feedzai | Solution Guide

Behavioral Biometrics Analysis

#ProtectYourCustomers

feedzai.com

Contents

What Is Behavioral Biometric Analysis?

Behavioral biometric technology is a highly accurate technology for authenticating users based on their behavior patterns. It identifies unique, individual characteristics in how people type and interact with their mobile device or computer. Other common technologies identify users based on their physical attributes (e.g., fingerprints or facial recognition), what they have (e.g., key fobs or phones), or what they know (e.g., passwords or out-of-wallet questions).

Digital IDs rooted in behavioral biometrics are as unique to a person as fingerprints. They can quickly and accurately verify the identity of a user from one session to the next and continuously verify the identity during a single session.

Any anomalies detected in the user's behavior at any point in their online session can signal that someone else is impersonating them if they are acting under duress, or that a security breach or attempted fraud is at hand.

Physical vs. Behavioral Biometrics

Physical biometrics relates to a person's biology, parts of the human body that can serve as an identifier – such as a fingerprint or retina scan. While behavioral biometrics refers to a person's unique pattern of behavior – such as the rhythm and cadence with which they usually type on their computer keyboard or the way they move the mouse.

Physical

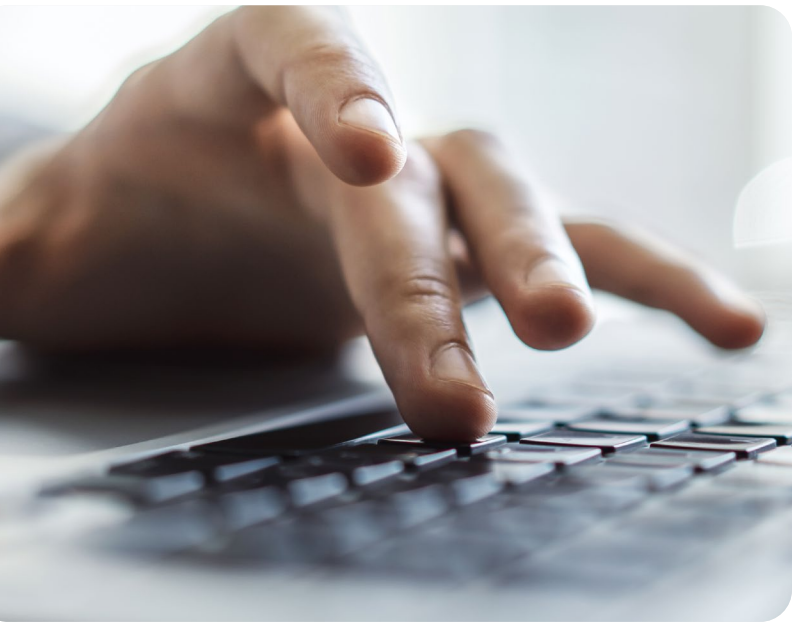
- Face
- Fingerprint
- Hand
- Iris
- DNA

We encounter physical biometric analysis for security purposes more often than we think, for example, when we unlock our mobile phones with a touch or go through an e-passport gate after looking into a camera.

However, behavioral biometrics is a newer technology gaining ground in online banking fraud prevention. Its power lies in authenticating genuine users - without requiring additional steps that add friction to the process - and spotting fraudsters who return to a bank's system.

Behavioral

- Keystroke Dynamics
- Cursor Movement
- Mobile Interactions
- Handling



> Behavioral Biometrics power lies in authenticating genuine users (...) and spotting fraudsters who return to a bank's system.

Examples of behavioral biometrics authentication include:

Keystroke Dynamics

Typing patterns that include a combination of keystroke speed, keystroke duration, variations in these for particular key sequences, and characteristic patterns that occur when typing common groups of keystrokes.

Mobile Interactions

Unique ways users type on the touch screens of mobile devices like tablets and phones.

Cursor Movement

Unique patterns in mouse or trackpad cursor movement, including paths, tracking speed, direction changes, and clicks.

Handling

The way an individual holds or handles a mobile device provides another unique behavioral biometric factor.

What is a BionicID™?

The fundamental building block of a BionicID™ is behavioral biometrics. Feedzai collects thousands of non-PII parameters starting with behavioral biometrics. This includes how a user handles a device and layers on behavioral analytics - when, from where, and what the user accesses. It also provides device and network information including all the associated data that is used to access a protected website or mobile application server.

Feedzai takes a unique approach to verify users at every point in the customer journey by continually asking, “are you really you?” Other behavioral biometrics companies compare users against a database of known bad actors, or segments of good actors, trying to answer the question, “do you look like a bad or good actor?” This approach can be effective. Still, in many cases, it is not granular enough.

