Aite Novarica

DECEMBER 2021

AITE MATRIX: LEADING FRAUD & AML MACHINE LEARNING PLATFORMS

FINANCIAL CRIME DETECTION'S NEXT FRONTIER

TRACE FOOSHÉE
CHARLES SUBRT

IMPACT REPORT

TABLE OF CONTENTS

LIST OF FIGURES

IMPACT REPORT

DECEMBER 2021

AITE MATRIX: LEADING FRAUD & AML MACHINE LEARNING PLATFORMS

Financial Crime Detection's Next Frontier

TRACE FOOSHÉE

CHARLES SUBRT

LIST OF TABLES

INTRODUCTION

The impact that financial crime has on the financial services industry continues to expand and with it, the pressure to find innovative strategies and solutions for striking a more optimal balance between loss reduction, client experience, operating efficiency, and regulatory compliance. Fortunately, as the criminal elements have become better organized and more sophisticated, so too have the risk management strategies and, importantly, the detection systems and practices for disrupting the criminals' activities. As the adoption of advancements in applied analytics has propagated through the industry, fraud and AML have proven to be among the most appealing use cases in terms of return on investment. This has transformed the market for fraud and AML solutions and, in doing so, is reshaping how fraud and AML practitioners approach the design, development, and transformation of their control frameworks.

Among the most significant developments of this evolving market are the emergence of fraud and AML detection solutions that provide FIs with the ability to optimize the performance of their controls by way of applying advanced analytical techniques to discover, develop, test, deploy, and tune highly customized detection logic and policy administration. These machine learning platforms and ecosystems have created a new segment of the market for fraud and AML detection solutions.

This Impact Report explores the evolving market for these fraud and AML detection solutions as well as the factors that FIs should consider in their pursuit of transforming their control frameworks. This 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, this report recognizes specific vendors for their strengths in critical areas.

METHODOLOGY

Leveraging the Aite Matrix, a proprietary Aite-Novarica Group vendor assessment framework, this Impact 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:

- Each participating vendor must have in production fraud and AML detection deployments in financial services, and its platforms must be able to support the deployment of (and have in production) customized machine learning analytics across multiple fraud and AML use cases.
- Each participating vendor must be able to support supervised and unsupervised model development, native custom model development authoring environments, the capacity to import and export custom model coding, on-premises and cloud-based deployments, and a robust set of APIs that enable external systems to trigger runtime execution of risk scoring tests that output results in real time.
- Each participating vendor must have had more than US$25 million in annual revenue in one of the last two prior years.

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

To further develop an overview of the trends and capabilities shaping the fraud and AML machine learning solution market, additional information to produce this Impact Report was collected through surveys and interviews with financial crime executives at FIs across the globe, along with desk research.

THE PLAYERS

This section presents comparative data and profiles for the individual vendors that were formally assessed in this Aite Matrix evaluation. This is by no means an exhaustive list of vendors, and firms looking to undergo 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 evaluated solutions.

TABLE A: EVALUATED VENDORS

FIRM	HEADQUARTERS	YEARS IN BUSINESS	TARGET MARKET	NUMBER OF EMPLOYEES	NUMBER OF MACHINE LEARNING CLIENTS
ACI Worldwide	Miami, Florida	46	Issuers, processors, intermediaries, acquirers, merchants, central infrastructures, and payment service providers—covering the entire payment ecosystem	4,000	220
DataVisor	Mountain View, California,	7	Financial services, insurance, airline, telecom, internet, e-commerce, and marketplaces	Over 140	75
Featurespace	Cambridge, U.K.	13	FIs, issuing and acquiring processors, and insurance and gaming firms	334	44
Feedzai	San Mateo, California	12	FIs, large merchants, issuing processors, and acquiring processors	500	67

