feedzai

Becoming Preventative vs. Reactionary:

Early Risk Detection for Account Takeover Mitigation

feedzai

Contents

feedzai

Account Takeover: Where Are We Now?

Account Takeover (ATO) fraud attacks that were once large-scale, “scattershot” campaigns have morphed into smaller, more honed attacks that are more finely tuned and, as a result, significantly more effective. Here’s what you need to know to fight back and protect your business.

Why Has the Cost of ATO Fraud Increased?

Fueled by societal and economic instability, fraudsters utilize fraud-as-a-service social engineering sites and easily obtain malware to commit identity theft and access customer accounts (i.e., phishing attacks, stolen account credentials, remote access trojans (RATs)). The costs of these attacks can be substantial. The UK financial services sector reported a 43% increase in remote banking fraud losses in 2020. Meanwhile, total consumer identity fraud losses grew to $56 billion (USD) in 2020.

It's no secret that fraud is a constant game of cat and mouse: bad actors develop new attack techniques and utilize the latest credential-stuffing automation technology while banks upgrade their capabilities in response to keep pace. But why is the cost of ATO rising so rapidly?

There is a two-part answer to this question. First, the expansion of new payment methods and increased speed of payment transactions over the past decade enables fraudsters to rapidly scale their operations and profit faster from their scams.

In the U.S., peer-to-peer (P2P) payment applications have steadily increased among consumers. As these P2P apps have been developed and rolled tout, they've been key targets for fraudsters to exploit. P2P platforms like Zelle, for example, saw a 49% rise in transaction volumes in 2021 from the previous year, with nearly half a trillion dollars sent to consumers and businesses. Meanwhile, the FTC reports fraud involving P2P payment apps has seen astronomical growth of 885% between 2018 and 2020.

Second, fraudsters realize that banks are often slow to determine whether an ATO attack is in progress and stop it before fraud is committed. Current ATO solutions are designed to detect and alert, placing the remediation burden on the bank's transaction monitoring system to stop the fraud. This gives fraudsters a window of opportunity to commit account takeover fraud before a bank responds.

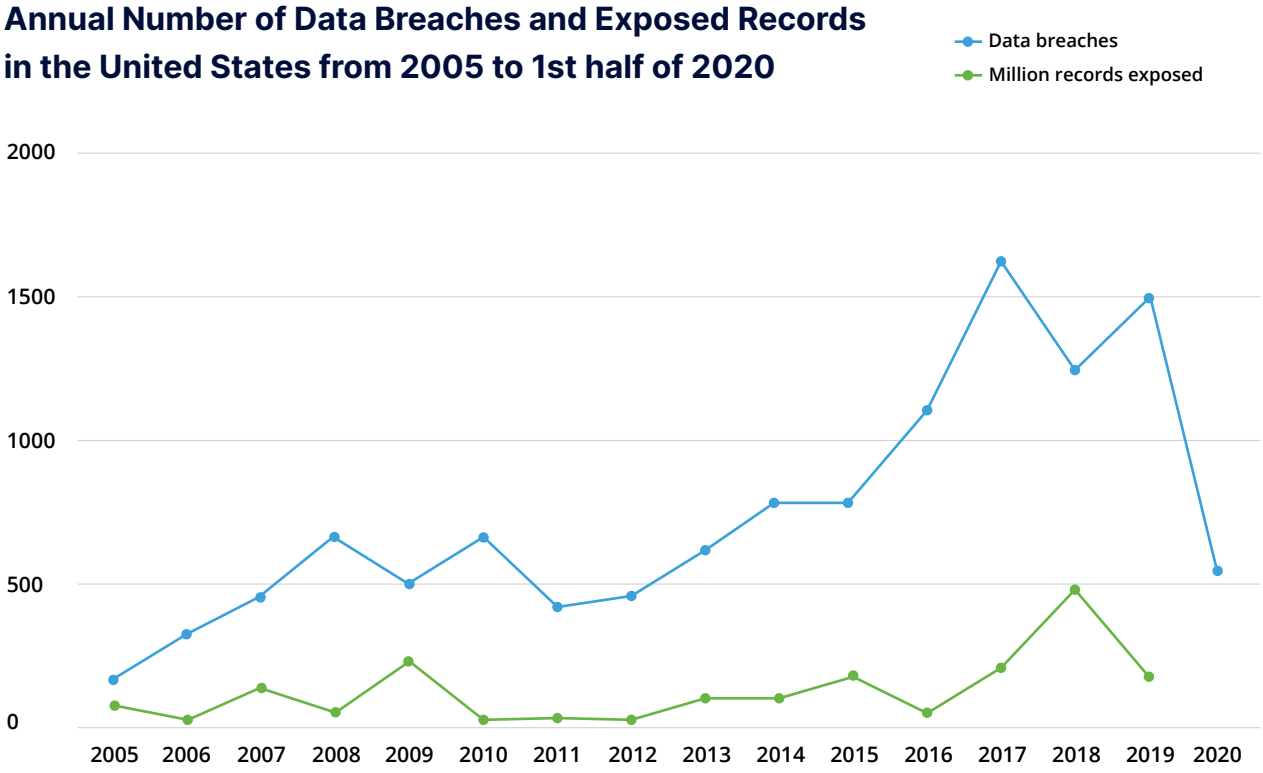
Recovering the money exfiltrated via these new digital channels is extremely difficult, which further contributes to the growth of ATO fraud. Combine that fact with the rapid growth of anonymous payment methods (e.g., different types of cryptocurrency), and fraudsters have several ways to move money quickly out of accounts.

