December 2023

Datos Insights Matrix: Behavioral Biometrics and Device Fingerprinting Solutions

Gabrielle Inhofe, David Mattei, and Jim Mortensen

This excerpt provided compliments of this Best-in-Class vendor:

December 2023

Datos Insights Matrix: Behavioral Biometrics and Device Fingerprinting Solutions

Gabrielle Inhofe, David Mattei, and Jim Mortensen

Table of Contents

List of Figures

List of Tables

Introduction

As the world becomes increasingly digital, users are conducting more e-commerce and financial services online. This is a great convenience for consumers who do not have to physically drive to a store or bank branch to conduct business, but it is also a haven for fraudsters who can commit their fraud with anonymity. Fighting fraud has traditionally been waged at the financial transaction level, determining whether to approve or decline the transaction. However, as incremental gains in this space have slowed, FIs, fintech firms, and e-commerce merchants have turned to user authentication as the next frontier to protect themselves and their customers. In addition, as scams have dramatically increased over the past several years, a need has arisen to ascertain whether a user is being coerced or coached by fraudsters to transfer funds to accounts controlled by the fraudsters.

Behavioral biometric and device fingerprinting solutions are gaining popularity as a way to authenticate a user and detect possible scam activity. While each of these functions came to market at different times over the past 10 years and as separate solutions, recent innovations from vendors are bringing these functions together into a single, unified solution. A strong benefit of this combined solution is that it is a passive authenticator running in the background, unbeknownst to the end user. As such, it provides strong fraud detection and a positive user experience.

This report explores some of the key trends within the behavioral biometric and device fingerprinting market and discusses the ways in which technology is evolving to address new market needs and challenges. The Impact Report also compares and contrasts the leading vendors' offerings and strategies, and it highlights their primary strengths and challenges. Finally, to help FIs make more informed decisions as they select new technology partners, the report recognizes specific vendors for their strengths in critical areas.

Methodology

Leveraging a proprietary vendor assessment framework, this Datos Insights Matrix Report evaluates the overall competitive position of each vendor, focusing on vendor stability, client strength, product features, and client services.

The following criteria were applied to develop a list of vendors for participation:

- The behavioral biometrics and device fingerprinting technology must be owned, developed, and maintained in-house by the vendor. Neither of these technologies can be licensed from a third party.
- The behavioral biometrics solution and the device fingerprinting solution must be available as stand-alone solutions for purchase and deployment by a customer. A vendor that has behavioral biometrics and device fingerprinting functionality that is part of or embedded within another offering and not available for purchase outside of that offering is not eligible.
- The behavioral biometrics and the device fingerprinting solution must support identity management of end users/customers of the vendor's client (CIAM). Solutions that only support identity management of employees of the vendor's client (IAM) are not eligible to participate in this study.
- Participating vendors must have production deployments in financial services. Their solutions must be able to support behavioral biometrics and device fingerprinting addressing identity proofing or user authentication use cases.

Participating vendors were required to complete a detailed product request for information (RFI) composed of both qualitative and quantitative questions, conduct a minimum 60-minute product demo, and provide active client references.

The Players

This section presents comparative data and profiles for the individual vendors that participated in the Datos Insights Matrix evaluation. This list is by no means exhaustive. Firms embarking on a vendor selection process should conduct initial due diligence prior to assembling a list of vendors appropriate for their own unique needs.

Table A presents basic vendor information for the participating solutions.

Table A: Evaluated Vendors

Firm	Headquarters	Founded	Number of employees	Target market
Accertify	Itasca, Illinois	2007	300	E-commerce merchants, FIs, and fintech firms
BioCatch	Tel Aviv, Israel, and New York	2011	Over 285	FIs, fintech firms, and e-commerce merchants
Callsign	London	2012	250	Primarily FIs; other industries include fintech firms, cryptocurrency firms, and e-commerce merchants
DataVisor	Mountain View, California	2013	130	FIs, fintech firms, cryptocurrency firms, and e-commerce merchants
Feedzai	San Mateo, California	2011	650	FIs and fintech firms
LexisNexis Risk Solutions	Alpharetta, Georgia	2000	9,200	FIs, e-commerce merchants, fintech firms, cryptocurrency firms, and others

Firm	Headquarters	Founded	Number of employees	Target market
Mastercard	Purchase, New York	1966	29,900	FIs, e-commerce merchants, and fintech firms
Sardine	San Francisco	2020	100	FIs, payment processors, fintech firms, e-commerce merchants, and cryptocurrency firms
ThreatMark	Charlotte, North Carolina	2015	130	FIs
XTN Cognitive Security	Trento, Italy	2014	30	FIs, fintech firms, and gambling firms

Source: Vendors

The Market

Numerous market trends are shaping the present and future of the behavioral biometric and device fingerprinting market (Table B).

