BIOCATCH™
Less Friction. Less Fraud.

From Login to Logout: Continuous Authentication with Behavioral Biometrics

April 2018

BIOCATCH
Less Friction. Less Fraud.

Continuous Authentication with Behavioral Biometrics

Contents

Introduction: 100% of Fraud is Done in Authenticated Sessions

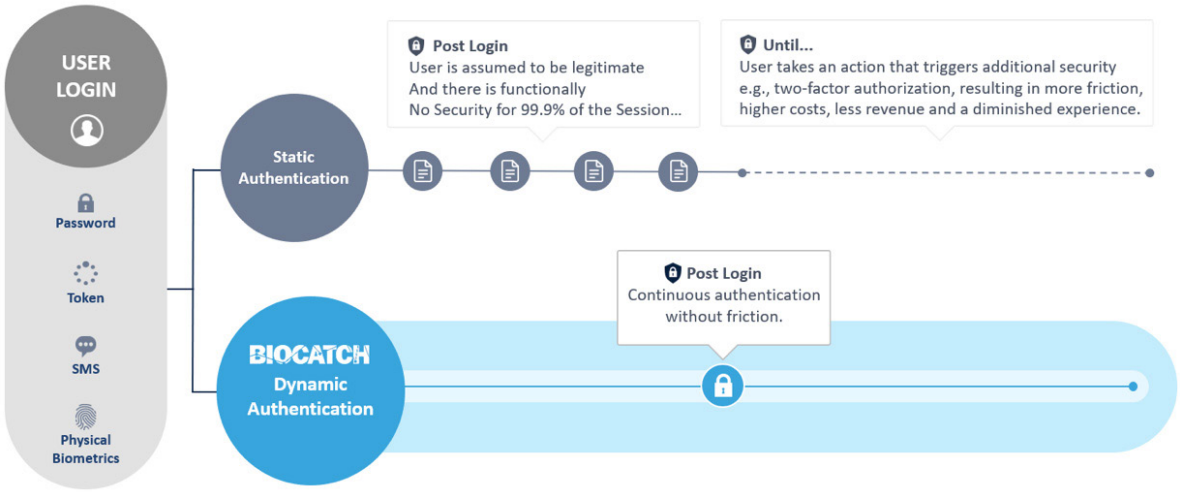
In recent years, a growing number of organizations have employed two-factor authentication (2FA) as a primary safeguard mechanism. They all share the notion that requiring a second security layer will be instrumental in reducing data breaches and identity theft. Two-factor authentication is based on the fundamental assumption that at least two out of three authentication factors are used in the process ("something you know, something you have, something you are"). 2FA is not a new security measure, nevertheless, it is in extensive use, despite the growing recognition that it is not so effective.