With the above method of exfiltrating funds, ATO attacks become even more widespread thanks to the availability of personal information compromised through data breaches. A recent report found data breaches soared by 68% last year, the highest increase on record. The sensitive data obtained from seemingly daily data breaches has only grown more valuable to fraudsters and poses an increasingly significant threat to banks.

This stolen information opens the door to a range of ATO techniques for bad actors. Data breaches and proactive means of stealing credentials such as phishing and its variations (smishing, vishing, etc.) have led to a wide range of consumer data available for purchase on the dark web, arming would-be fraudsters with the tools they need to convincingly pretend to be legitimate customers.

A report by Aite Group revealed only 43% of US consumers use a different username and password combination for separate sites. As more and more bank account credentials are compromised and bought and sold on the dark web, fraudsters can successfully use each set of credentials on both the compromised account and other businesses that use the same email address or phone number.

vanced methods of compromising information include ID-stealing malware, where targeted malicious code is designed to swipe banking credentials. Stolen credentials enable fraudsters to use legitimate credentials to break into a customer's account, change contact information to receive alerts and one-time passcodes (OTPs) and drain the account of funds. Some bad actors use a class of malware called remote access tools or trojans (RATs) designed to hijack a customer's banking session or transaction after the legitimate user has already logged in.



Source: Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 1st Half 2020, Statista

So the question remains: with the confluence of new digital payment technologies, the ease for fraudsters to move money and struggle for banks to recover it, and dramatic increase in availability and quality of breached records, how can banks ensure that they can stay ahead?

Leveling Up Fraud Detection to Combat ATO Growth

The key to keeping pace with new ATO attacks boils down to a simple concept: building a robust data and prevention strategy that enables **earlier indicators** in the fraud lifecycle. Current systems, regardless of whether they rely on rules or machine learning for fraud detection, often are limited in their capabilities as they score at the transaction level. The difficulty with scoring specifically at a transaction level (not including enrichment) is that by the time banks are scoring a transaction, the fraudsters are already attempting to move the money out of the bank. At this point it is more often than not **too late** to be able to detect fraud. And, if the bank gets it wrong, the money disappears into the fraudster's pockets.

Leveraging a robust data and prevention strategy to identify fraud early in the fraud lifecycle breaks down into two distinct data-themed categories:

First, banks can rely on data enrichers. These enrichers are critical in the creation of fraud modeling and customer profiling since it enables banks to lift the 'iron curtain' that digital transactions enable fraudsters to hide behind. When a fraudster/legitimate customer walks into a bank in person, a number of authentication measures can be enacted that just simply can't be replicated in digital channels. In order to account for this, banks need to pull in 3rd party data (such as device, geolocation, behavioral analysis, RAT detection, malware detection, device emulation, etc.) so they can understand the context the transaction is happening in. For example, if the geolocation of the transaction matches historical data, but it's evident that the device is hidden behind a proxy, that may be reason for concern.

Second, banks need to be able to bring together their data from all other channels. Omnichannel solutions, which incorporate data from other payments channels (i.e. combining data from credit card & non-card channels), have been shown to drastically increase detection accuracy. However, for ATO fraud specifically, it's key that data is brought together from all **customer touchpoints** (whether it be call centers, online touchpoints, or others) when making decisions. This is the key to detecting fraud earlier. Take for example the following scenario:

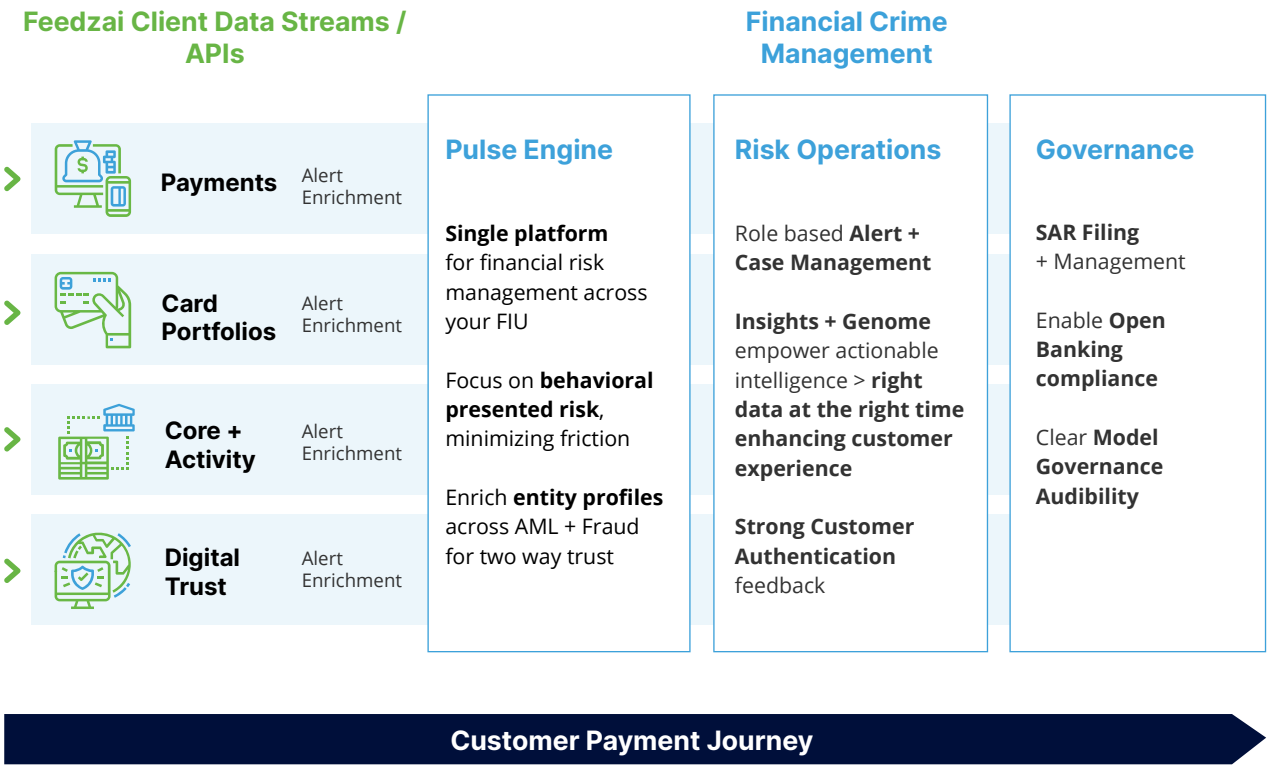
- A caller claiming to be Bob calls into a call center to check on his bank account, and after a few minutes of talking with the representative he thanks him — he's just verified that Bob actually has an account with the bank.
- "Fraudster Bob" calls multiple-more-times to gain additional information and credibility, a change email on-file was made to a fraudulent one by a call center agent.

- As "Fraudster Bob" gained credibility he was able to get the online bank account password reset sent to the fraudulent email address through a call center agent. "Fraudster Bob" was able to gain access to the online bank account and look at account balances.
- Bob's account has a new login from a location that is outside of 500 miles of his normal transaction area.
- Bob makes a $2,500 instant transfer to a seemingly good instant transfer account.

Looking at the transaction information in isolation, they are missing a key part of the picture. Multiple non-monetary events - calls, change of email, login attempts from a new device, and access from a new geolocation - all should have triggered warnings. But, without the appropriate context, the wrong decision can be too easily made.

With the appropriate combination of both internal data sources and 3rd party data sources, banks can shift their focus to earlier in the fraud lifecycle. This enables better ATO mitigation.