FIRM	HEADQUARTERS	YEARS IN BUSINESS	TARGET MARKET	NUMBER OF EMPLOYEES	NUMBER OF MACHINE LEARNING CLIENTS
GBG	United Kingdom	31	Banks, fintech firms, building societies, credit unions, digital banks, remittance, person-to-person lending, auto finance and auto leasing, and insurance	1,000	3
INFORM	Aachen, Germany	51	Banking, payment service providers, insurance, and telecommunications	850	75
ISoft	Saint Aubin, Paris, France	31	FIs, payments processors, insurance, and e-commerce merchants as well as governments	60	Not disclosed
LexisNexis Risk Solutions	Alpharetta, Georgia	21	FIs, healthcare, insurance, payment processors, government, hospitality/gaming, communications, mobile, media, utilities, social media, software services, money transfer, and logistics	9,000	Not disclosed
NetGuardians	Yverdon-les-Bains, Switzerland	11	Top-tiered banks (through partners and the standard solution)	Over 90	53

FIRM	HEADQUARTERS	YEARS IN BUSINESS	TARGET MARKET	NUMBER OF EMPLOYEES	NUMBER OF MACHINE LEARNING CLIENTS
NICE Actimize	Hoboken, New Jersey	22	FIs, credit unions, insurers, midsize to small businesses, payments providers, gaming, and casinos	Over 1,600	430
SAS	Cary, North Carolina	45	FIs, issuing processors, acquiring processors, and merchants	13,939	120

Source: Vendors

THE MARKET

The tide of financial crime continues to rise and with it, a continued increase in market activity for detection solutions in general. As more FIs seek to transform their legacy control frameworks into those that more closely resemble the emerging control framework model, machine learning platforms will likely enjoy an increasing share of the overall market, though much of this adoption will likely be additive rather than cannibalistic.

The following market trends are shaping the present and future of the market for fraud and AML machine learning platform solutions (Table B).

TABLE B: MARKET TRENDS AND HOW THEY SHAPE THE FRAUD AND AML MACHINE LEARNING MARKET

MARKET TREND	IMPACT
Demand is strong and growing for platform and ecosystem-based risk engines that are abstracted from signal detection systems.	FIs that have the resources and capabilities to support transforming their legacy control frameworks with machine learning platforms and ecosystems will enjoy benefits from improvements to detection rates, accuracy, and operating efficiency that outpace the benefits from making incremental improvements to legacy control framework models.
The number of vendor solutions has been increasing as the scope and sophistication of financial crime expand.	As control frameworks have expanded to mitigate risks, solution providers have sought to meet expanding demand through innovations in their core technology, how they position themselves in the control framework, and which segments of the market they emphasize. Practitioners have responded by rethinking relevant use cases and the overall control framework models. Moreover, the overall scope of the market has expanded to include nonfinancial organizations such as merchants.

MARKET TREND	IMPACT
The barriers that have inhibited FIs from adopting and maturing their capacity to leverage advanced analytical techniques will remain a headwind to adoption but will diminish as vendors improve model development automation and guidance.	The market for machine learning platforms and, perhaps especially, ecosystems will expand as an increasing number of FIs mature their nascent data science capabilities and as more vendors continue to advance model development automation, guidance, and documentation features.
Differences between fraud and AML (e.g., financial crime operational structures, ownership, needs, regulatory context) have driven divergent approaches to how solution providers approach the market.	As the convergence movement and control framework models, along with experience with emerging segments of those models (like those that leverage machine learning), continue to mature, an increased adoption of solutions that support a cohesive approach and a more robust range of use cases is likely.
Differences in the needs, resources, and risk appetites of big and small financial organizations have played (and will continue to play) a huge role in how the market is structured.	As the needs among smaller, midsize, and larger institutions mature, the approaches that solution providers take will get more nuanced as niches emerge and market opportunities are exposed. As differences solidify and the niches stabilize, so too will the smaller segments of the market and the players in it.
One of the biggest drivers in innovation has been the adoption and proliferation of applied analytics and advancements among both the practitioners and the solution providers in terms of the degree to which they use and benefit from these practices.	Many firms want the benefits of applying advanced analytics without spending the time and money necessary to mature their capacity to develop and manage the data science. Taken as a discrete group, these firms represent a segment of the market that is interested in prepackaged offerings that feature lower costs and increased time to value, often at the expense of less agility and flexibility in terms of use cases or functionality. This has been a significant driver behind Software-as-a-Service (SaaS) offerings and the increasing push for offerings targeting the non-data scientist.