Table B: The Market

Trends	Implications
Scams	With the growth in social engineering attacks resulting in scam fraud, FIs and fintech firms need better defenses to detect and stop this form of fraud, especially in light of the regulatory scrutiny on this subject.
Increased sophistication of fraud attacks	The robustness of new tools available to fraudsters makes it more difficult for legacy fraud solutions to detect new attack vectors.
Advances in artificial intelligence (AI) and machine learning (ML) technology	As the power of AI/ML technology increases and the cost decreases, vendors can bring more powerful fraud solutions to market.
First-party fraud	Consumers are becoming more brazen by lying to their FIs about not recognizing purchases they made. This could be exacerbated by future regulatory changes to scam fraud in which some or all liability moves from consumers to FIs.
Mobile banking and e-commerce	Consumers are transacting more online than ever before. FIs, fintech firms, and e-commerce merchants can leverage the wealth of information available in the mobile channel to deploy stronger fraud solutions with less user friction.
Budget and IT constraints	As FIs are pressed to "do more with less," they will look for ways to get more fraud-mitigating functionality from fewer vendors. Point solutions from multiple vendors will give way to multipronged solutions from one or a few vendors.
Evolving regulatory landscape	The regulatory landscape continues to evolve in the face of novel and expanding fraud threats that may result in a shift of liability. Fraud fighters must keep abreast of these changes to protect companies and their customers.

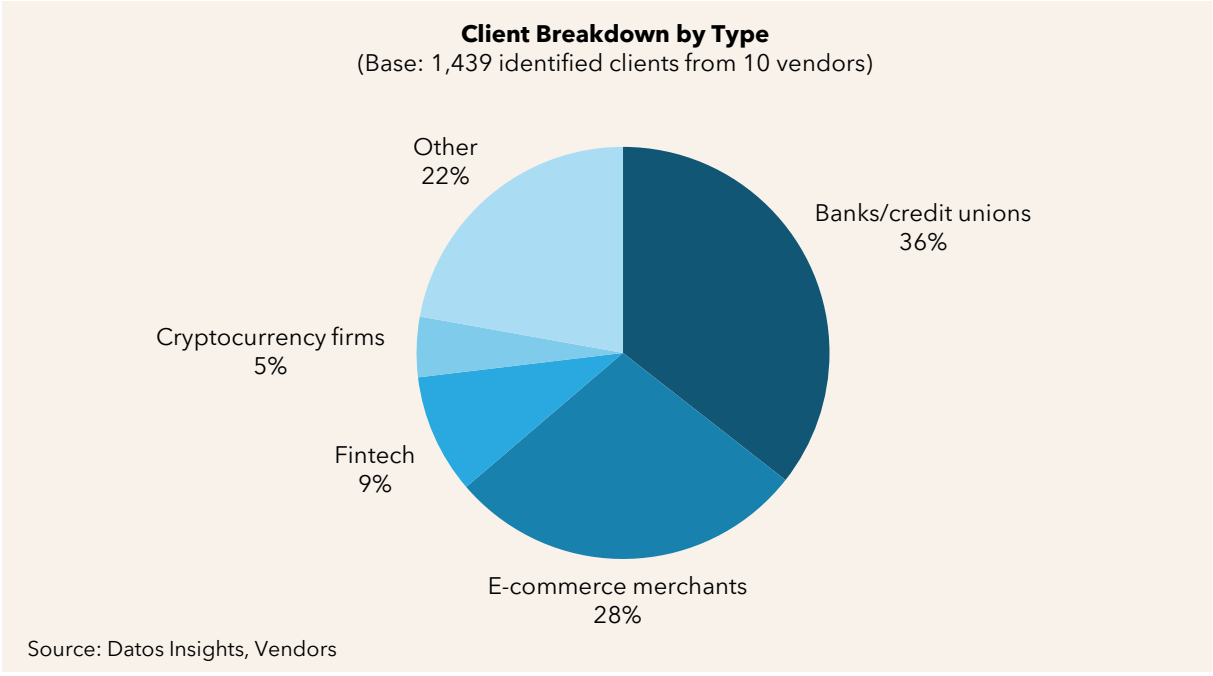
Trends	Implications
Changing face of digital identities	Companies are challenged to verify the identity of an online user at the time of account creation (identity proofing) and when returning online users log into the website or mobile app (authentication). No single tool sufficiently addresses this. A multipronged approach is needed.