The Transaction Journey

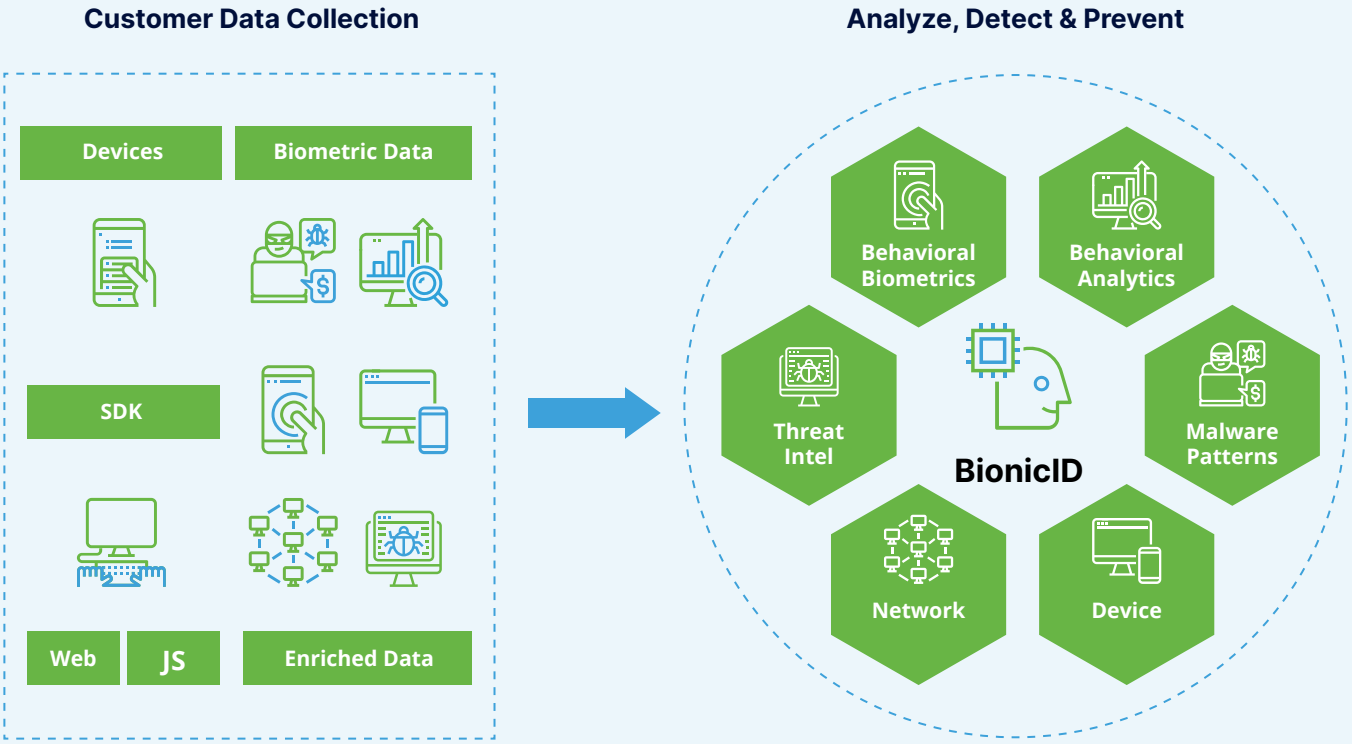


How Feedzai Executes and Elevates Early Risk Detection for ATO

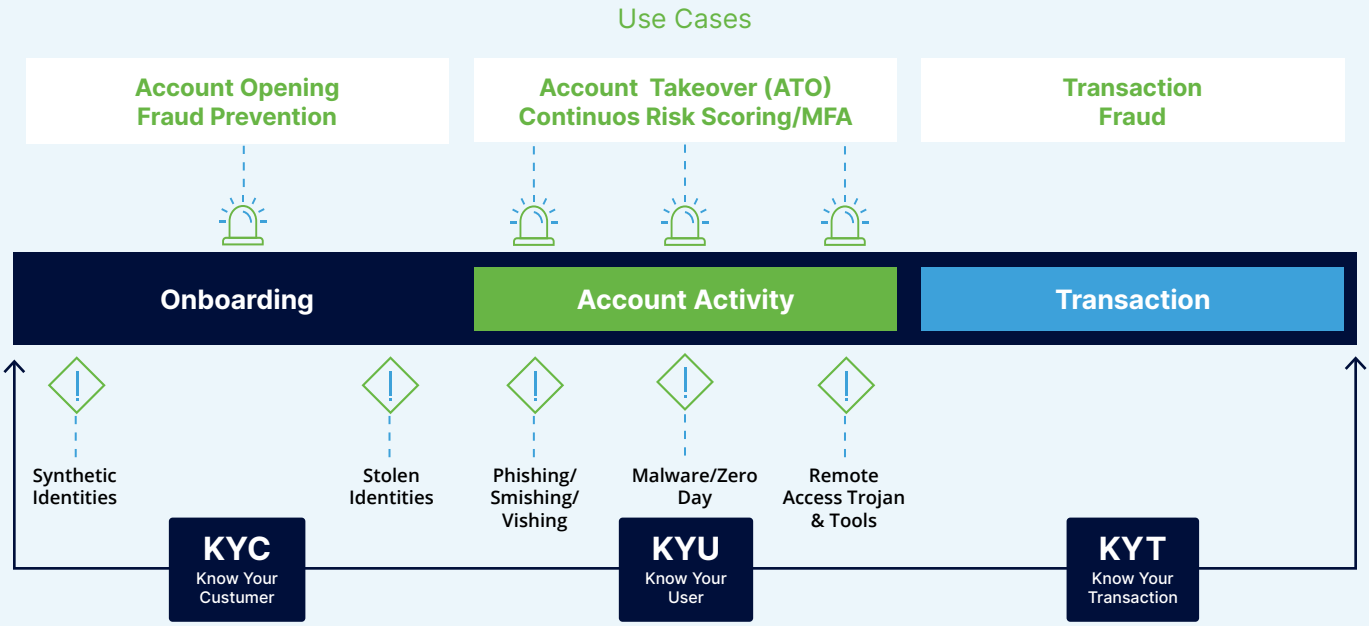
Feedzai has built a unified platform to manage the entire risk lifecycle of fraud. By utilizing all data and tools for cross use-case scoring, Feedzai can provide **earlier detection**. Rather than relying on the transaction to be the detection or fail point, Feedzai incorporates all available data into a decision — enabling more accurate spotting and stopping of fraud.