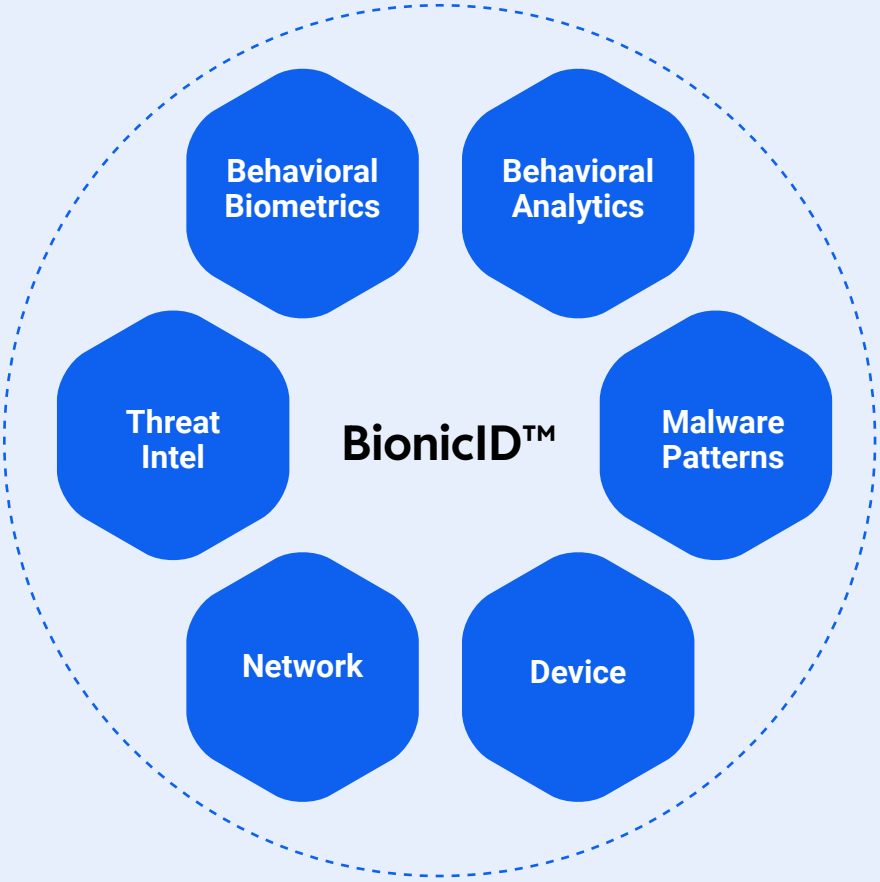
Moreover, it does not provide complete coverage - leaving the possibility that sophisticated bad actors will slip through early on in a new account signup process or at other points in the user journey.

The “do you look like a bad actor?” method of determining legitimate users vs. bad actors does not work in scenarios where insiders - people who have verified identities and are not part of the larger universe of cybercriminals - attempt unauthorized access to bank accounts.

> **“ Feedzai BionicID™ is based on full user context and built to recognize every single user.**

Feedzai BionicID™ is based on full user context and built to recognize every single user. They are established quickly and can start answering the question “are you really you?” accurately in just a couple of interactions.

The Components of BionicID™



Feedzai's BionicID is a "cyber-DNA" or a digital fingerprint, built using thousands of parameters about the user's context based on behavioral biometrics, behavioral analytics, and device profiling, network data, geolocation, malware patterns, and other threat intel data.

As a result, it recognizes the real person behind each user in as little as two interactions, with a 99.2% accuracy in just milliseconds!

99.2%

accuracy in recognizing the real person behind each user

feedzai

What Makes Feedzai's BionicID™ Solution Unique in Fraud Prevention?

BionicID™ data collection and analysis is the foundational technology in Feedzai's multi-channel fraud prevention solution. Feedzai's Platform is unique. It does not just detect anomalies, score risks and raise alerts; it also empowers fraud teams to easily configure the system to handle many fraud cases automatically.

This active defense approach protects users without them even knowing about threats, reduces call center costs, and reduces the burden on fraud analysts. In addition, it frees fraud teams from handling routine alerts and proactively assists in investigating more complex cases.

With Feedzai, analysts can take a preemptive defense approach, take down bad actors and mule accounts and stop fraud before it happens.

> **With Feedzai, analysts can take a preemptive defense approach and stop fraud before it happens.**

What Makes Feedzai's BionicID™ More Accurate than Other Behavioral Biometric Solutions?

Unlike other behavioral biometrics vendor's solutions that classify users as "good" or "bad," Feedzai takes a different approach. Since most online users are legitimate, Feedzai asks, "are you really you?" at every interaction, using a hybrid AI system that utilizes Deep learning algorithms under expert supervision.

These per-user models compare users to themselves and take less time to train, leaving a shorter window of fraud vulnerability when a user starts interacting with the system and is verified. The system also continuously scores risk based on population-based models and bad actor models. If we detect an anomaly, we immediately spring into action and take defensive measures.

