BIOCATCH™
Less Friction · Less Fraud

Invisible Challenges™

BioCatch's Game-Changing Technology for Online Fraud Prevention

April 2017

White Paper

Table of Contents

Executive Summary

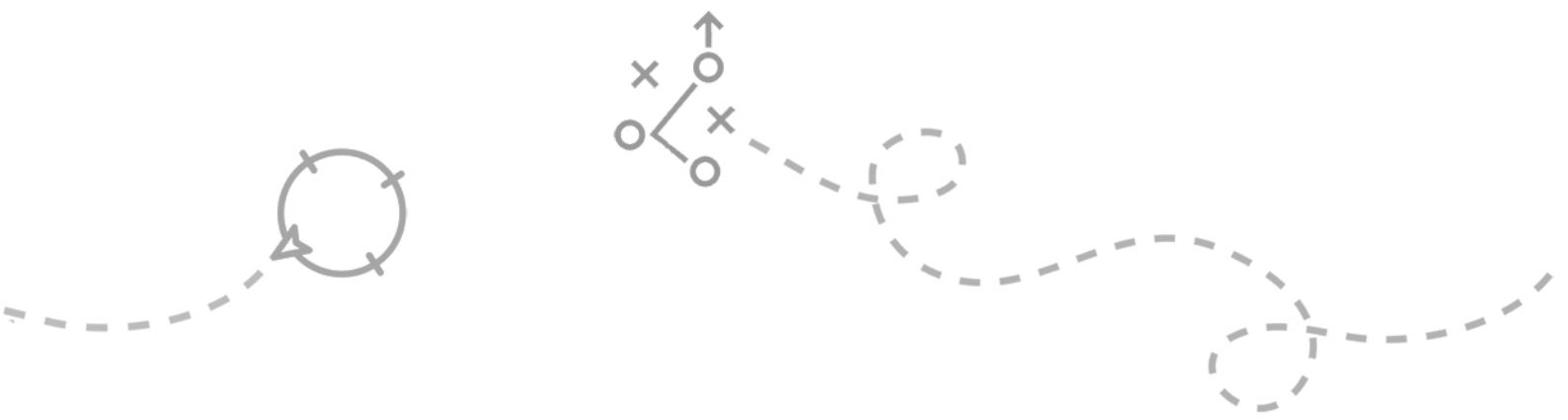
BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions, to protect users and data. Banks and other enterprises use BioCatch to significantly reduce online fraud and protect against a variety of cyber threats, without compromising the user experience.

One of the key aspects that distinguishes BioCatch as the market leader in behavioral biometrics is its patent portfolio, which as of this writing is made up of 46 patents, 17 of them granted or public. Among them, is a group that pertain to a capability called "Invisible Challenges™".

Invisible Challenges refer to tests that are invoked into an online session without the user's knowledge, but that elicit subconscious responses that can be used to distinguish a fraudster from a legitimate user.

This powerful mechanism represents the latest generation of fraud prevention tools, that addresses the weakness of traditional approaches that rely on malware libraries, two-factor authentication, device ID and other means that the sophisticated fraudsters of today have figured out how to circumvent.

Invisible Challenges also separates BioCatch from other behavioral biometrics providers that are focused on traditional keyboard, mouse movements and gesture analysis, in terms of accuracy and being able to deal with different types of replay attacks, human interaction simulation and advanced malware injections.



Introduction to Behavioral Biometrics & Invisible Challenges

The BioCatch system authenticates users by who they are, rather than by what they know (e.g, passwords, security questions). Employing cutting-edge behavioral biometric technology, the system analyzes more than 500 different behavioral patterns during a session (post-login) to determine whether the user is in fact the genuine user and not a human/non-human imposter. These parameters include:

- **Cognitive factors** such as eye-hand coordination, applicative behavior patterns, usage preferences and device interaction patterns.
- **Physiological factors** such as left/right handedness, press-size, hand tremors, arm size and muscle usage.
- **Contextual factors** such as transaction, navigation, device and network patterns.