On top that, Feedzai counts natively with tons of signals to improve accuracy and increase detection capabilities, such a device assessment, behavioral biometrics and malware detection.

Continuous Risk and Threat Analysis with BionicID



Continuous Customer Authentication



End-to-end **RiskOps** Platform to manage financial risk

Full Risk Cycle

PREVENT
Prevention strategies enable protection at the earliest stage

DETECT
Risk based data, cyber and customer history operate cohesively

REMEDIATE
Customers who are captured in financial crime are managed efficiently and with trust

COMPLY
Ensure compliance and transparency end to end

Feedzai **RiskOps** Platform is set on 3 main pillars

Comprehensive Architecture | **Human-centered AI** | **Collaborative Analytics Suite**

Our platform and tools are built with a four-pronged risk mitigation approach in mind. Following this approach, and incorporating data and insights from each portion of this journey, enables Feedzai's tools to detect fraud, like ATO, earlier.

Key features of our platform that enable earlier detection include:

Better Detection: Advanced AI

Leveraging years of data science-specific domain experience, Feedzai's real-time decision engine unites data across disparate streams and builds hypergranular Segment-of-One profiles of baseline (or normal) behavior. By leveraging a number of modeling techniques to compare current behavior to existing profiles, Feedzai's AI provides unparalleled detection accuracy.

Better Decisions: Best-in-class Tools

Give analysts the tools to make the best decisions possible. Omnichannel Case Manager ensures that all transaction and enrichment data can be brought together to improve risk assessment, and analyst efficiency. Combined with future-focused tools - like Feedzai's visual link analysis tool - see investigation times plummet while accuracy significantly increases.

Open Platform

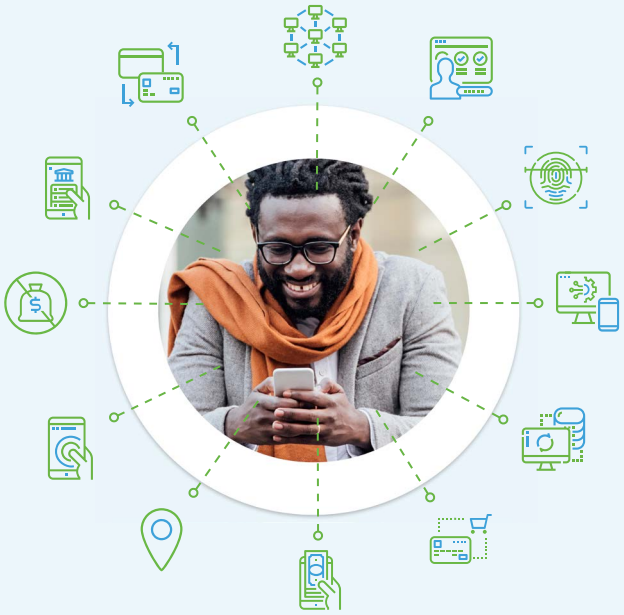
Feedzai's platform was built in alignment with key open capabilities. These capabilities enable quick data normalization, dataset augmentation, profile creation, and support non-traditional modeling methods for detecting account takeover attacks. Additionally, Feedzai's platform touts other industry-first open platform capabilities, such as OpenML, to enable more agile fraud prevention responses. Feedzai's OpenML is a feature that gives data scientists the flexibility to use their own models and data science tools while working in the Feedzai ecosystem to fight fraud more effectively.

