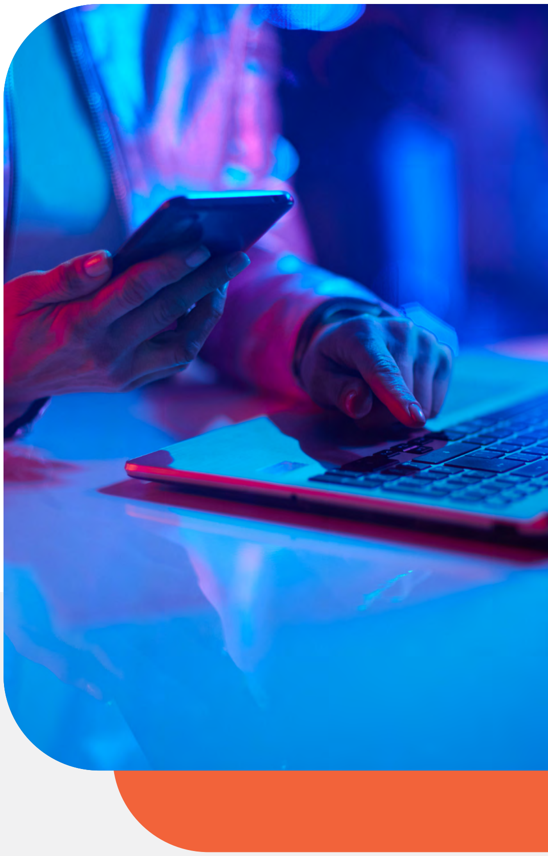
SOLUTION BRIEF

BioCatch CONNECT



The Leader in Digital Fraud and Response

With more than 11 years of research and development, and founding the use of behavioral insights to protect customers from fraud, BioCatch has grown to become the global leader in digital fraud detection and response powered by behavioral biometric intelligence.

BioCatch by the Numbers

7B+	250M+	$2.3B
Sessions continuously protected per month	Users protected	Fraud losses prevented in 2022

Be the Hero of Your Customers Story

At BioCatch, we help the world's largest, most recognizable brands build trusted relationships with their customers by keeping them safe from digital fraud. We believe behavior has become the only element of our digital identities that is truly, and uniquely, human.

Our People are our Power

We are a data science company powered by incredible people who fuel our passion for helping you keep your customers safe from fraud. Our team brings fraud, AML, and cyber practitioner experience from more than 50 of the world's largest financial institutions and spans more than 22 time zones. Our unique, holistic service and support model provides each of our 100+ customers with a team of threat analysts, global advisors, and solution engineers to ensure rapid time to value, decreased fraud incidents, and a better customer experience across all of your brand's products.

The Difference is Human

At BioCatch, we believe customers are an important part of the solution. We believe getting to know them, their idiosyncrasies, their digital habits – the when, how, where, and why they bank – is all part of their unique journey and relationship with your brand. Customers do not have to be the weak link in your fraud prevention and anti-money laundering strategy.

In partnership with our 100+ customers, we have proven that if we pay close attention to the behavior and intent behind the biometrics, device, geo-location and other machine-created signals, we can empower you to deliver your customers a seamless digital banking experience free from fraud and safe from criminals.

And for you, and your fraud, AML, and cyber security teams, we deliver meaningful reduction in fraud, ease the burden on your operations teams and proactively identify bad actors and accounts while connecting you to the most curious, experienced, and thoughtful community of Fraud Fighters on the planet.