Each user profile is based on the 20 parameters that are most unique to them. After comparing the session data to the genuine user's profile, BioCatch provides a risk score in real-time that can be used as a standalone indicator or in combination with other threat detection systems. Our solution is designed to reduce friction associated with authentication, save costs associated with escalations to cost-centers because of failed authentications and false alarms and reduce overall fraud by recognizing fraudster behavior as opposed to fixed means of identity which may be lost, stolen or circumvented.

At the heart of what makes this possible with very high accuracy, are the Invisible Challenges. These are patented techniques that introduce subtle tests into the online session that users subconsciously respond to without sensing any change in their experience. The response contains behavioral data that is used to distinguish a real user from an imposter, whether human or non-human (robotic activity, malware, aggregator, etc.). It is important to note that BioCatch's team of researchers test each challenge and its corresponding deviation to determine the threshold at which users notice a change in experience on the mobile or website.

The following are some examples of Invisible Challenges. Note that this list is provided solely for illustrative purposes and does not represent the full range of Invisible Challenges that may be employed.

Invisible Challenges Facts

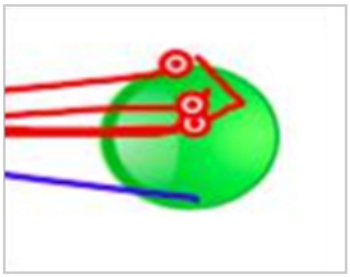
- Proactive and passive
- Injected at specific points within a session
- Change each time in a randomized way
- Elicit unique behavioral and cognitive parameters
- Do not alter the user experience

Rotation of Movement

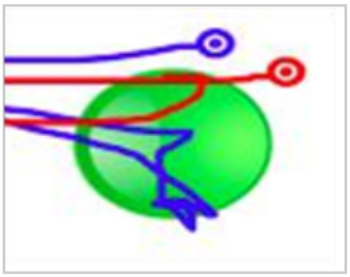
Challenge: Introduce a deviation in the mouse movement.

The example below (left image) shows a user reacting to the Invisible Challenge by making a small correction to a right-side deviation that would have made him miss his target without compensating. When given this challenge repeatedly, this user typically makes one small correction at a 60-80 degree (red hook) made during the last 10% of the movement.

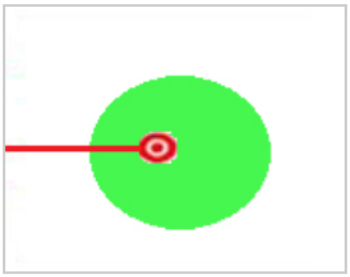
But other people respond differently to the same challenge. In the middle image, a QA manager responds with multiple corrections (blue lines). She begins her correction during the last 20% of the movement. Both users reported that they did not sense the challenge or notice anything different in the user experience. A robot (right image) would not need to compensate at all, because such movement does not involve hand-eye coordination.



User 1



User 2



Robot

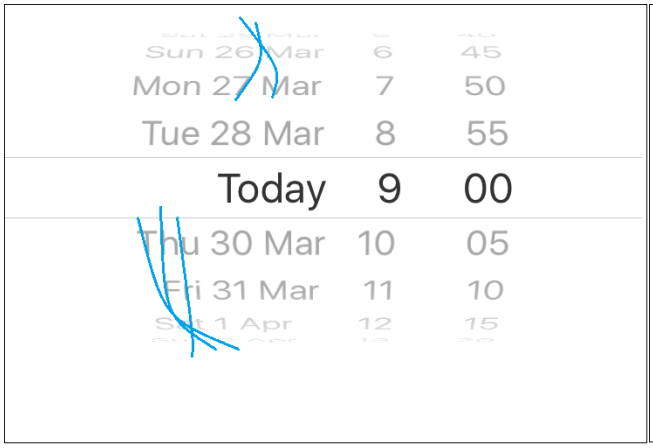
This example demonstrates an iPad touch interface challenge-response by leveraging a *drag-and-drop* effect, without any change to the user experience. Additional challenges can involve scrolling, swiping, typing and pinching/zooming.

