BioCatch

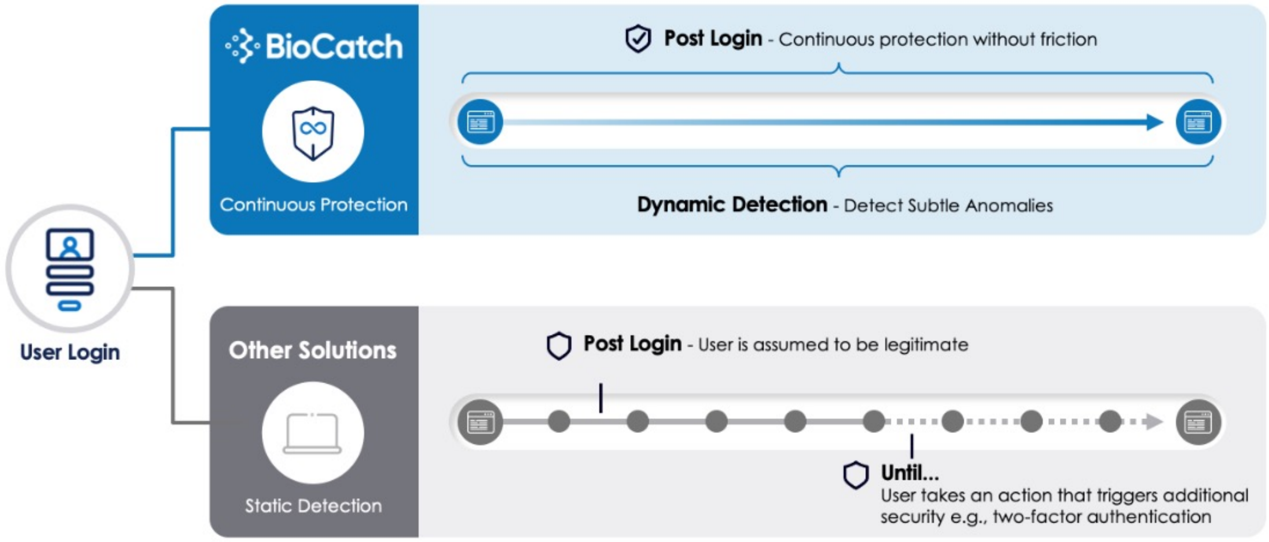
Data Sheet

Protection that Never Sleeps with BioCatch

Despite increased investments in fraud protection, organizations continue to experience astronomical financial losses, exposing gaps in traditional controls. According to PwCs 2020 Global Economic Crime and Fraud Survey, fraud cost participating organizations $42 billion over a period of 24 months[1]. In our digital-first world where cybercriminals rapidly develop new methods to perpetrate fraud and identity theft, continuous protection is key.

BioCatch Continuous Protection

BioCatch takes fraud protection to a new level. Contrary to traditional authentication and identity verification controls, the BioCatch platform passively determines whether a user is genuine continuously throughout an entire session, not just at a single point in the digital flow such as at log in or point of payment, to provide organizations with a greater breadth of coverage.


BioCatch
Continuous Protection
Post Login - Continuous protection without friction
Dynamic Detection - Detect Subtle Anomalies
User Login
Other Solutions
Static Detection
Post Login - User is assumed to be legitimate
Until...
User takes an action that triggers additional security e.g., two-factor authentication

The BioCatch Continuous Protection Advantage

See All

Continuously monitor user behavior

Detect Early

Identify risk before fraud occurs

Drive Action

Consume BioCatch insights in real time

BioCatch Continuous Protection Empowers Organizations to:

identify Risk Before Fraud Happens

Oftentimes before making a fraudulent payment or transfer, cybercriminals carry out an initial test or reconnaissance session. For example, cybercriminals typically conduct login-only sessions to validate a user's credentials, verify funds, test their attack tool, or gather information about the account or user to later manipulate the victim as part of a social engineering scam. While this activity traditionally goes unnoticed, with continuous session visibility, organizations can act on these early signs of fraud.

Detect Sophisticated Attack Methods

Many of today's most sophisticated fraud attack methods can only be detected when meticulously monitoring for extremely subtle deviations in user behavior. For example, in a social engineering voice scam where the user's behavior will highly correlate with their past activity, only careful and continuous monitoring will surface subtle anomalies that suggest a person is conducting a transaction under the influence of cybercriminal.

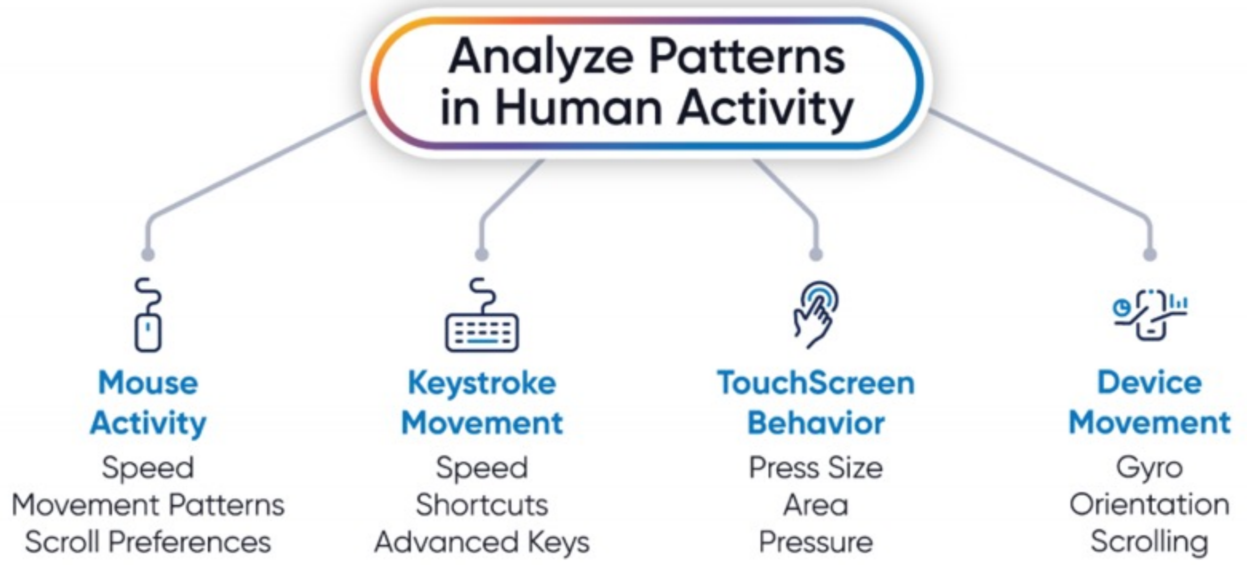
Introduce Adaptive Risk-Based Experiences