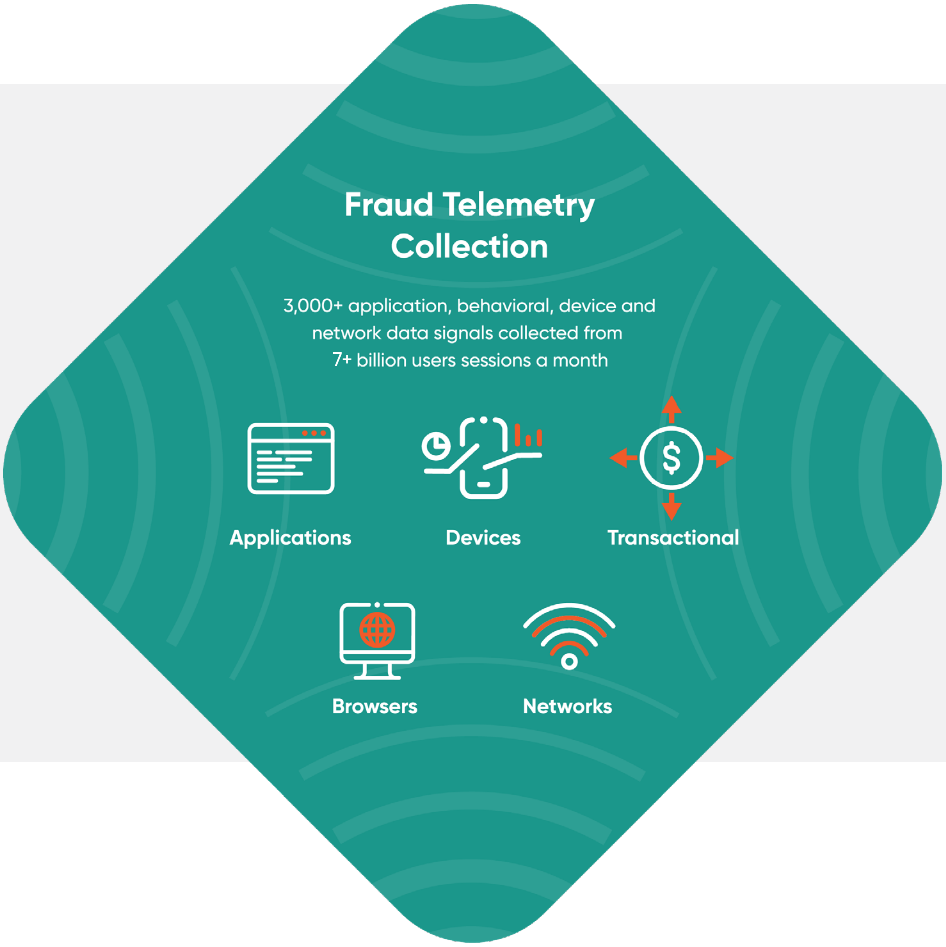
SOLUTION BRIEF

BioCatch CONNECT

BioCatch Connect™ is a first-of-its-kind converged digital fraud, anti-money laundering and impersonation detection solution purpose-built to proactively detect and identify traditional and emerging fraudulent activities and actors targeting customers of the world's largest banking and financial services organizations.

It offers digital fraud and AML teams next-generation insight and analysis in support of an ever-growing number unique use cases across five foundational solution and compliance models: account acquisition; account takeover; scam identification; money laundering; and inherence analysis for strong customer authentication (SCA).

BioCatch ConnectTM is powered by an unmatched collection of machine learning engines, including rules, supervised, unsupervised, and deep learning, that ingest thousands of signals continuously and simultaneously throughout each and every customer's online session. This process of collection, validation, and analysis of signals across the different fraud types and uses cases is powered by **BioCatch's Continuous Behavioral Sequencing™ (CBS) technology**.


Fraud Telemetry Collection
3,000+ application, behavioral, device and network data signals collected from 7+ billion users sessions a month
Applications
Devices
Transactional
Browsers
Networks

Data At Scale

The foundational element of BioCatch Connect™ is fraud telemetry collection. The fraud telemetry module utilizes a lightweight mobile and web SDK to continuously collect thousands of application, behavioral, device, network, and transactional signals from more than eight billion individual user sessions. Whether the customer is using a web browser to access their finances online or directly from a banking application on the more than one billion mobile devices in the BioCatch network, data elements are collected to analyze session activity and protect them from becoming victims of fraud.

Continuous User Validation and Recognition

Deviations in a user's normal behavior consistent with known fraudulent behavioral attributes, such as hesitation, abnormal navigation within an application, the presence of remote access tools, copy and paste activity, typing cadence, an active phone call during a session, and hundreds more are used to evaluate the authenticity of each user during a unique session.

Individuals' needs and behaviors can change slowly or quickly depending on their purpose, need, or desire. These changes are reflected in our analysis, and based on the contextual data, only BioCatch's CBS technology can most accurately determine if these changes are legitimate, permanent, or fraudulent and provide highly accurate risk scores specific to that user's session attributes.