Agile Platform

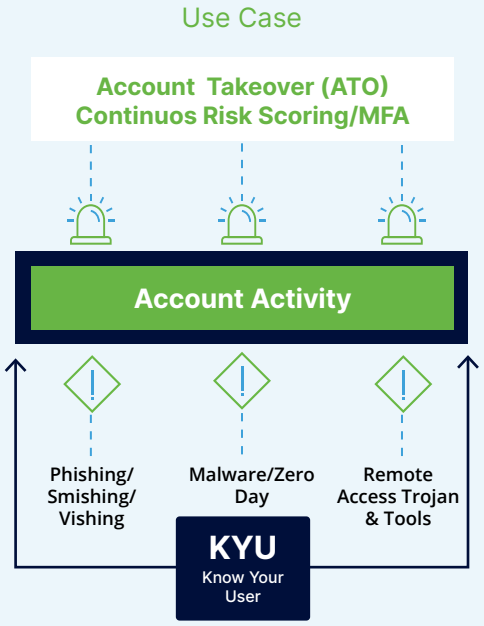
Built with three dimensions of agility in mind (agile deployment, speed of scoring, and speed of responding to new fraud trends), Feedzai's platform and tools enable banks globally to adapt to a changing ATO landscape. These three dimensions all support organizations to quickly respond, triage, and stand up counter controls to mitigate fraud losses and reputational risk.

Data Agnostic

Merge together digital footprint data and transaction data within Feedzai's platform. By incorporating data from across channels, ensure that you can notice red flags before the money moves out of your business.