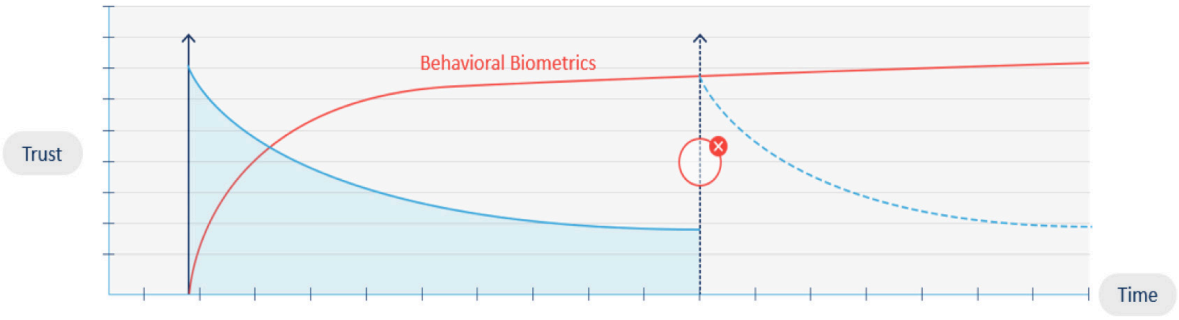
Bypassing Two-Factor Authentication

Hackers and cyber-criminals use various attack methods to bypass 2FA safeguards and commit fraud. The prevalence and sophistication of these attacks has increased every year, resulting in astronomical financial losses. In fact, according to October 2017 Global Fraud Index study released by PYMNTS.com study, account takeover losses have jumped 45% in Q2/3 2017 alone, resulting in $3.3 billion in losses, Among the techniques that fraudsters use to bypass 2FA defenses are: credential theft, Man in the Middle (MitM)/Man in the Browser (MitB) and social engineering, the latter accounting for almost 50% of all bank account takeover cases, according to Cifas UK. And with the continued prevalence of data breaches and personal information that is available for sale on the dark web, the risk continues to grow.

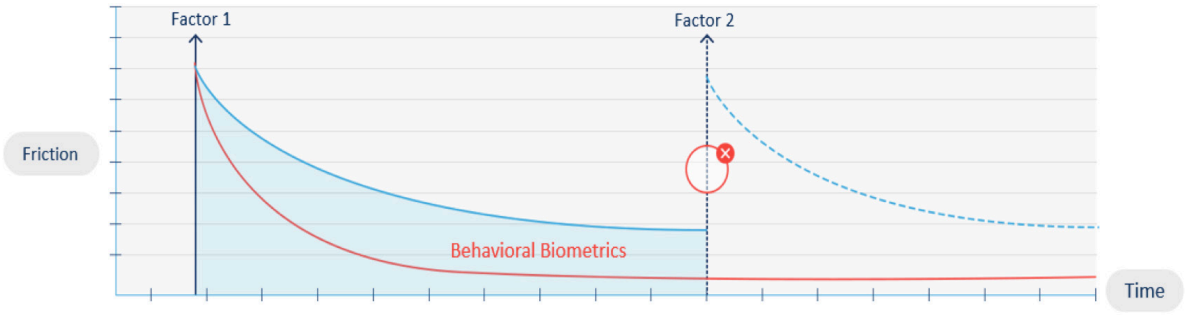
Static Login vs. Continuous Authentication

Part of the problem with two-factor authentication is that it is based on static factors, like PINs, passwords, credentials, physical biometrics or a combination of these. So even if the initial authentication is valid and done by the legitimate user, by definition, given the sophisticated hacker techniques outlined above, the integrity of the session gradually erodes over time, and the only way to restore it is by introducing additional authentication factors. However, traditional factors like fingerprints, facial recognition and passwords can cause disruption and friction, which will degrade the user experience. The optimal solution to this problem is using a safeguard that increases trust and avoids friction during the session, that can run passively in the background and provide escalation triggers based on risk.





Trust: When authentication factors are introduced during a session, the level of trust is high and then slowly decreases until the next factor is introduced. On the other hand, behavioral biometrics continuously authenticates the user and provides a consistent level of trust.



Friction: Authentication factors cause friction once introduced, whereas, behavioral biometrics continuously monitors the session without disrupting user experience.

Continuous Authentication with Behavioral Biometrics

With cyber-attackers becoming much more sophisticated, security measures must get smarter too. The key is to implement security measures that continuously monitor and test the authenticity of users in ways that are difficult to replicate. Many experts and market leaders agree: behavioral biometric profiling is the only effective way to achieve this level of security.

BioCatch provides a passive and continuous authentication layer that maintains the integrity of sessions without any friction or disruption. Behavioral biometrics runs in the background seamlessly. In the event of anomalous behavior, real-time alerts and analyses are provided to support the customer's authentication policy. This capability provides ongoing security throughout the session and guides the customer to escalate only in which the anomaly rate is very high.

Continuous Authentication - Benefits

- Builds user confidence and device trust during sessions.
- Continuously authenticates the user to prevent account takeovers through malware, bots, aggregators, remote access Trojans and social engineering schemes.
- Reduces friction-related costs caused by false positives, authentication escalations, and step-ups.
- Reduces the loss of users due to a bad experience and session abandonment.

