What Is Behavioral Biometrics?

The behavioral profile is based on:

- Behavioral Attributes: such as holding, device orientation, swiping, touch applications and hand-eye coordination.
- Cognitive Attributes: user-computer/device interaction preferences, handedness, hand tremors and input habits.
- Response Attributes: responses to Invisible Challenges, such as curvature compensation, response time and mouse movement patterns.

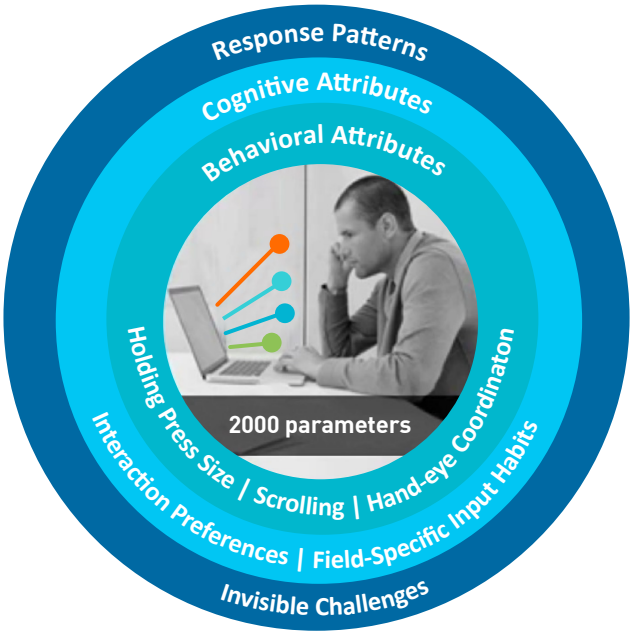
Core Capabilities:

- Identity Proofing: Analyzes how information is entered to detect the use of stolen or synthetic identities in filling out online applications to stop fraud at the source
- Continuous Authentication: Continuously authenticating user sessions in real-time by matching behavioral biometric profiles, and to prevent account takeover and other cyberthreats after the login
- Fraud Detection: Real-time detection of malware, robotic activity and social engineering attacks that are not recognized by traditional fraud prevention methods.

Overview

Behavioral biometrics is a breakthrough cybersecurity technology that identifies people by how they do what they do, rather than by what they are (e.g., fingerprint, face), what they know (e.g. secret question, password) or what they have (e.g. token, SMS one-time code). Behavioral biometrics measures and analyzes patterns in human activities. Historically, these included keystroke patterns, gait, signature and the like. Today's advanced behavioral biometric techniques capture an array of human interactions between a device and an application, such as hand-eye coordination, pressure, hand tremors, navigation, scrolling and other finger movements, etc.

BioCatch's behavioral biometric solutions selects 20 unique features from its 2000 behavioral profiling metrics to authenticate a user — without any disruption in the user's experience. The features are selected according to highly-advanced machine learning algorithms, which are employed to maximize the profiling process. After a few minutes of user activity, a robust user profile is built. Once established, the system can detect anomalies and suspicious behavior at an extremely high-level of accuracy and low rate of false positives.



How Does It Work?

BEHAVIORAL BIOMETRIC PROFILING:

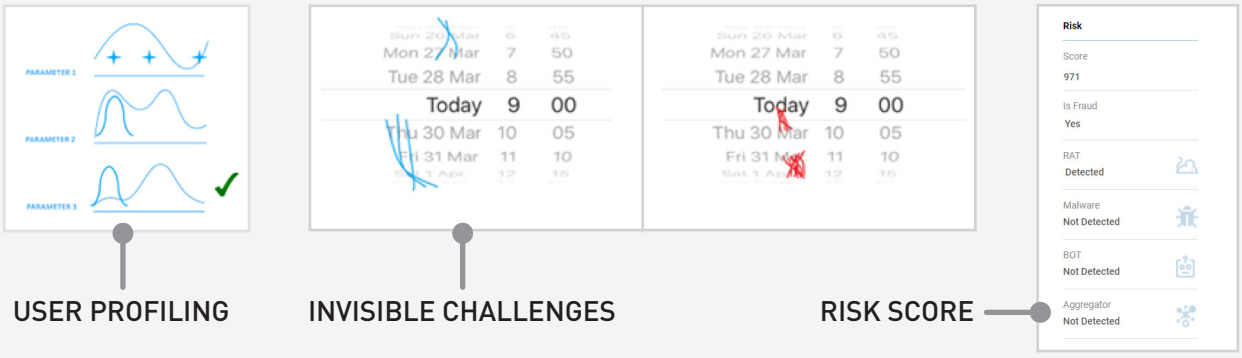
The BioCatch solution collects and analyzes over 2000 behavioral parameters including hand-eye coordination, pressure, hand tremors, navigation, scrolling and other finger movements, etc. To optimize user profiling, the system detects the behavioral parameters that are most strongly associated with the user meaning that, for those parameters, the user does not behave like the rest of the population. Each person's profile is comprised of unique behavioral features and can be linked across devices.

INVISIBLE CHALLENGES: This patented technology, refers 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. Since the user is unaware of the challenge, there is no way for a human or bot to mimic or predict the response.

ACTIONABLE RISK SCORE & THREAT INDICATORS: The BioCatch solution searches for different kinds of fraudulent activity – criminal behavior, malware, bots, RATs, aggregators, etc. – and analyzes the behavior in a session to compare against the user's behavioral profile. Real-time alerts are generated and the activity is logged and visualized in the BioCatch Analyst Station.

About BioCatch

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. 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. For more information, please visit www.biocatch.com.



USER PROFILING | INVISIBLE CHALLENGES | RISK SCORE

BIOCATCH
Less Friction. Less Fraud.

www.biocatch.com | info@biocatch.com | @biocatch | www.linkedin.com/company/biocatch