MARKET TREND	IMPACT
Regulators are becoming less averse to the adoption of advanced detection systems, such as those that machine learning platforms and ecosystems leverage. Yet, along with increased adoption of solutions with advanced analytics has come the need to provide more transparency for regulators.	Receding concerns over the use of machine learning modeling to manage detection logic and the continually maturing nature of model risk management processes will add fuel to the additive growth in the market for machine learning platforms and ecosystems.

Source: Aite-Novarica Group

KEY STATISTICS

This section provides information and analysis on key market statistics related to the fraud and AML machine learning platform vendor market.[1]

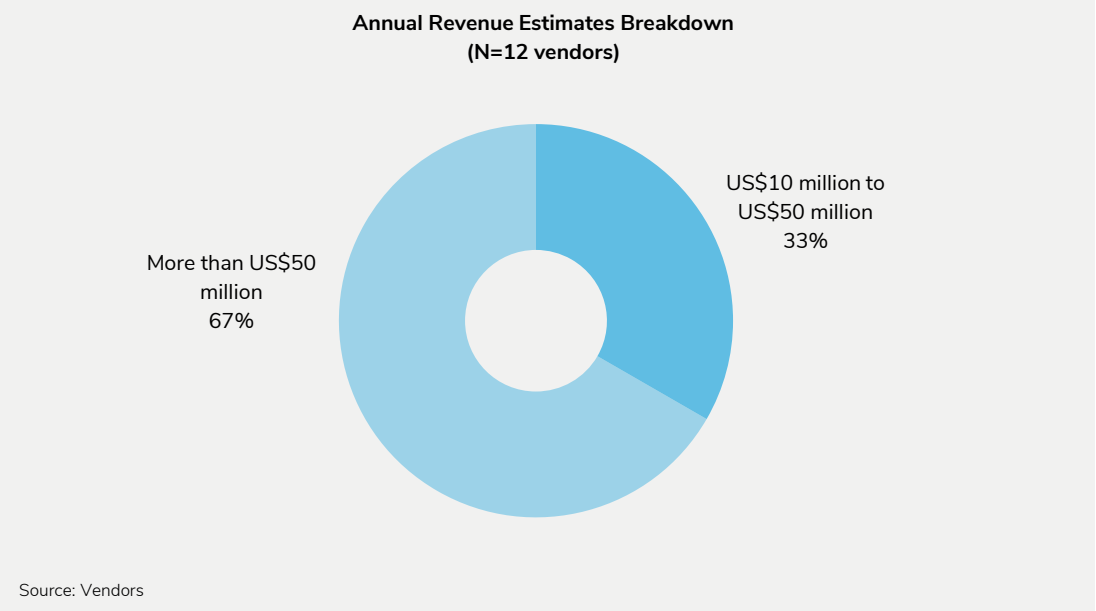
ANNUAL REVENUE ESTIMATES ANALYSIS

The vendors that provide machine-learning-enabling platforms consist of both long-time established market incumbents and relatively new entrants. Well-established providers have strong client bases, robust revenue streams, and financial strength. Many of these companies are publicly owned enterprises generating annual revenue substantially over US$50 million. Compared to their more established peers, new enterprises generate lower annual revenue but they are penetrating the market, including neobanks, fintech companies, merchants and enterprises outside the financial industry.

In 2019, when Aite-Novarica Group last completed this vendor evaluation, half of the vendors evaluated earned more than US$50 million in revenue per year. In 2021, with the accelerated growth of the market, two-thirds of the vendors evaluated earn more than US$50 million in revenue per year. Long-time firms such as SAS generate significantly more (Figure 1).