Mapping and monitoring these behavioral patterns, throughout the users' time within the application, continuous authentication can indicate fraudulent behavior that occurs after the login, that is, after the two-factor authentication has been validated. With no disruption of user experience, this method also reduces the risk of false alarms, as opposed to traditional device ID or IP address validation and identifies threats immediately. This means stopping fraud in real-time and protecting consumers against the range of cyber threats. Moreover, this approach can be used for risk-based authentication that triggers escalations only when determined absolutely necessary after behavioral biometric assessments during the session.

BioCatch has established itself as the market leader, which provides the most advanced continuous authentication capabilities.

How Does It Work?

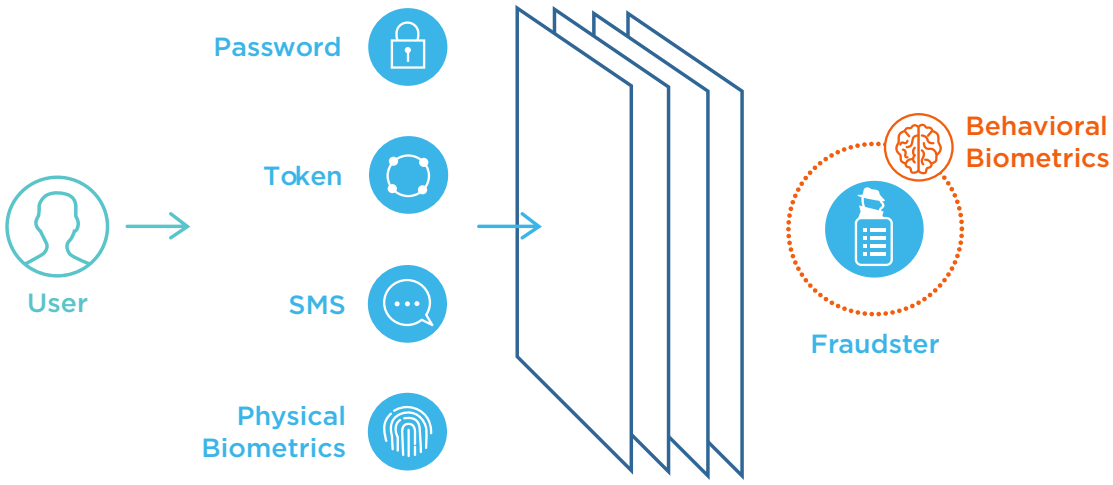
BEHAVIORAL BIOMETRIC PROFILING: The BioCatch solution collects and analyzes over 2000 behavioral parameters including hand-eye coordination, pressure, hand tremors, navigation, scrolling and other finger movements, etc. To optimize user profiling, the system detects the behavioral parameters that are 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 approach, 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, vishing, social engineering schemes – 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.

How BioCatch Prevented a Vishing Attack with Continuous Authentication

A user received a phone call from a supposed cable provider representative that through deceptive social engineering extracted sensitive financial information. A few minutes later, the victim received another phone call from a supposed bank representative, informing that her account was compromised by fraud. Using the personal details extracted from the first phone call, the fraudster convinced the victim into transferring money from her account to a "new account". During the online session, BioCatch detected various anomalies which suggested it was the correct user who was not behaving in a consistent manner, sent an alert in real time and prevented the transfer from going through.



Since the vast majority of cyber defenses are focused on the login process, once the authentication method is circumvented, the fraudster can proceed unchallenged to take over the user's account. Behavioral biometrics provides a post-login security layer that is 100% seamless and frictionless.

Stronger User Confidence, Less Fraud and Friction

- User trust is built throughout the session to provide a high-level of confidence continuously, even after the introduction of other authentication factors.
- Friction is minimized, providing a 100% seamless and frictionless user experience. This means applying step-up authentication requirements based on risk, and de-escalating where there is a high assurance of the proper user inside a session.
- Actual fraud savings as well as significant operational savings due to fewer escalations to call centers.

BIOCATCH
Less Friction. Less Fraud.

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

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.