In the event behavioral anomalies or popular attack tools are detected, organizations can modify the customer experience in real time based on the level of risk and indictors surfaced. For example, in the event a remote access tool (RAT) or signs of social engineering are detected, the organization can limit the functionality available to the user or implement a temporary freeze on payments while they investigate.

Platform Components

End-to-End Session Visibility

The BioCatch platform continuously monitors a user's physical and cognitive behavior from login to logout. By capturing a vast realm of digital activity including how the user moves their mouse, types, swipes, and navigates, the solution eliminates blind spots, providing organizations with the level of visibility they need to detect the most subtle signs of an imposter and determine the appropriate course of action.



Analyze Patterns in Human Activity

Mouse Activity
Speed
Movement Patterns
Scroll Preferences

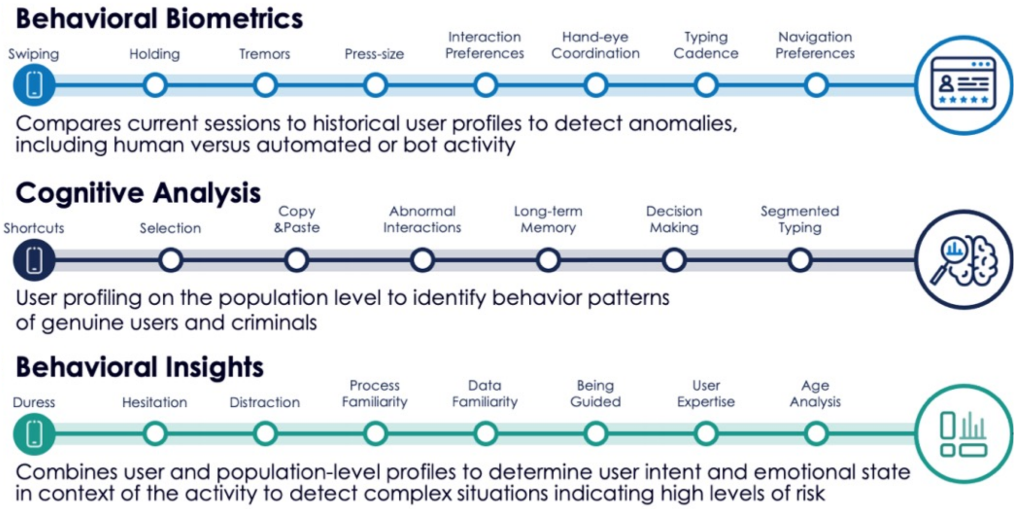
Keystroke Movement
Speed
Shortcuts
Advanced Keys

TouchScreen Behavior
Press Size
Area
Pressure

Device Movement
Gyro
Orientation
Scrolling

Analysis that Goes a Step Beyond

The BioCatch platform analyzes digital interaction behavior at both the user and population level to surface user behavioral anomalies and patterns of genuine vs. criminal activity. This level of analysis enables the solution to determine user intent and emotional state in order to provide coverage against the most complex fraud attack methods, such as social engineering voice scams.



Behavioral Biometrics

Compares current sessions to historical user profiles to detect anomalies, including human versus automated or bot activity

Cognitive Analysis

User profiling on the population level to identify behavior patterns of genuine users and criminals

Behavioral Insights

Combines user and population-level profiles to determine user intent and emotional state in context of the activity to detect complex situations indicating high levels of risk

Real-Time Fraud Alerting

The BioCatch push API implementation enables proactive notification of high risk to empower organizations to act on the earliest signs of fraud. While the BioCatch platform can be configured to deliver a risk analysis at critical points in the digital flow to support real-time decision making, such as determining whether a payment should be allowed or denied, push API notifications allow organizations to feel confident their users are fully protected in scenarios where a decision is not required, such as when a user simply logs into their account, checks their balance, and logs out. Organizations define when a push API notification is triggered within the BioCatch Rule Manager according to their unique risk appetite and strategy.

> *"The competitive advantage that BioCatch offers is that the solution goes beyond basic comparisons of biometric templates to run-time data, using applied research, it abstracts from these behavioral elements in order to perform cognitive analysis. These innovative techniques provide unparalleled insights into legitimate and malicious behavior, thereby reducing the risks of fraud to their customers."*
>
> ***John Tolbert***
> *KuppingerCole Analyst*

BioCatch

BioCatch pioneered behavioral biometrics, which analyzes an online user's physical and cognitive digital behavior 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 behavior, BioCatch is the leader in behavioral biometrics. For more information, please visit **www.biocatch.com**

www.biocatch.com
E: info@biocatch.com
@biocatch
in /company/biocatch

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