BioCatch

Solution Brief

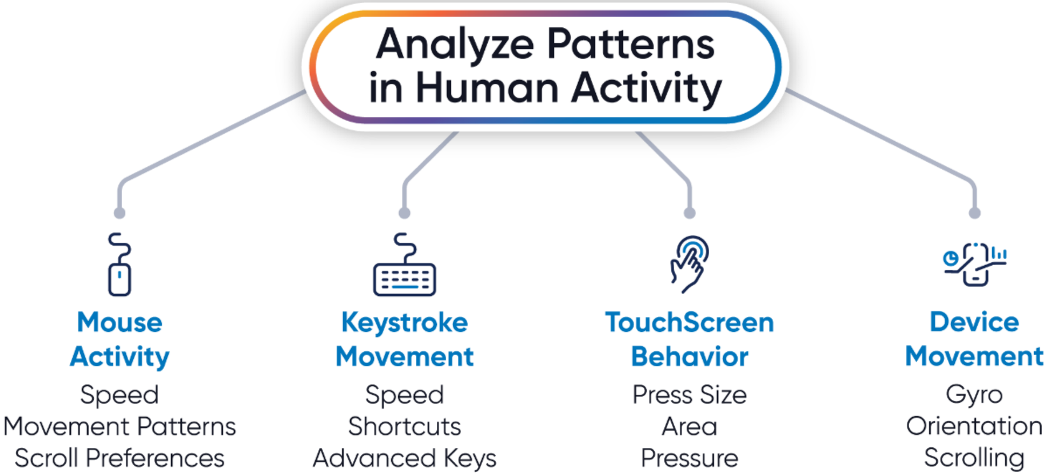
BioCatch Account Takeover Protection

Building Trust and Safety with Behavioral Biometrics

Account Takeover attacks are on the rise as cybercriminals continue to develop new methods and tools to take over accounts from afar and automate fraud. Despite the widespread adoption of traditional protection solutions, such as those that rely on two-factor authentication and device ID, fraud continues to occur in fully authenticated sessions. Malware, Remote Access Tool attacks, sophisticated social engineering scams, and other creative account takeover methods have proven to successfully bypass common cybersecurity safeguards, costing financial institutions millions of dollars per year and damaging customer confidence.

Protection That Never Sleeps

BioCatch Behavioral Biometrics delivers continuous protection without disruption by passively monitoring a user's physical and cognitive behaviors from login to logout. Contrary to solutions that conduct a point-in-time analysis, the BioCatch platform leaves no behavioral indicators behind. By continuously analyzing a vast realm of digital activity including how the user moves their mouse, types, and swipes, the BioCatch platform generates powerful behavioral insights, giving organizations the visibility they need to prevent more fraud and increase trust.



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

Transforming Behavioral Data into Powerful Insights

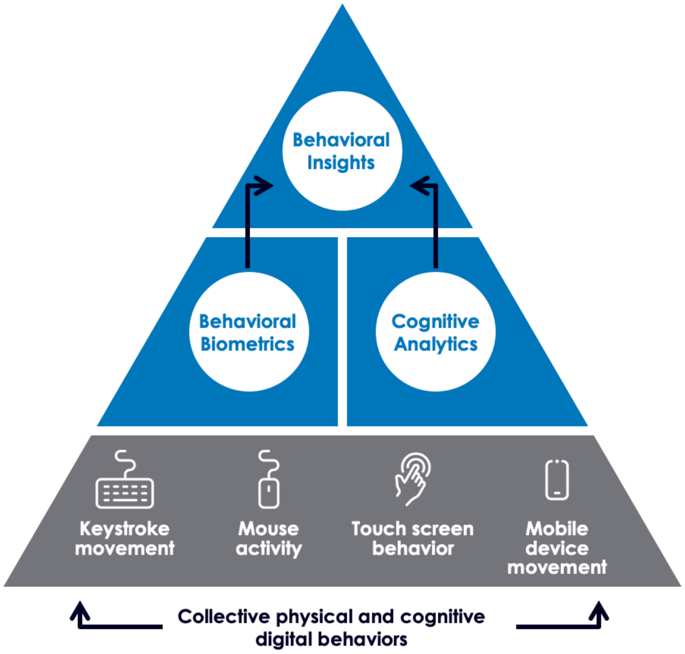
BioCatch risk models leverage innovative research and a decade of behavioral data to distinguish between genuine users and cybercriminals. Using a multi-layered approach to analysis, BioCatch empowers organizations to detect more fraud without worrying about disrupting the experience for genuine customers.