Continuous Behavioral Sequencing

Behavioral data science analyzes more than 300 unique user actions and cognitive patterns

- Age Analysis
- Being Guided
- Distractions
- Copy & Paste
- Active Phone Call
- Selection

Predictive Intelligence

Intent signals inform AI models that validate user motivation and identify risk of potential fraud

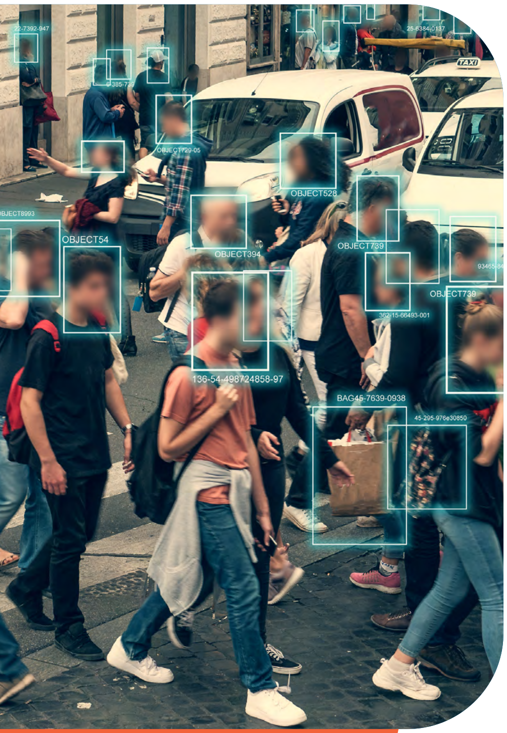
- Risk Score
- Risk & Genuine Factors
- Data Points
- Threat Indicators

Optimize fraud and AML response

As BioCatch continues to innovate and build the latest predictive fraud and AML models, the data collection, consumption, and output sharing are top priorities. Once the appropriate data has been collected and sequenced, it is fed through the BioCatch Predictive Intelligence module to generate outputs, such as threat indicators, risk and genuine factors, risk scores, and unique data points. These outputs, paired with our investigation tools, allow financial institutions to validate user intent and identify potential fraud. This predictive and proactive approach can mitigate the highest amount of risk while maintaining a frictionless customer experience.

BioCatch CONNECT

SOLUTION BRIEF



Predictive Intelligence Tools

BioCatch delivers actionable intelligence and empowers financial institutions to align action with risk and minimize disruptions. In addition to the visibility provided through the risk score and indicators of fraud, the BioCatch platform enhances investigations and decision-making with the following customer investigation and intelligence tools:

Analyst Station: Provides deep visibility into the sessions including video playback to study, determine, and learn about new trends and attack vectors.

Rule Manager: Enables the creation of configurable rules to automate actions based on risk scores and indicators. Easy to configure. And easy to fine tune.

Insights Query Engine: IQE empowers customers analyse and share structured data across multiple teams to enable quicker, deeper analysis.

BioCatch Scout: The latest addition to our predictive intelligence tool belt. Scout for Mule Account Detection is a link analysis tool that graphically showcases the money laundering and mule account problems that banks and FIs face. The tool utilizes Viva Graph technology to help fraud fighters easily visualize, connect, and prioritize their investigative efforts.

Integration with In-house Tools: Organizations who prefer to work with existing fraud tools can consume our behavioural insights in their own established fraud management tools and systems through a robust set of push APIs.

Foundational Solutions

Whether new account fraud detection, account takeover, the ever-growing types of scams or the multi-faceted network of money laundering syndicates, we are focused on helping financial institutions protect their customers:

Account Opening Protection: Account Opening Protection from BioCatch analyzes the data and interactions on a new application to determine if the request is genuine or fraudulent. This process reduces friction for true customers and protects you from fraud and reputational losses.

Account Takeover Protection: BioCatch Account Takeover Protection continuously monitors web and mobile sessions for user application, behavioral, device, and network anomalies and applies advanced risk models to expose a broad range of account takeover threats that legacy fraud prevention controls miss.

Mule Account Detection: Identify money laundering activity and proactively detect mule accounts before the funds are moved. Mule Account Detection can help mitigate financial, reputational, and regulatory risk.

Social Engineering Voice Scam Detection: Given the prevalence of modern scam techniques targeting the customer, leveraging behavioral insights has become more important than ever. Using these additional insights in combination with traditional device and network controls enables financial institutions to intercept the scam before the funds are transferred and the damage is done.

Inherence Analysis for Strong Customer Authentication (SCA): Enhance your existing SCA-compliant solution by adding an extra level of behavioural protection. This integration increases your overall defences against payment fraud without increasing customer payment abandonment.

About BioCatch

BioCatch is the leader in Behavioral Biometrics which analyzes an online user's physical and cognitive digital behavior to protect individuals and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of analyzing data, over 60 patents and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit **www.biocatch.com**

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