1 The key statistics within this section relate to the 12 vendors that participated in the Aite Matrix; however, one vendor opted out before the completion of the evaluation.

FIGURE 1: ANNUAL REVENUE ESTIMATES ANALYSIS

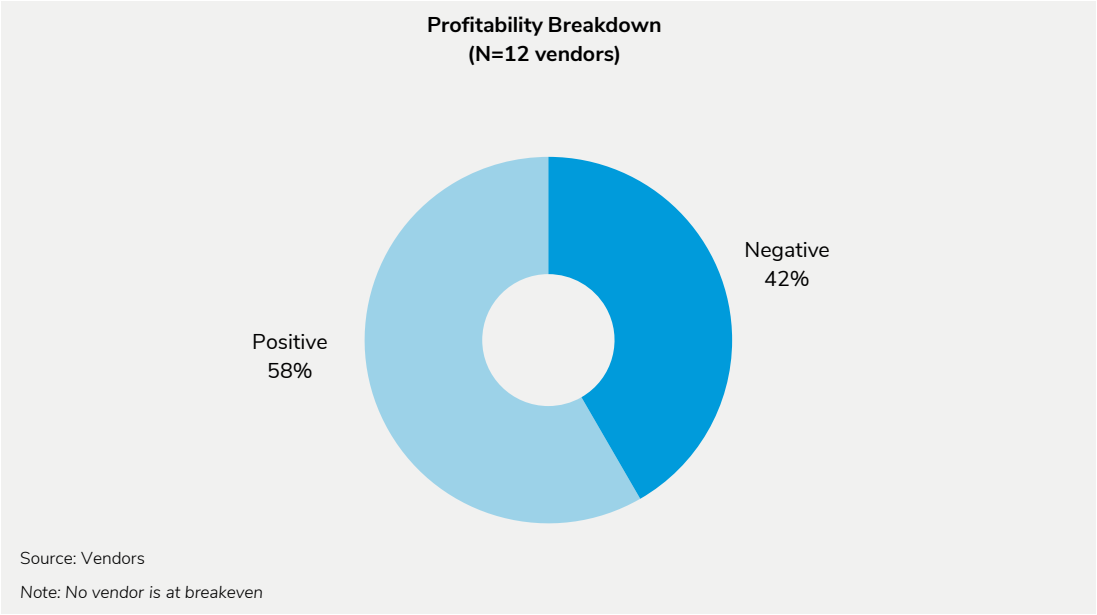


Source: Vendors

PROFITABILITY ANALYSIS

More than half of the participating vendors (58%) generate a profit. Many with negative profitably are relatively new enterprises that continue to invest significantly in R&D (Figure 2). It is interesting to note that nine of the 12 participating vendors generate more than 50% of their annual revenue from machine learning solutions.