Source: Datos Insights

Client Breakdown by Type

User authentication is a need across many industries, not just among FIs. The largest proportion of clients among the vendors are banks and credit unions at 36%, followed by e-commerce merchants at 28% (Figure 1). Twenty-two percent of the vendors' clients fall into the "other" category, which encompasses a variety of industries, including gaming. The fewest clients are in the fintech and cryptocurrency industries, at 9% and 5%, respectively. As fintech and cryptocurrency firms continue to emerge and increasingly fall under regulation, these numbers could potentially rise.

Figure 1: Vendor Client Breakdown by Type



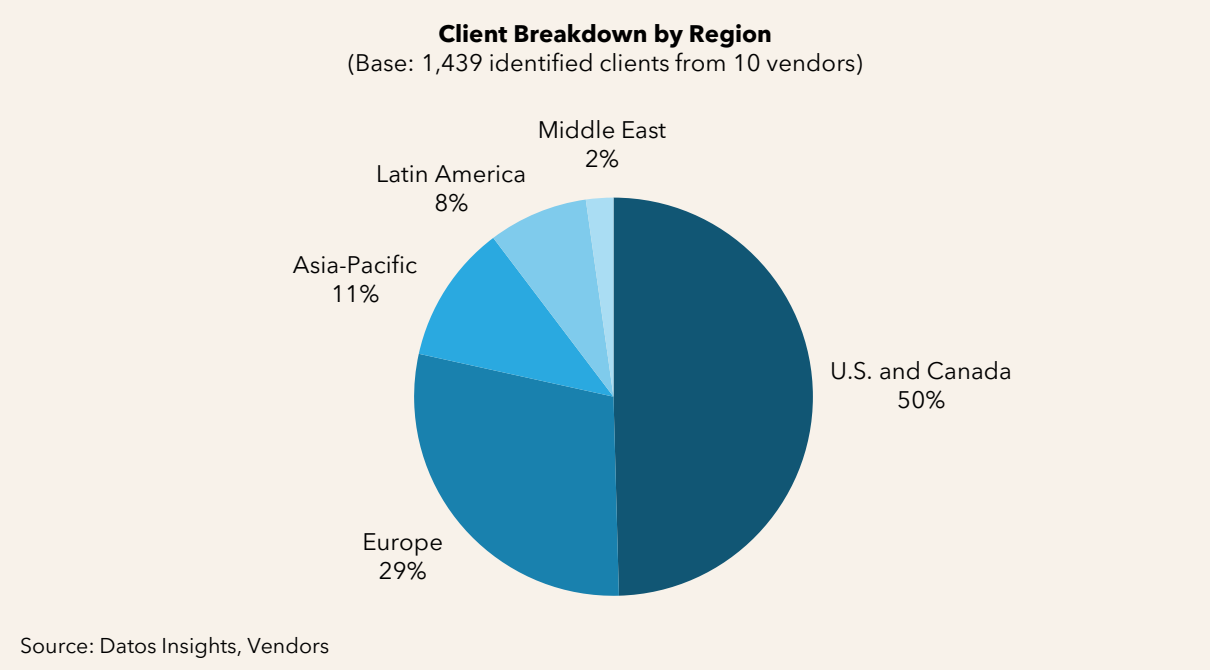
Source: Datos Insights, Vendors

Client Breakdown by Region

Capturing an impressive 50% of global client distribution, North America (the U.S. and Canada) is perhaps unsurprisingly the biggest market for behavioral biometrics and device fingerprinting solutions within the participating vendors (Figure 2). Though Europe takes almost a third of global client distribution at 29%, there is a significant gap between it and North America.

Asia-Pacific comes in at 11%, followed by 8% for Latin America. The Middle East and Africa have a very small client presence, given less robust financial services industries and more nascent regulatory frameworks in the financial crime space. As emerging markets continue to develop, it is expected that the demand for behavioral biometrics and device fingerprinting solutions will expand in these geographies.