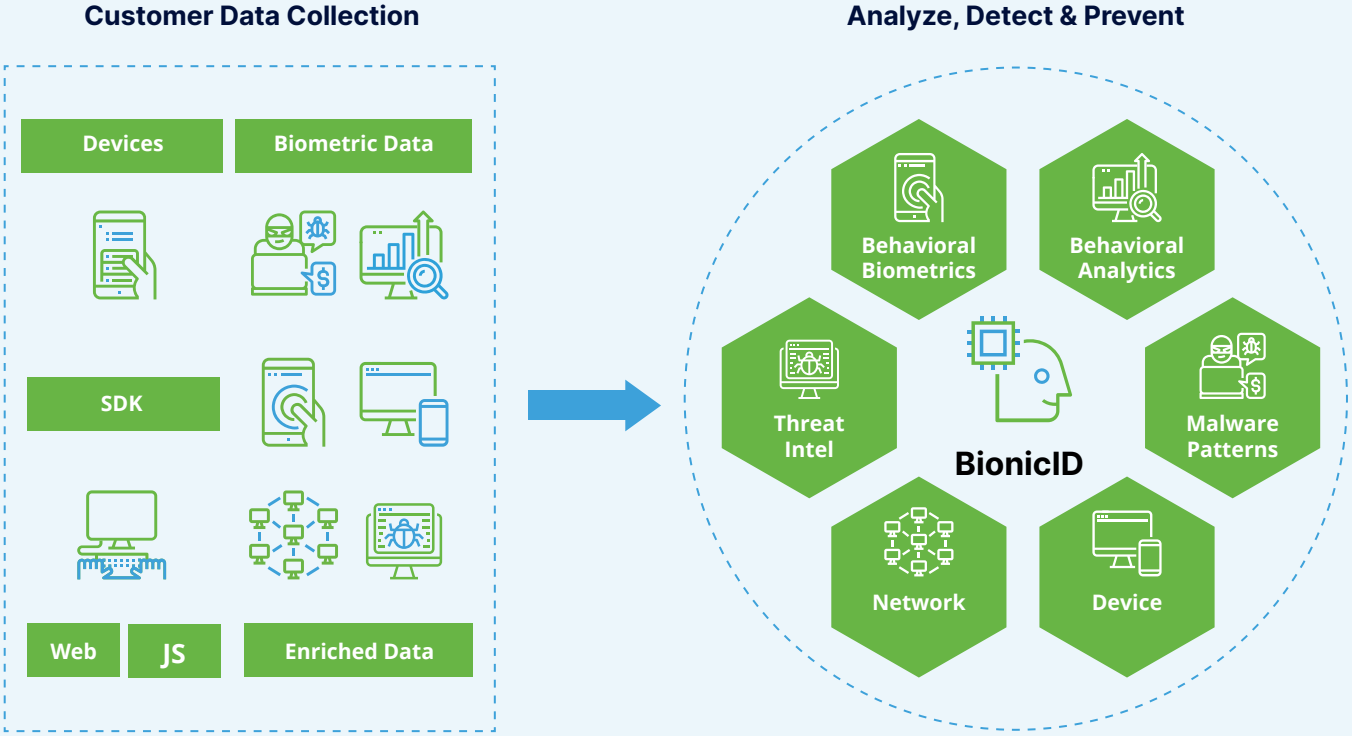


Know your user



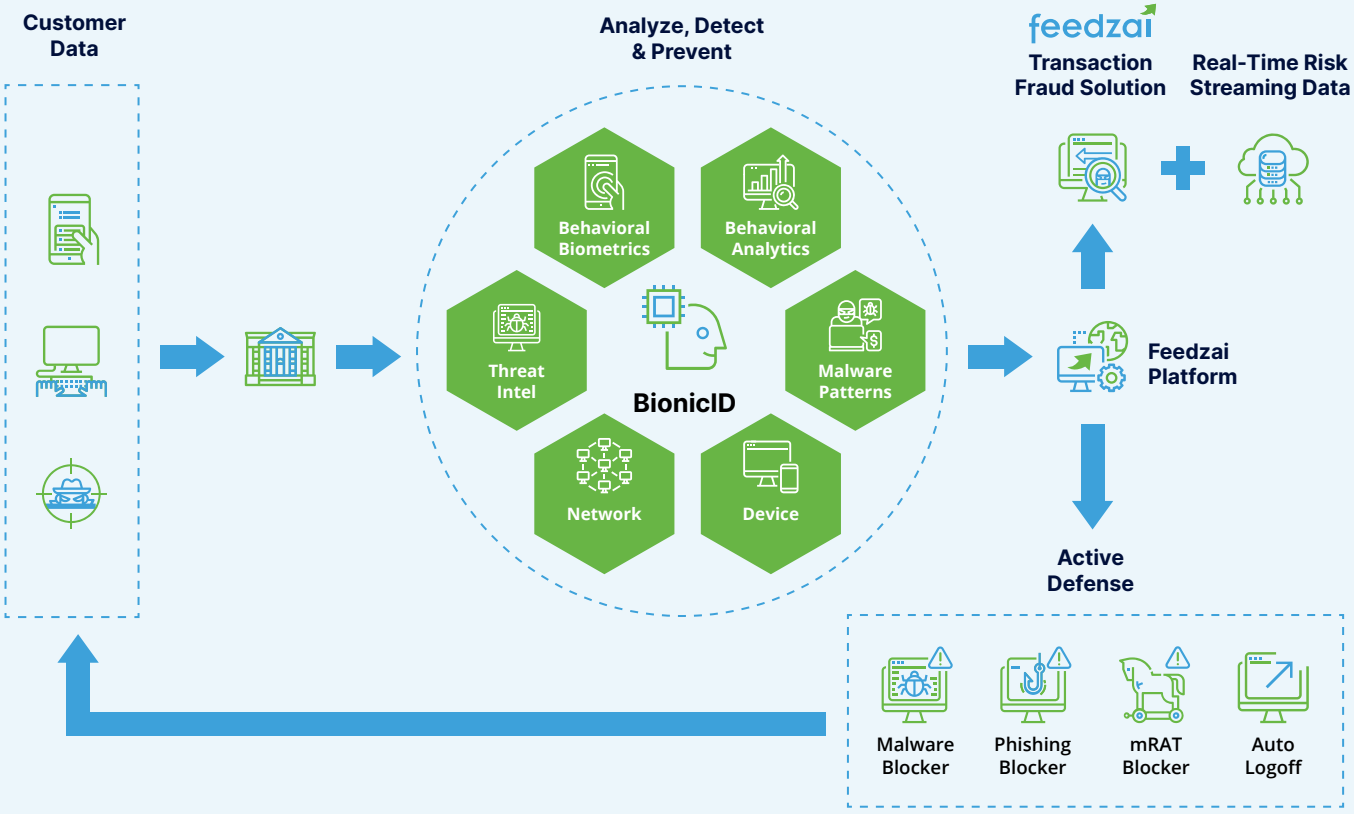
BionicID

Create multi-layered AI models that build specific profiles per user based on their unique characteristics gathered in a friction-less mode from data of their devices, networks, mobile and browser parameters, threat intelligence, behavioral biometrics and behavioral analytics.



Active Defense

Take customized real-time actions to prevent fraud on end-user devices before it happens.



Accelerating Detection by Leveraging Cloud

Agility is key when it comes to combating fraud. And, when under a fraud attack one thing reigns above all else: response time. When a fraud response isn't fast enough, fraud attacks can often compound and quickly snowball out of control. In order to develop a quick response strategy, banks need the flexibility to not only identify the root cause of the attack, but also identify and fix any strategy gaps where incremental tools or data streams must be added into the process.

With Feedzai's open platform, banks can easily connect new data streams from previously disparate sources via an API. These new data streams can be quickly incorporated into a cloud-based scoring process, enabling an agile fraud response.

Why Cloud?