FIGURE 2: PROFITABILITY ANALYSIS



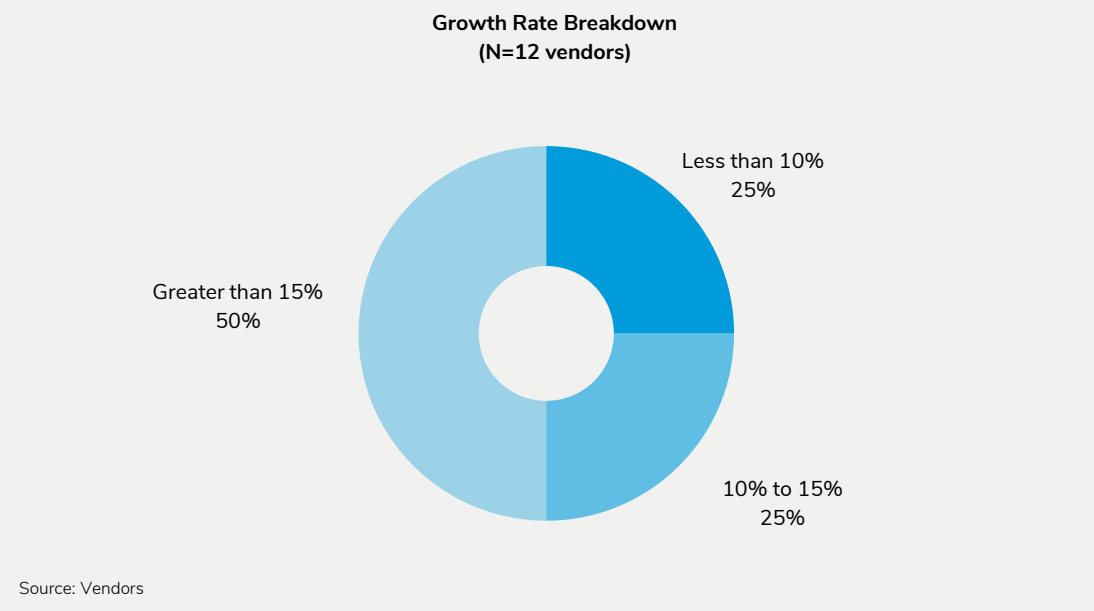
Source: Vendors

Note: No vendor is at breakeven

GROWTH RATE ANALYSIS

All participating providers reported as growing. Half increased annual revenue by more than 15%, and the remaining segment's growth rate was evenly split between less than 10% and between 10% and 15% (Figure 3). These figures illustrate the expanding appetite among financial crime executives to leverage machine learning capabilities—inside and outside of North America and Europe and beyond the traditional financial services industry—and the growing opportunities within the overall fraud and AML machine learning solution market.