The BioCatch platform determines a session's risk level by analyzing a user's digital behavior **on three levels:**

Behavioral Biometrics: The BioCatch platform compares a user's physical behavior, including navigation preferences, hand-eye coordination, and press size, against the user's historical profile to detect anomalies, including human versus automated or bot activity.

Cognitive Analysis: The BioCatch platform compares a user's cognitive behavior, including the use of shortcuts, long-term memory, and navigation patterns, against population-level profiles to identify genuine and criminal behavioral patterns.

Behavioral Insights:
The BioCatch platform determines user intent and emotional state by surfacing behaviors that align with complex fraud threats, such as social engineering voice scams, including hesitation, dictation, duress, and more.



Tackling the Most Sophisticated Fraud Threats

Through continuous session visibility and advanced profiling capabilities, the BioCatch platform detects even the most subtle signs of criminal activity, providing a greater breadth of coverage against the **most sophisticated account takeover attacks including:**

- **Bots & Aggregators**
- **Malware**
- **Social Engineering Voice Scams**
- **Remote Access Tools**
- **Mobile Emulators**
- **Stolen Account Credentials**

The BioCatch solution detects key behavioral indicators that align with popular attack methods, such as automated patterns which can indicate account takeover via bot or malware, and surfaces anomalies that can suggest a human imposter, such as dominant hand change and expert user patterns.

Reduce Fraud. Increase Trust.

Effectively manage risk across digital channels to build customer trust and confidence

Instantly Gain Actionable Insights

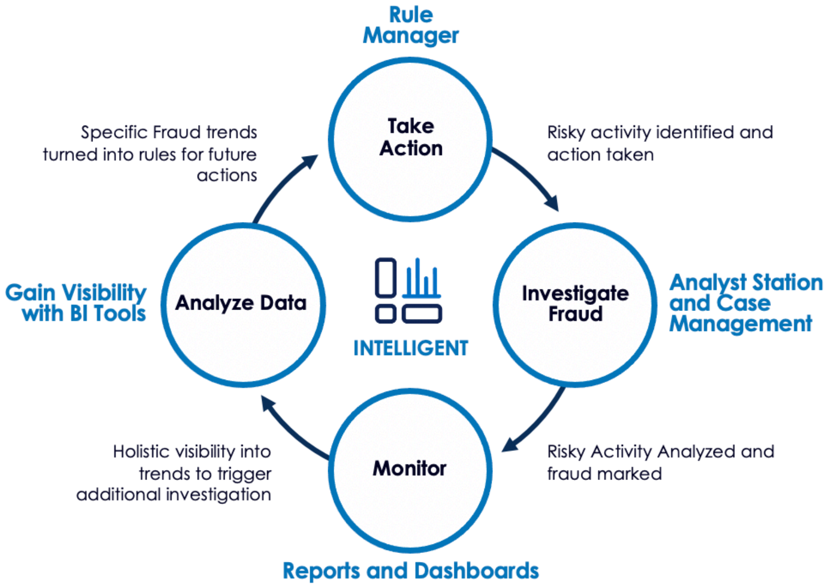
Leverage unique behavioral insights to determine the appropriate course of action

Improve Customer Experience

Significantly reduce false positives and abandonment to banish friction and boost user experience

Driving Real-Time Action

BioCatch Account Takeover Protection delivers profound visibility into fraud risk through a powerful set of platform tools; these tools enable fraud teams to drive real-time action and investigate fraud incidents with ease. Organizations that prefer to perform their own analysis can consume BioCatch risk scores, threat and genuine indicators, and raw data via API.


Rule Manager
Take Action
Risky activity identified and action taken
Analyst Station and Case Management
Investigate Fraud
Risky Activity Analyzed and fraud marked
Monitor
Reports and Dashboards
Holistic visibility into trends to trigger additional investigation
Gain Visibility with BI Tools
Analyze Data
Specific Fraud trends turned into rules for future actions
INTELLIGENT

Change the Game for Your Business

67%

Decrease in Social Engineering Fraud

Top LATAM bank reduces social engineering fraud targeting mobile users by 67% just months after deployment

£1.6M

Fraudulent Transaction Prevented

Top 5 UK bank prevents a £1.6M transaction attempted using sophisticated malware with remote access functionality

95%

Reduction in Friction

A Top 5 UK bank reduces friction by 95% during the credential re-enrollment process with a risk-based approach

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 60 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