Figure 2: Vendor Client Breakdown by Region



Source: Datos Insights, Vendors

Vendor Evaluation

This section breaks down the individual Datos Insights Matrix components, drawing out the vendors that are strong in each area and how they are differentiated in the market.

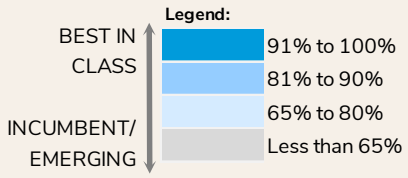
Datos Insights Matrix Components Analysis

Figure 3 provides an overview of how each vendor scored in the various dimensions of the analysis. Each vendor is rated, in part, based on its responses to the RFI distributed by Datos Insights and the information provided in product demos and follow-up discussions as part of the Datos Insights Matrix process. Ratings are also driven by the vendors' client references to support a multidimensional rating.

Figure 3: Datos Insights Matrix Component Analysis Heat Map

Overall score by average of each criteria

Vendors	Vendor stability	Client strength	Client service	Product features
	93%	90%	76%	85%
	85%	94%	88%	88%
	81%	81%	83%	91%
	80%	82%	89%	92%
Feedzai	87%	85%	97%	87%
	93%	92%	92%	90%
	87%	92%	83%	82%
	82%	84%	82%	89%
	75%	80%	77%	90%
	74%	87%	78%	94%



Source: Datos Insights

Vendor Stability

Factors driving high scores include company size (number of employees and geographies in which they operate), profitability, debt levels, amount of recurring revenue, and others. Client impressions of the vendors' talent, R&D investment, innovation, and risk management practices also contribute to the vendor stability rating.

Clients tend to deploy an authentication solution and stay with it for a number of years. It is important that a vendor has the stability and financial wherewithal to support a client over

a multi-year relationship and the ability to continue investing in its solution to address the ever-evolving threat vectors that fraudsters devise.

Client Strength

Factors influencing this rating include the number of industry verticals supported across a vendor's client base and the geographical diversity of its clients. This rating also included client feedback on vendor satisfaction, the likelihood of recommending the vendor, and the likelihood of replacing the vendor.

A diversified and satisfied client base is an important consideration for prospective buyers. Buyers want some level of assurance that the vendor can support their future growth goals. Existing clients that are highly likely to recommend a vendor they are using, even after going through the initial implementation phase and ongoing usage, speak well of how the vendor manages its clients.

Client Service

Feedzai excels in client service, with a score of 97%. This score is driven by the number of client engagement options the vendors support, attractive pricing, and client feedback on the vendors' responsiveness to servicing issues, delivering on promises, and the variety of professional services offered.

No two clients are exactly the same. They have different needs and expectations of the vendors they select. Service and support are important to the client's ultimate success with a commercial solution. The account representative or relationship manager is usually the main point of contact for the client, and that person has a strong influence on client service. Vendors that invest in this aspect of their staff usually see dividends on that investment in the form of happy customers.

Product Features

This vendor performed well in areas such as risk-scoring strength, implementation options, number of public clouds supported, low latency, reporting capabilities, and breadth of other authentication solutions. Clients also provided insights into the vendor's ability to support customizations, ease of implementation and deploying upgrades, and level of integration of the behavioral biometrics and device fingerprinting capabilities.

With over 40 vendors offering some type of behavioral biometrics and device fingerprinting solution, a broad suite of out-of-the-box functionality that is easy to deploy is table stakes in this competitive industry. However, there are times when a client will have

needs that either the vendor does not currently support but would benefit all clients or are unique to the client. Hopefully, ongoing innovation and product investment will deliver that capability. When it doesn't, a vendor that can deliver needed functionality in a reasonable time frame provides the most flexibility to its clients.