FIGURE 3: GROWTH RATE ANALYSIS

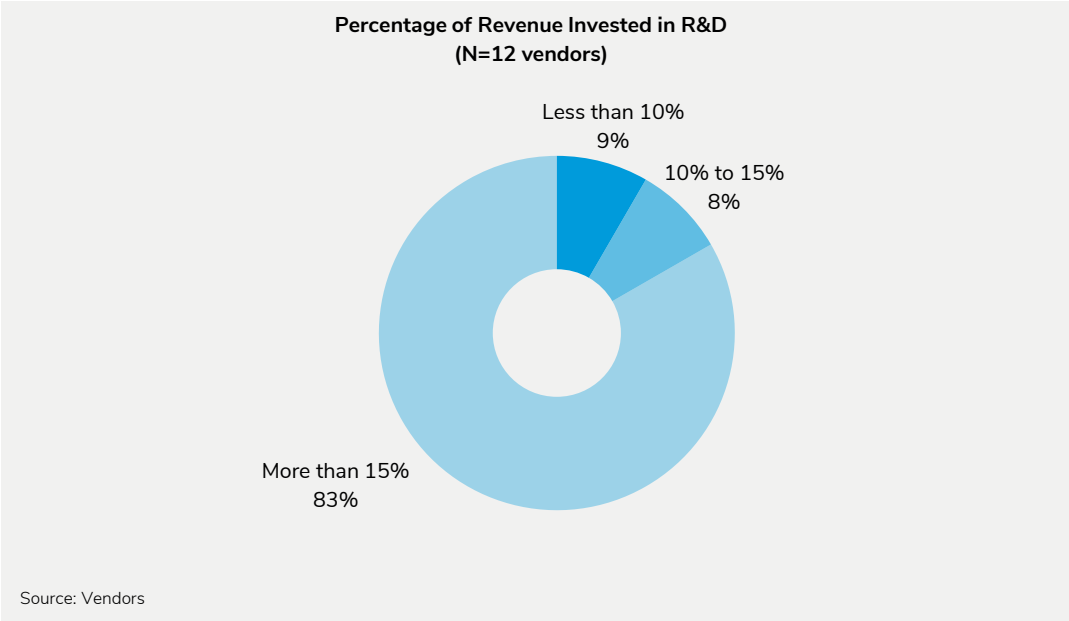


Source: Vendors

R&D INVESTMENT ANALYSIS

As firms inside the financial services industry demand better tools and data to meet increasing financial crime threats and intensifying regulatory expectations as well as more effectively tackle the ongoing business and operational challenges, vendors are continuing to invest substantially in their product suites and to expand their capabilities, functionality, and features. Otherwise, they would fall behind their competition. The vast majority of vendors (83%) in the space invest more than 15% of their revenue in ongoing R&D (Figure 4). Those vendors that fall below 15% tend to be larger vendors that have higher levels of annual revenue, thus making it harder to hit the higher percentages of revenue invested in R&D.

FIGURE 4: R&D INVESTMENT ANALYSIS



Source: Vendors

MACHINE LEARNING PRODUCTION INSTALLATION ANALYSIS

The machine learning production installation breakdown among the participating vendors illustrates that full machine learning model adoption for financial crime monitoring and detection is still in its early phase. Forty-one percent of the vendors report having a total of more than 100 machine learning model platform installations, with another 42% reporting 50 or fewer total installations (Figure 5). Yet installations are growing, as 42% report more than 10 average net new client wins for machine learning analytics production installations over the last three years, and 25% report between six and 10 net new wins over that same time period (Figure 6).

FIGURE 5: MACHINE LEARNING PRODUCTION INSTALLATION ANALYSIS

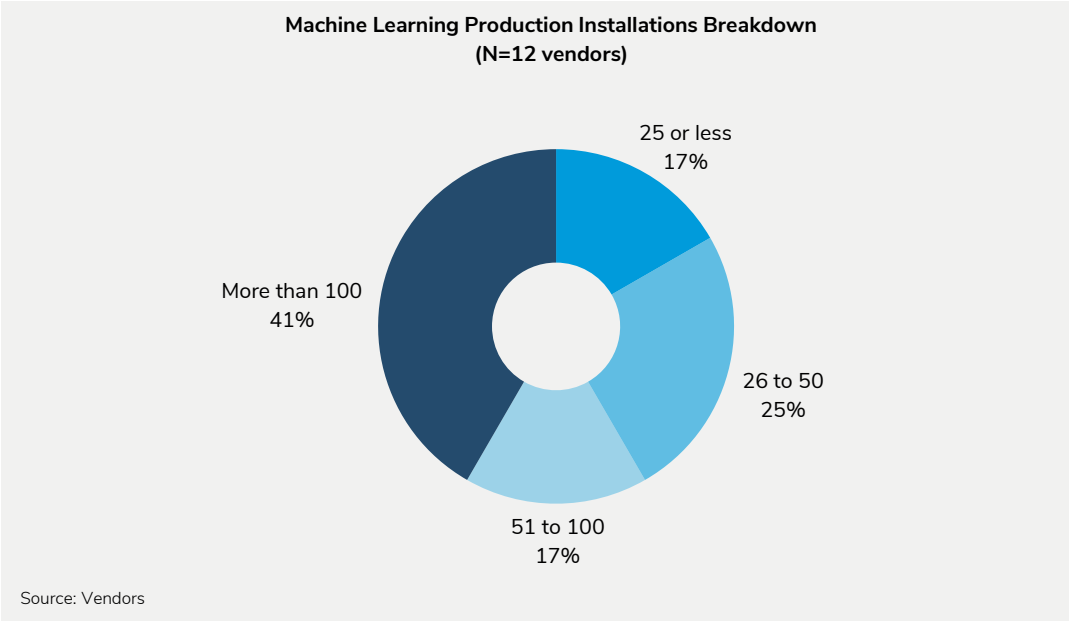
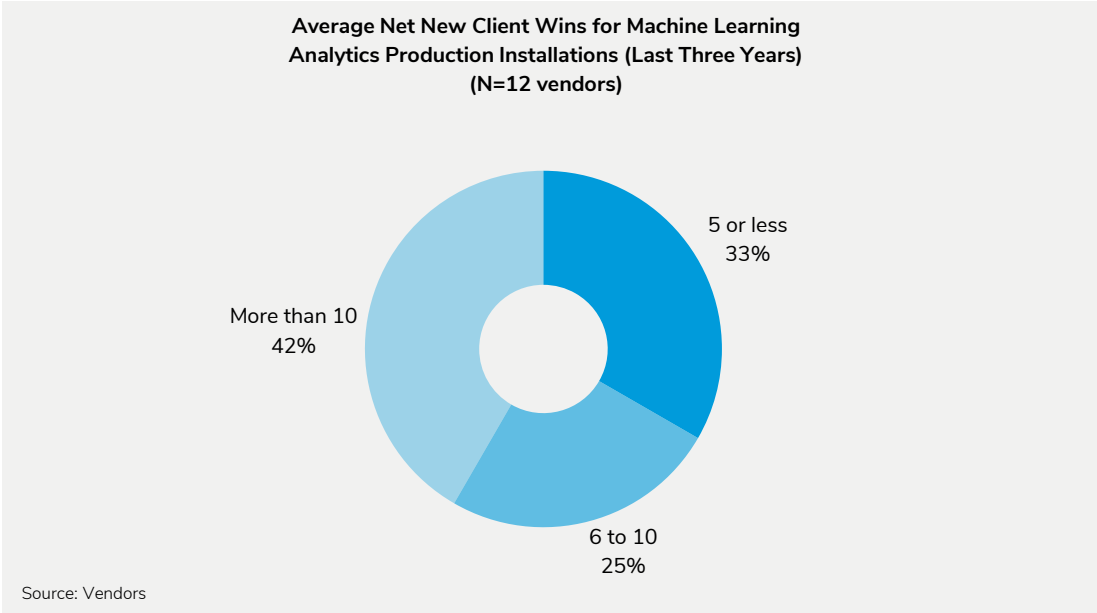


