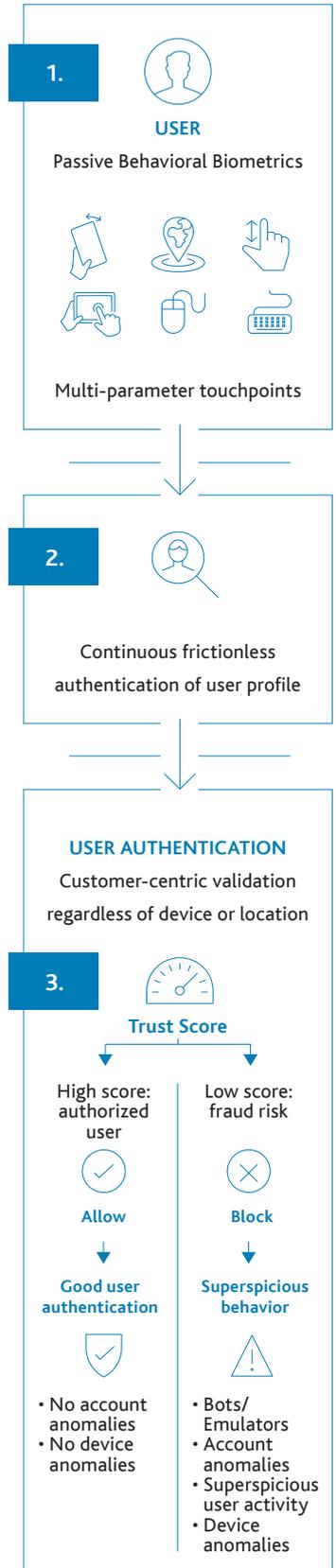


3. TRUST SCORE GENERATION

A Trust Score is established in real-time and reflects a finely calibrated level of confidence that the user is not only a person, but also the right person.

This enables making real-time decisions within sessions and decreases the risk of fraud.

The confidence scoring allows for real-time alerting, automated fraud detection and identification of legitimate users. Accepting transactions from trusted customers or blocking activity from suspicious users is then an automated process allowing for process efficiency and optimization of the customer experience.



Benefits and added value : building block for a future-proof business

Behavioral Biometrics helps by accurately distinguishing between legitimate customers and cybercriminals in real-time: maximizing security and trust, minimizing friction and risk. It is designed to help you combat fraud, accept genuine customers optimizing their customer experience, streamline decision-making processes and increase revenues.

The right application of Behavioral Biometrics will give a business competitive advantage in a fast-paced, digital driven world.

1. Continuous & frictionless online authentication

The solution runs in the background within the website & app and continuously authenticates the user's behavior against the unique user profile from the first moment of browsing. It results in providing a seamless experience and eliminating the need for multiple step-up authentication requests.

2. User validation and fraud detection independent from hardware, device & location

Automated detection of fraud attacks and validation of users based on behavioral analytics. The process is carried out continuously, throughout the user's interaction with the application. Any deviation from what is defined as 'normal behavior' of a specific user, with a specific device, using a specific account, is flagged as being an anomaly.

3. Technical data analysis - no personal data collected or stored

Behavioral Biometrics is based on using only technical data instead of personal data, complying with data protection regulations such as GDPR. This reflects the overall approach of combining high-end data analysis within the required legal parameters.

Applying Behavioral Biometrics results in trusting your customers, stopping fraud and growing your business.



Smart user identification: invisible to the user, enabling a seamless customer journey.



Advanced fraud prevention: additional security layer, powered by machine learning / AI.



Increased revenue: real-time detection of fraudulent activity, reducing losses.



Competitive services: provide competitive services and compliance with regulations such as General Data Protection Regulation (GDPR).

Do you want to know more about Behavioral Biometrics?
Please feel free to contact us.

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