Easy to Deploy:
Ready to-go detection scenarios and case investigation interfaces

Cost-effective:
Premium services and advanced technology at a competitive price

Quicker Time to Value:
Quick time to value, tangible ROI on deployment

Turnkey AI:
Zero-day strategies with auto-configured models

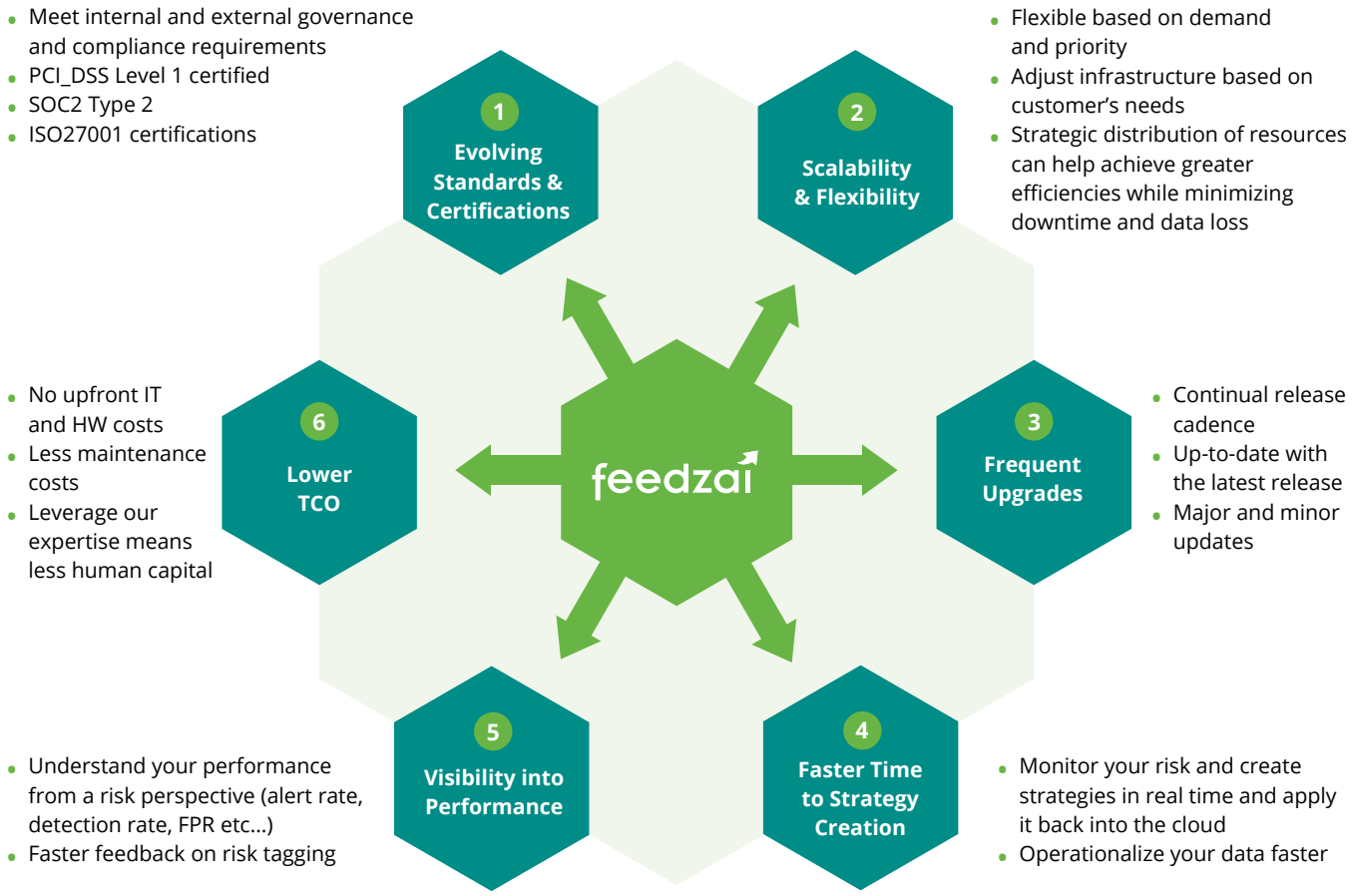
Quantifiable results

57%
Improvement in a major retail bank's fraud detection rate compared to a previous system.

39%
Decrease in false positive rate compared to the retail bank's previous system.

Global Fraud Network

Leveraging reported fraud across a customer network enables banks to stop the fraud before it starts. Shared negative intelligence near real-time is so powerful to curve the attacks. This give to get model has been proven to methodology in the space of account takeover. Data attributes like digital attributes, addresses, phone numbers, emails, and account number detail are just a few examples of fields that can be used to identify rogue activity. Cloud technology has leapfrogged intelligence sharing making it way more efficient than it has been in the past where email lists were the most popular way to share.



feedzai

The RiskOps Platform

Transform your risk management.

Feedzai's AI stays ahead of emerging fraud and financial crime and mitigates even the most deceptive schemes so that banks, issuers, acquirers, and merchants can focus on growth.

Feedzai is considered best in class by Aite and one of the most successful AI companies by Forbes. The world's largest organizations use Feedzai's fraud and financial crime prevention products to safeguard trillions of dollars and manage risk while improving customer experience.

Account Opening | Anti-Money Laundering | Transaction Fraud

feedzai.com **info@feedzai.com** **sales@feedzai.com**