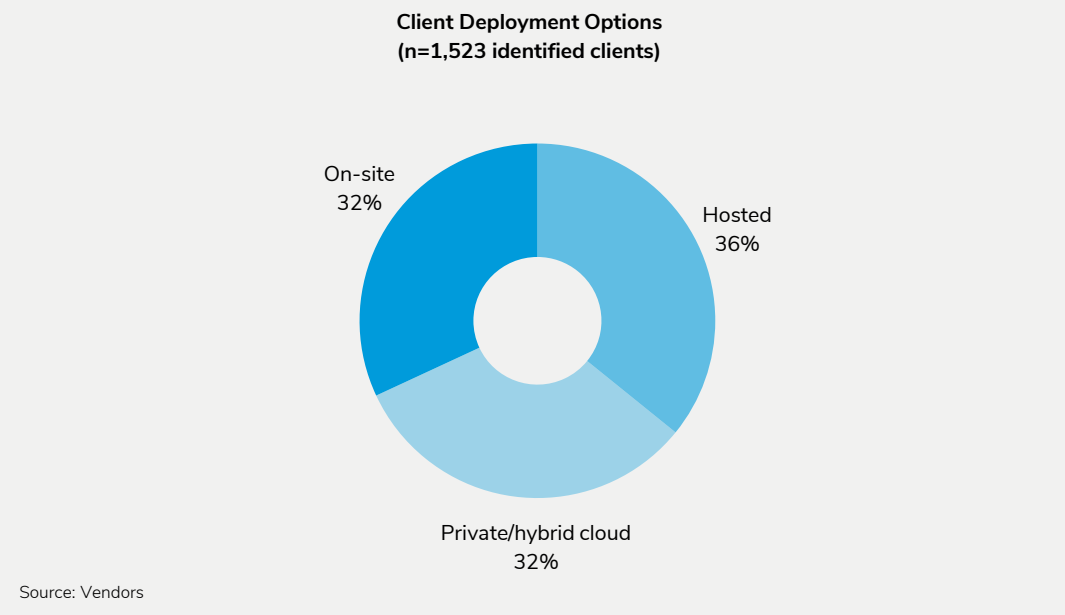
FIGURE 6: AVERAGE NET NEW CLIENT WINS FOR MACHINE LEARNING ANALYTICS PRODUCTION INSTALLATIONS