This approach eliminates misidentification. And it reduces both false positive alerts and false negatives that miss signals of actual fraudulent activity. We minimize identification times by assigning all incoming events to the best artificial intelligence and machine learning analytics module for the task.

These models are continually updated with the latest knowledge of adversary tactics, techniques, and procedures so you can stay ahead of the rapidly evolving threat landscape.

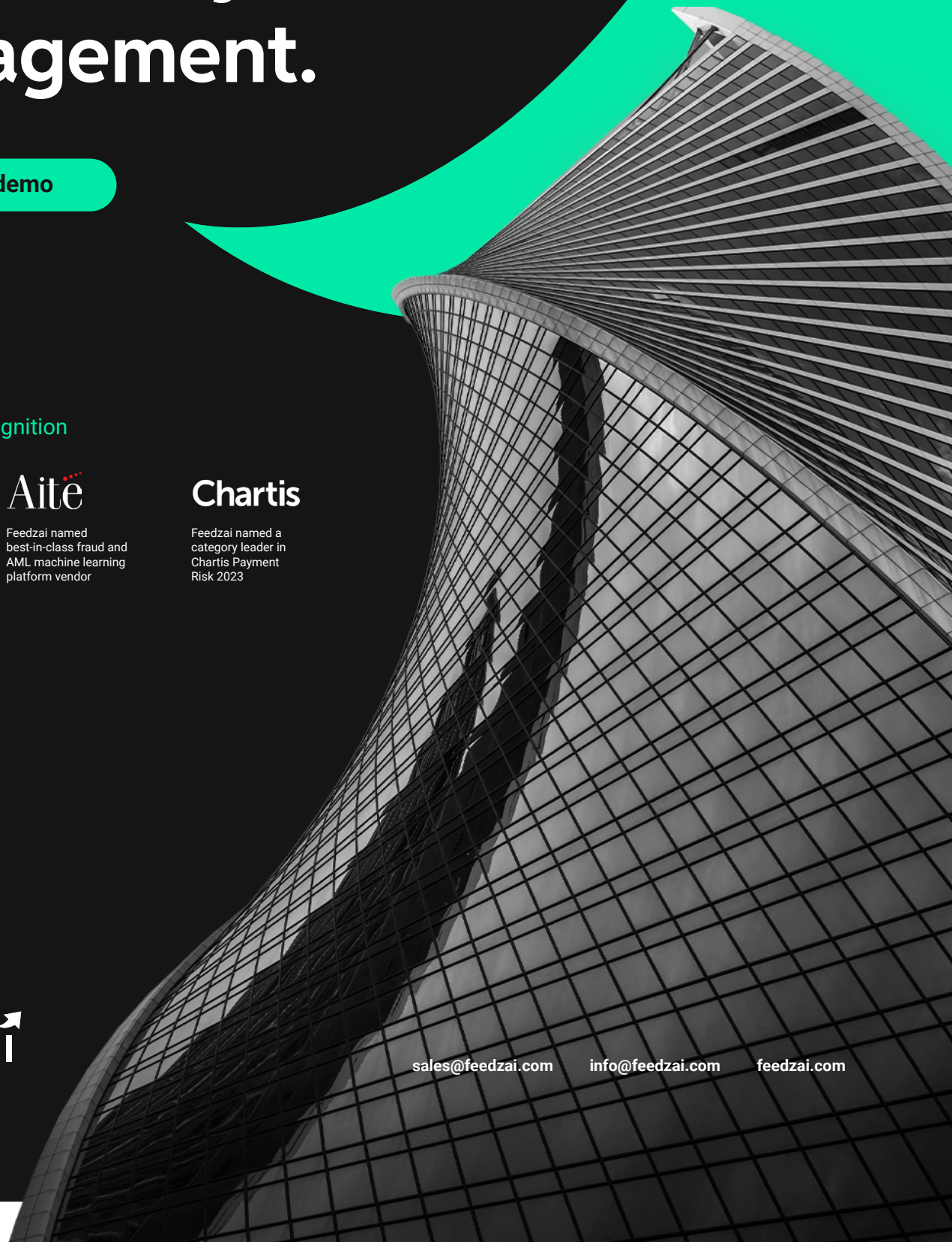
> **"Feedzai asks, "are you really you?" at every interaction.**

See for yourself how Feedzai works. We're standing by to show you how behavioral biometrics analysis enables you to know your customer at every interaction. Request a demo to see how our solution can work for your organization.

The world's first RiskOps platform

Transform your risk management.

Request a demo



Awards and Recognition

Quadrant Knowledge Solutions

Feedzai named a leader in SPARK Matrix AML.

Aité

Feedzai named best-in-class fraud and AML machine learning platform vendor

Chartis

Feedzai named a category leader in Chartis Payment Risk 2023

feedzai

sales@feedzai.com info@feedzai.com feedzai.com