Spinning Wheel

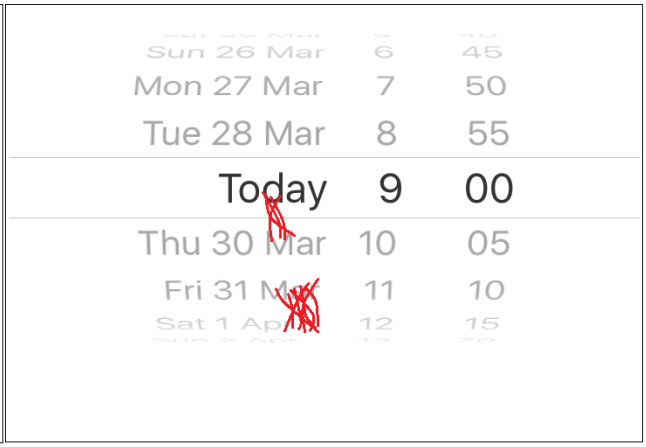
Challenge: Introduce a fluctuation in the way the selection wheel spins.

A common user interaction element in mobile apps is the spinning selection wheel for dates, time, numbers, etc. This is often used when entering information such as a new destination account for money transactions.

BioCatch collects passive measures related to spinning the wheel (speed, stopping strategy, corrections towards the end), but also introduces subtle fluctuations that help us see how the user subconsciously reacts.



User 1



User 2

User 1: The challenge is injected, and the wheel spins slowly (not kinetically). The user compensates by a few long and continuous "pushes" to spin the wheel, and adds two powerful strokes in the other direction for fine-tuning and final targeting.

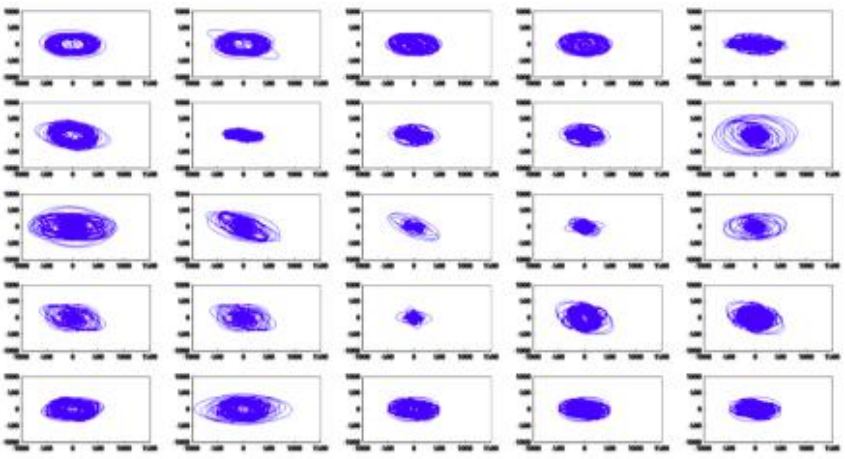
User 2: The challenge is injected, and the wheel spins slowly (not kinetically). The user compensates by many small and short "pushes" to spin the wheel. Afterwards, the user adds several short, concentrated and powerful strokes in the same direction for final targeting.

Disappearing Mouse

Challenge: Hide the cursor.

Users search for the cursor/mouse in very different and unique ways. Some use wide search patterns, others use small ones, some are horizontal while others are diagonal, and certain users always search counter-clockwise. Sometimes users move on a certain learning curve and their responses vary according to their location on the curve. All these can be captured as unique parameters, however, typically this is not practical, because the time required for the user to provide enough relevant mouse movements to accurately authenticate themselves is too long. Invisible Challenges unconsciously "forces" the user to make various mouse movements in a very short time, allowing BioCatch to capture adequate data from the user in 500 milliseconds. This makes it useful for detecting anomalies in user behavior in near real-time.