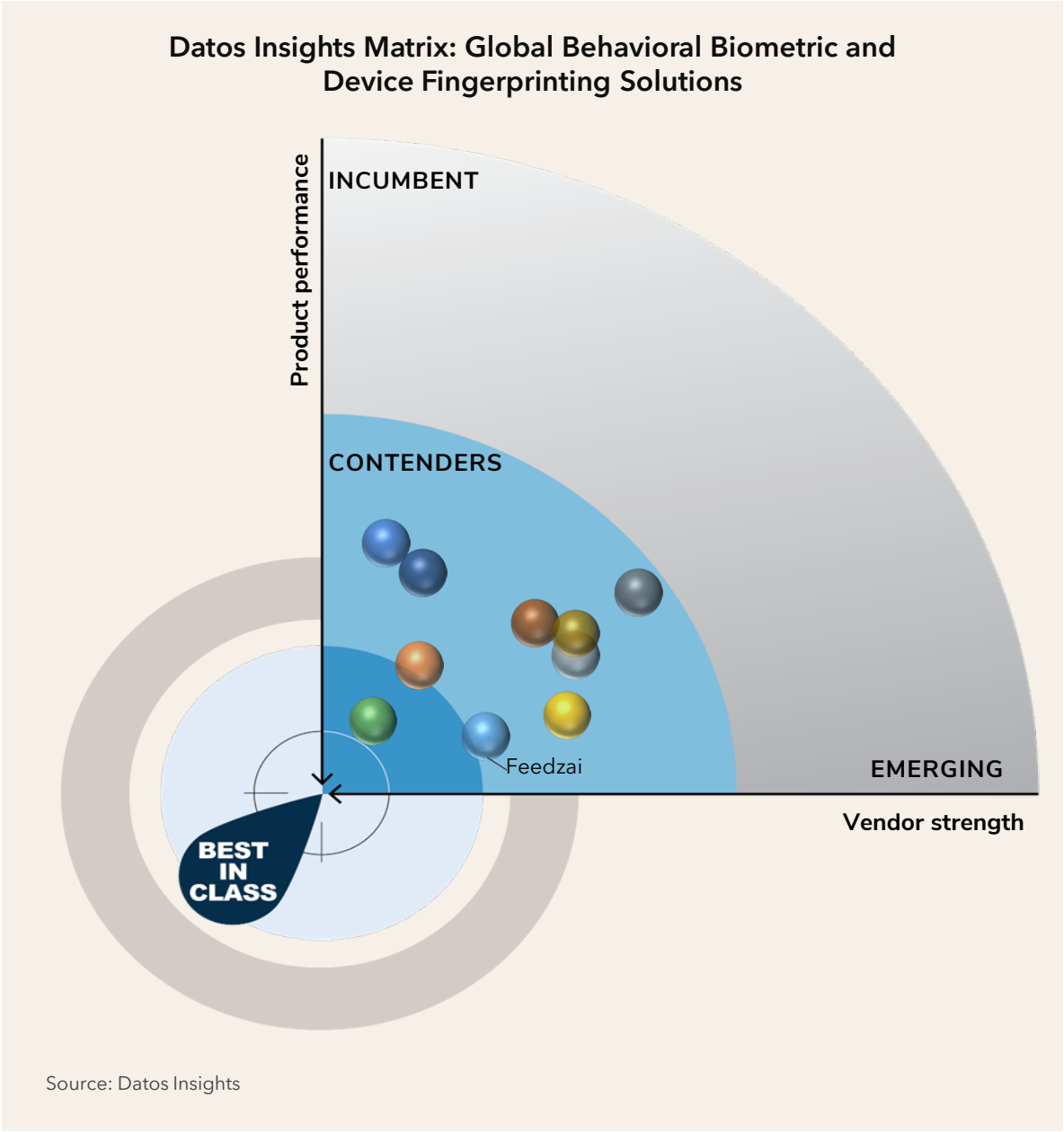
The Datos Insights Matrix Recognition Vendor Evaluation

Three major factors drive the final results of the vendor evaluation:

- Vendor-provided information based on Datos Insights' detailed RFI document
- Participating vendors' client reference feedback or feedback sourced independently by Datos Insights
- Analysis based on market knowledge and product demos provided by participating vendors

Figure 4 presents the final evaluation in this Datos Insights Matrix Report, highlighting the leading vendors in the behavioral biometrics and device fingerprinting market.

Figure 4: Behavioral Biometric and Device Fingerprinting Datos Insights Matrix



Source: Datos Insights

Leading Contender: Feedzai

Feedzai amped up its game in the fraud space in 2021 when it acquired Revelock, a digital identity firm. This provided a strong complement to Feedzai's legacy financial transaction fraud detection solution. Feedzai has brought its data modeling experience into the Revelock technology stack to make improvements in its authentication solutions. Clients praised Feedzai for "strong risk scores," "continuous innovation and enhancements," and its "intuitive console for conducting threat analysis."

