BIOCATCH™

SOMETHING YOU HAVE VS. SOMETHING YOU ARE:

The Difference Between Device Recognition and Behavioral Biometrics

The ongoing cat-and-mouse game between cybercriminals and security experts has generated a variety of methods to prevent identity theft and reduce friction in the authentication process. Behavioral biometrics upends the paradigm by profiling and analyzing a user's physical and cognitive behavior as opposed to what they have or what they know.

Something You Have: Device Recognition

Device Identification (a.k.a. Device Fingerprinting) attempts to identify a user by collecting device data such as geo-location, IP address, device features and network information. Device recognition capabilities are typically limited to answering the following question: is this a trusted device that is typically used for this user account? Each user account can include multiple devices, and the system decides whether the session is coming from a recognized or new device.

Something You Are: Behavioral Biometric with BioCatch

Behavioral biometrics analyzes a user's physical and cognitive digital behavior to distinguish between genuine users and criminals in order to detect fraud and identity theft and improve customer experience. This is done by profiling user behaviors such as mouse movements, typing cadence, swipe patterns or device orientation and comparing these against a user's historical profile to provide an additional (passive) authentication layer and against population-level behavioral patterns to determine whether the user's behavior is statistically "good" or "bad".

Behavioral Biometrics: How It Works

FRICTIONLESS EXPERIENCE: Current fraud controls often treat customers like criminals, introducing additional friction into the user experience. This is especially true in the online account opening process where applications are deferred for manual review which can incur high operational costs. Behavioral biometrics delivers better detection of account opening fraud by understanding behavioral intent to identify illegitimate activity versus that of a legitimate applicant. By monitoring user behavior in addition to their location or device to assess a session's risk, false declines are signifcantly reduced. The BioCatch solution is designed with customer experience in mind. It is invisible to the end user, allowing consumers to go about their banking activities while also being guaranteed maximum security. With the right tools in place, you can ensure that customer experience is prioritized, and the balance between trust and risk is properly calculated and aligned to business priorities.

CONTINUOUS PROTECTION: Providing continuous protection is not only about reducing fraud losses but building trust in digital interactions. Unlike other fraud solutions, BioCatch provides truly continuous protection by collecting and analyzing data throughout the entirety of a session, so even the most subtle changes do not go undetected.

The BioCatch Risk Engine is powered by machine learning algorithms that analyze physical and cognitive digital behavior of users across web and mobile channels. The model takes into consideration real-time physical interactions such as keystrokes, mouse movements, swipes, and taps. This data is used to profile users on three levels:

Behavioral Biometrics: Profiling a user against their historical profile based on physical traits such as typing, mouse movement, swiping and press, to detect anomalies, including human versus automated or bot activity.

Cognitive Analysis: Profiling a user against population-level behavioral patterns based on cognitive choices, such as how they input data or navigate throughout a session, to identify genuine vs. criminal behavioral indicators.

Behavioral Insights: Combines user and population level profiling to determine user intent and emotional state in context of the activity to detect complex situations indicating high levels of risk. For example, detecting false claims about user age or actively operating inside the online account under the guidance of a voice scammer which is presented with signs of duress and distraction.

BioCatch analyzes each user session and delivers a risk score based on this deep user behavioral profiling. Depending on the risk score, organizations can initiate additional actions such as requiring step-up authentication or manual review. BioCatch also provides organizations with the top threat indicators to allow further visibility into risk. Confirmed fraud feedback is incorporated to continually enhance the accuracy of the model and adapt to new and emerging attacks. Based on analysis of over a decade of data intelligence, BioCatch offers several risk models out-of-the-box to provide immediate value to customers.

	Device Recognition	Behavioral Biometrics
SPOOFING:	It's easy to spoof a user's device. Spoofing techniques are commonplace and render device identification impractical for authentication.	BioCatch works irrespective of device type, analyzing user behavior, which relates to the interaction patterns with a given application/device.
ADVANCED ATTACKS:	Device-based detection is unable to detect sophisticated attacks such as Social Engineering Scams and automated attacks including Man in the Browser/ Man in the Middle, BOT and Remote Access Tool (RAT) attacks. In addition, there is no protection for account opening fraud use cases for unknown devices.	The BioCatch platform continually collects behavioral data throughout the session to detect subtle changes. Even if a genuine user is logged in and is being socially engineered, subtle session anomalies will indicate the presence of a RAT or evidence of the user being scammed.
FALSE ALARM RATE:	Device-based detection generates many false positives (30-50%) due to geo-location sensitivity. For example, a user traveling abroad and using a new device (PC or mobile) becomes suspicious and can be potentially denied access.	BioCatch analyzes user behavior to continually authenticate users against previous behaviors and distinguish between legitimate and cybercriminal behavioral patterns. BioCatch's multi-layered appraoch to analysis ensures high detection and low false positive rates.
ACTIONABILITY:	Relying on device ID to determine the appropriate action is limited due to the number of users using new devices and new locations. Legitimate users using unknown devices will be introduced to friction and considered higher risk.	BioCatch prevents fraud in real time by identifying behavioral anomalies and returning actionable alerts and risk scores.

BioCatch pioneered behavioural biometrics, which analyzes an online user's physical and cognitive digital behaviour to protect users and their data. Today, customers around the globe leverage BioCatch's unique approach and insights to more effectively fight fraud, drive digital transformation and accelerate business growth. With nearly a decade of data, over 50 patents and unparalleled experience analyzing online behaviour, BioCatch is the leader in behavioural biometrics. For more information, please visit www.biocatch.com

BIOCATCH™ www.biocatch.com info@biocatch.com @biocatch www.linkedin.com/company/biocatch

Tel Aviv | New York | Boston | London | São Paolo | Santiago | Mexico City | Melbourne | Mumbai