The example below shows 25 users, each with a slightly different search pattern for a missing cursor.



Invisible Challenges, Invincible Challenges

As a class of technologies, behavioral biometrics offers distinct advantages over other authentication modalities. It is passive, seamless, works in the background and does not require active enrollment. On the other hand, all these characteristics also makes high accuracy hard to obtain. In the world of online transactions, it is critical to keep false positives and user friction to an absolute minimum, while ensuring very accurate fraud alerts. Invisible challenges make this possible.

Invisible Challenges help deliver the promise of behavioral biometrics for continuous authentication and overcome many of the challenges that traditional behavioral and fraud prevention approaches do not address:

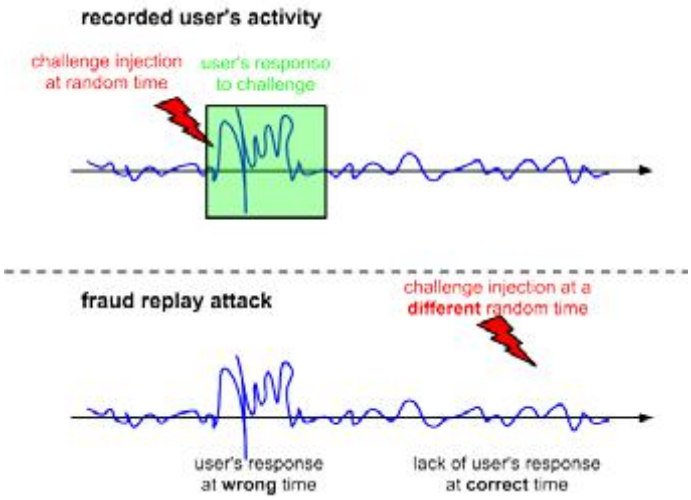
- **Accuracy:** Invisible challenges generate more data, which cannot be captured in other ways. The data captured via Invisible Challenges is intimate in the sense that it divulges cognitive and physiological parameters. In the world of machine learning and deep learning, the amount of data and the quality of data is what determines accuracy. Invisible Challenges not only speed up the data collection process, but the overall detection and false positive rates.

- **RAT and device spoofing detection:** Invisible Challenges can detect an unnatural response or delay indicating a remote connection or Virtual Machine attack; for example, if there are two responses to a single challenge, this can be indicative of a Remote Access Trojan or Man in the Browser attack. With BioCatch, this method of detection can be done without any active enrollment or indexing of the malicious tool, at an Equal Error Rate (EER) of 0%.

- **Robotic detection:** Traditional bot detection involves device fingerprinting, IP address verification, user analytics, and end up being a cat and mouse game that requires learning the behavior of bots and classifying them as harmful or not. Invisible Challenges circumvents all this by requiring the user to compensate subconsciously via hand-eye coordination. Given that bots are automated tools, by nature they ignore the challenges.

- **Malware detection:** Traditional behavioral approaches to malware detection simulates human interaction and compares it to the malware interaction for a given activity. This is problematic because it requires the system to "know" the malware and the learning phase takes some time. By using Invisible Challenges in a randomized way, the malware will not know how and when to respond, and it is therefore not necessary to maintain malware libraries which are inevitably obsolete the moment they are updated. This method has had perfect success to date.

- **Replay attacks:** Traditional behavioral approaches recognize replay attacks by comparing the behavior in a given session against the behavior in a prior session. This is not ideal because replay attacks contain natural "noise" which invariably makes them different from previous sessions but still similar enough to be marked as valid. Invisible Challenges are random in timing, intensity and flavor, so no past activity can be used to produce a legitimate response to the challenge, making BioCatch immune to replay attacks. See figure below.