Feedzai was founded in 2011 by data scientists with the mission of making banking and commerce safe. The world's largest banks and payment providers use Feedzai's ML-driven RiskOps Platform to manage the risks associated with banking and payments, whether in person, online, or via mobile devices.

In August of 2021, the company acquired Revelock (formerly buguroo), a behavioral biometrics and device fingerprinting solution provider, which greatly expanded Feedzai's fraud prevention capabilities. This has allowed the company to offer behavioral biometrics and device fingerprinting as a stand-alone solution. More importantly, it has increased the robustness of its transaction fraud detection solution.

From the outset, Feedzai took a big-data and ML approach to protecting digital commerce for FIs and fintech firms. The firm began by offering an AI-powered fraud solution to protect financial transactions and expanded into protecting digital accounts. Supported fraud use cases include account opening, ATO, and financial transactions. Supported compliance use cases include AML, KYC/customer due diligence and watchlist screening.

The company boasts a list of impressive clients, including CaixaBank, Raiffeisen, Al-Rajhi, KutxaBank, and Cajamar.

Datos Insights' Take

From its beginnings, Revelock built its solution by taking into consideration behavioral, device, network, and malware simultaneously rather than starting with one and then adding others. There is one API, one SDK, and one JavaScript collector that provides access to all capabilities within the solution. This is particularly attractive in that it makes for a seamless and comprehensive integration and allows the clients to focus on the use of the platform as opposed to dealing with myriad connection points in their technology stacks.

The workhorse of Feedzai's solution is the data gathered from a user's online session, which feeds into multiple ML models. Model scores can be used stand-alone or within rules that are part of a policy manager. A suite of rulesets is available out-of-the-box addressing various use cases such as ATO, malware, network, and device anomalies for clients to leverage as a starting point before implementing any customizations. A graphical user interface is also provided for managing the rulesets. In addition, multiple ML scores are combined into a super score for the biometric model called the Fraud Profiler.

Feedzai includes three additional data parameters—Bio-Profile, Quality, and Similarity—to provide context for the ATO Profiler score. Bio-Profile represents how much information has been collected to-date to provide a strong profile of the user. Similarity represents how common the user's session is to prior sessions. Quality represents the confidence that it knows the user. These data parameters provide useful guidance as to what type of action should be taken with user interaction. After an average of five user visits, the solution can uniquely identify individuals. Combined, these elements make Feedzai a strong contender worth consideration for buyers seeking a behavioral biometrics and device fingerprinting solution.

Basic Firm and Product Information

Table C provides basic firm and product information for Feedzai.

Table C: Basic Firm and Product Information, Feedzai

Category	Description
Headquarters	San Mateo, California
Founded	2011
Website	https://feedzai.com/
Number of employees	650
Ownership	• Privately held • Series D funding raised a total of US$270 million
Global business footprint	The U.S., Europe, Asia-Pacific, Latin America, the Middle East, and Africa
Key product names	Feedzai Digital Trust

Category	Description
Target customer base	Banks/credit unions, fintech firms
Number of clients	105
Average net new clients per year	16
Implementation options	Public cloud
Pricing structure	Based on the number of users (customers) per year

Source: Feedzai

Key Features and Functionality Based on Product Demo

- Feedzai offers an integrated solution that encompasses behavioral biometrics, device fingerprinting, and malware detection, making it well-suited to combat a breadth of financial crime activity without impacting the customer journey. It offers support for fraud and AML use cases.
- Continuous risk scoring and customer verification across the entire digital journey protect users and organizations more comprehensively than a static, one-time authentication.
- Link graph analysis identifies fraudsters and entities associated with them. This is key in helping analysts to visualize complex relationships more readily, such as fraud rings.
- Feedzai offers a policy manager for rule writing and strategy management, which leverages both raw data elements gathered by the solution and ML scores. The User Console provides raw data insight into a customer session as well as aggregated risk alerts and scores that supplement risk decisions and treatment strategies.
- Integration with Feedzai's Transaction Fraud solution leverages pre-transaction behavior and risk signals to make a more informed approve/decline decision on the financial transaction. This approach more comprehensively evaluates risk as it expands the view beyond just the transaction, enabling more precise and earlier intervention.

