Real-Time Fraud Detection Through Continuous Authentication

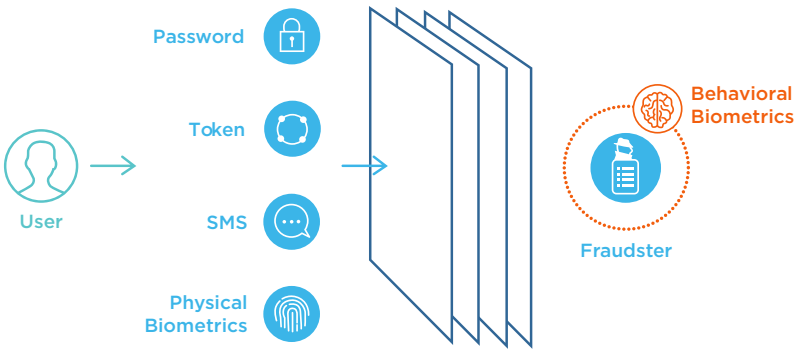
Behavioral Biometrics for Continuous Authentication - Benefits

- Builds user confidence and device trust during sessions.
- Provides a 100% frictionless and seamless user experience.
- 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.

Two-factor authentication typically relies on at least two out of three authentication factors to validate identity ("something you know, something you have, something you are"). According to recent surveys, more than 90% of organizations are implementing two-factor authentication in some capacity, based on the assumption that requiring a second security layer will be instrumental in reducing data breaches and digital identity theft.

Bypassing 2FA

Recently, however, hackers and cyber-criminals have used various attack methods to bypass 2FA safeguards and commit fraud. Unfortunately, these attacks have increased every year, resulting in astronomical financial losses. Fraudsters use numerous methods and techniques to bypass 2FA defenses, namely: social engineering, credential theft and MitM/MitB attacks.



Attack Methods:
1. Social Engineering (Phishing/Spear-Phishing)
2. Credential Theft
3. MitM/MitB Attacks

Continuous Authentication with Behavioral Biometrics

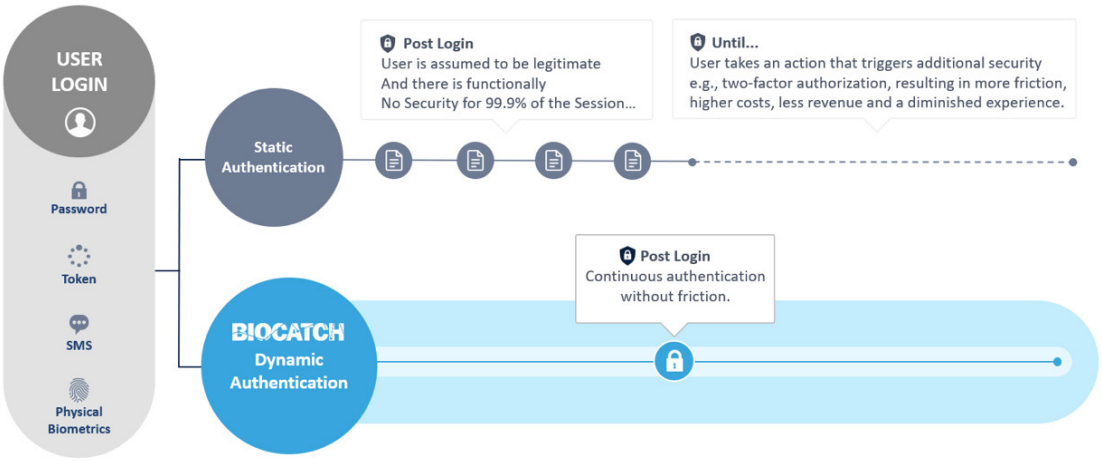
With cyber-attackers becoming much more sophisticated, security measures must get smarter too. The key is to implement security measures that continuously monitor and test the authenticity of users in ways that are difficult to replicate. Many experts and market leaders agree: behavioral biometric profiling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

BioCatch behavioral biometrics provides a continuous authentication layer that works passively in the background to maintain the integrity of online sessions without any friction or disruption. In the event of anomalous behavior, real-time alerts and analyses are provided to support the customer's authentication policy.

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 the 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 a full range of cyber threats. Moreover, this approach can be used for risk-based authentication that triggers escalations when anomalies are detected inside a session.

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.



BIOCATCH
Less Friction. Less Fraud.

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