- **Risk-based authentication:** By definition, risk-based authentication is a method of applying varying levels of stringency to the authentication processes based on the risk profile of the person or the sensitivity of the application being accessed. Because Invisible Challenges are completely transparent to the user, they can be introduced at different junctures, and in different flavors, to increase the accuracy of the detection rate. This makes it easy to establish different business rules *within* an application, so that higher risk activities, like adding a new payee, changing the

phone number for the account, making large transfers, etc. can have specific challenges assigned to them in a random manner, while keeping friction and false positives low.

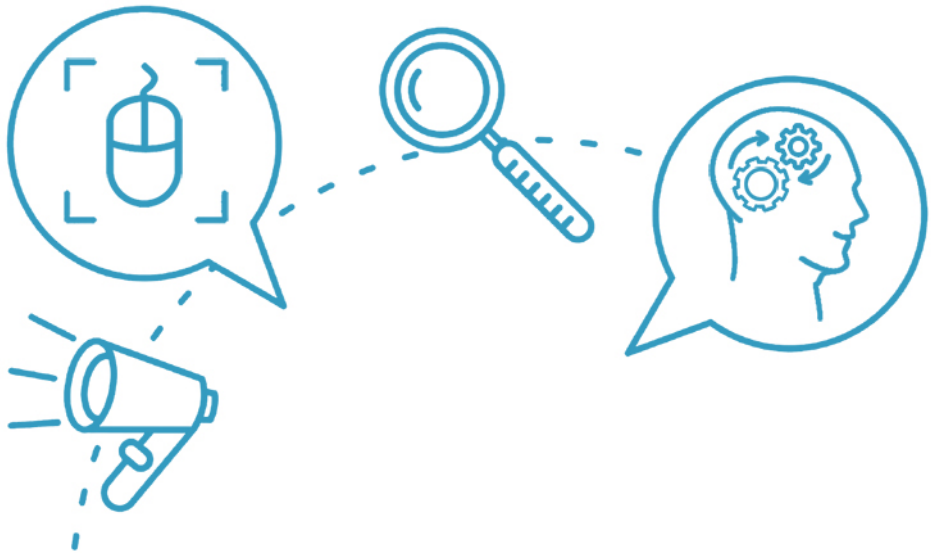
Results and Conclusion – Less Friction. Less Fraud.

As stated earlier, maintaining the balance of identifying real fraud while maintaining low false alarm rates and low user friction is the catch-22 for behavioral biometrics which are passive in nature and do not require an active enrollment.

BioCatch Invisible Challenges optimize this balance. Introducing a single challenge into a session can lower the EER of any by 3%; adding more challenges drives performance exponentially[1]. Critical to this is the timing in which the Invisible Challenges are injected. Using advanced data science and machine learning methods, the challenges are introduced as a form of risk-based authentication prior to crucial online tasks such as: changing payees, transferring large sums of money, updating personal details, card activation and deactivation. Moreover, challenges may also be injected when the system requires more behavioral data to calculate a more deterministic risk score.

This approach ensures very high detection rates with extremely low-rates of false positives by definition, and differentiates BioCatch from other behaviorial biometrics approaches, delivering immediate results and return on investment, without being hostage to the cat-and-mouse game of traditional fraud prevention approaches.

[1] These figures are based on real data coming from the 2 million transactions per month that are monitored by the BioCatch system, together with numerous simulated transaction experiments.



About BioCatch™

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. Banks and other enterprises use BioCatch to significantly reduce online fraud and protect against a variety of cyber threats, without compromising the user experience. With an unparalleled patent portfolio and deployments at major banks around the world that cover tens of millions of users to date, BioCatch has established itself as the industry leader. The company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks and e-commerce websites across North America, Latin America and Europe. For more information, please visit: www.biocatch.com

Contact Us

www.biocatch.com

info@biocatch.com

@biocatch

www.linkedin.com/company/biocatch

BIOCATCH
Less Friction. Less Fraud.