Top Three Strategic Product Initiatives Over the Last Three Years

- Integration with Feedzai Transaction Fraud solution, which analyzes pre-transaction behavior and risk signals in making a more informed approve/decline decision on the transaction.

- Creation of Feedzai ScamPrevent to address institutional financial loss and customer impact of authorized fraud attacks. For banks and payment providers, the solution will flag when a customer's behavior is out of the ordinary using multidimensional detection layers, optionally combined with existing fraud risk controls to protect customers and improve awareness and trust.
- Enhancements that enable minimal banking application and website coding to permit easier integration and implementation, resulting in a faster and simpler user experience.

Top Three Strategic Product Initiatives in the Next 12 to 18 Months

- Expansion of Feedzai's behavioral biometrics and device fingerprinting consortia—from identifying good versus fraudulent users across all clients to identifying a unique individual across all clients.
- Support a new use case where a user is unknown and is being seen for the first time, such as in digital account applications where the user shows an unusually high degree of online form familiarity. In addition, other planned use cases will be supported based on customer requests, including the extension of first-time user verification for e-commerce guest checkout purchases.
- Aggregation of multidimensional threat intelligence signals across malware, threat indicators, and remote-access tool detection (mobile and desktop) capabilities that will target ATO and customer-compromised scam use cases.

Client Feedback

Clients are pleased with the direction Feedzai is headed and viewed the Revelock acquisition favorably. Clients feel that it extended Feedzai's capabilities into new areas, allowing legacy customers of both firms to expand their relationships. The customer support team also gets high marks for the level of care and attentiveness they provide.

One client interviewed recently conducted an RFP to understand what capabilities are available on the market and decided to stay with Feedzai based on the cost-to-value ratio it currently receives. Clients also praised the speed with which they were able to deploy the solution initially. They saw this as a significant benefit, particularly at the beginning of the relationship with Feedzai.

Table D provides the vendor's strengths and challenges.

Table D: Key Strengths and Challenges, Feedzai

Strengths	Challenges
Strong risk-scoring technology	Desire to receive proactive alerts when suspicious activity is detected within the Feedzai environment
Continuous innovation and product enhancements	It takes a while to access information about a client's online session when deployed on the cloud
Strong support staff who listen to client needs, think of solutions, and are quick to respond	Ability to extract data about a client's device or behavior that can be acted upon in non-Feedzai applications (e.g., if an emulator is detected, leveraging that information within the firewall system)

Source: Datos Insights

Conclusion

Behavioral biometrics and device fingerprinting solutions are becoming table stakes in the fight against fraud as essential components of an effective authentication framework. When these solutions come together and leverage risk signals on a combined basis, they form an effective fraud prevention tool that values the customer experience. This is beneficial for buyers and can be advantageous for vendors who can effectively integrate the underlying capabilities. Below are points of consideration for buyers in the market for this type of solution and for vendors looking to enhance their positions in a crowded marketplace.

Buyers:

- Understand your threat landscape, related defensive needs, and constituent group requirements before developing your list of potential solution providers and entering into discussions with them. This will help create the list of potential vendors.
- Ensure your intended solution addresses your current specific authentication and fraud prevention needs and that it can expand into additional use cases, particularly when those needs emerge. A likely implementation strategy will be to start with one or two primary use cases and expand once you start seeing success.
- Understand your current authentication control framework and its strengths, weaknesses, and gaps to ascertain whether new tools and capabilities are necessary or whether your current solution simply requires augmentation. Also, ensure that any new solution supports a straightforward integration within your existing technology stack.
- Evaluate the solution efficacy of the finalist vendors through a bakeoff, if possible, and discussions with client references—either provided by the solution provider or those sourced through your professional network. Many of the behavioral biometric and device fingerprinting solutions appear similar in terms of functionality, but performance can vary widely.
- Understand budget parameters and perform a total cost of ownership before making any purchasing decision, as usage costs over time can be more expensive than a larger initial purchase price.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:
sales@datos-insights.com

Press inquiries:
pr@datos-insights.com

All other inquiries:
info@datos-insights.com

Global headquarters:
6 Liberty Square #2779
Boston, MA 02109
www.datos-insights.com

Author information

Jim Mortensen
jmortensen@datos-insights.com

David Mattei
dmattei@datos-insights.com

Gabrielle Inhofe
ginhofe@datos-insights.com