DEPLOYMENT OPTIONS ANALYSIS

Historically, financial crime units have been reticent to embrace cloud-based deployments, particularly due to concerns over data security, latency, and customization capabilities. In 2019, more than 70% of deployments were on-premises. However, that trend is changing quickly. Executives are becoming more comfortable with cloud and vendor-hosted options with the promise of facilitated integration, increased scalability and flexibility, multitenancy, and lower operational expense. As reflected in Figure 7, only 32% of deployments reported in this vendor evaluation were on-premises, with the remaining either hosted (36%) or on a private/hybrid cloud (32%).

FIGURE 7: DEPLOYMENT OPTIONS ANALYSIS



Source: Vendors

AITE MATRIX EVALUATION

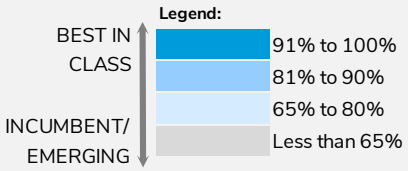
This section breaks down the individual Aite Matrix components, drawing out the vendors that are strong in each area and how they are differentiated in the market.

THE AITE MATRIX COMPONENTS ANALYSIS

Figure 8 provides an overview of how each vendor scored in the various areas of importance. Each vendor is rated, in part, based on its own data provided when responding to the RFI distributed by Aite-Novarica Group as well as on product demos and follow-up discussions as part of the Aite Matrix process. Ratings are also driven by the reference customers of the examined vendors, along with analyst knowledge of the space, to support a multidimensional rating.

FIGURE 8: AITE MATRIX COMPONENTS ANALYSIS BY HEAT MAP

Vendors	Vendor stability	Client strength	Client service	Product features
ACI Worldwide	87%	83%	77%	80%
DataVisor	84%	87%	94%	88%
Featurespace	93%	87%	95%	91%
Feedzai	95%	90%	86%	91%
GBG	93%	89%	86%	72%
INFORM	92%	87%	84%	89%
ISoft	80%	84%	80%	91%
LexisNexis Risk Solutions	89%	88%	73%	75%
NetGuardians	77%	94%	84%	78%
NICE Actimize	92%	95%	91%	86%
SAS	95%	96%	90%	93%



Source: Aite-Novarica Group

Vendor Stability

Rapidly growing and ultra-competitive, the fraud and AML machine learning platform market consist of both long-established market incumbents and relatively new entrants. Well-established providers have strong client bases, robust revenue streams, and financial strength. Many of these companies are publicly owned enterprises generating annual revenue substantially over US$50 million. Not surprisingly, many of these providers profiled in this report scored well for vendor stability.

Compared to their more established peers, new enterprises generate lower annual revenue, but they are penetrating the market, including neobanks, fintech companies, merchants, and enterprises outside the financial industry. Note that several new ventures have emerged that are making significant penetrations within the market by offering robust capabilities and data science expertise, along with strong and committed management teams and superior customer service.

SAS is among the vendors with the highest scores in this category. Profitability and corporate financial stability (a varied range of products contributing revenue) all contribute to strong performance in this category.

Client Strength

SAS scored in the best-in-class range for client strength. Key scoring drivers in this category include the total number of machine learning instances in production, client retention rate, and client reference checks on the vendor's reputation in the market.

Client Service

Strong client service has become a must to achieve customer satisfaction and demonstrate how committed a vendor is to the concept of ensuring that its customers receive the highest standard of products and services. Financial crime compliance executives often expect vendors to become strategic partners—collaborating and guiding them on near-term and long-term technology adoption. Customers continue to seek greater visibility into and enhanced documentation on current product changes as well as future product development. Customers expect quick resolution of defects and issues as well as continual advancements on design, usability, functionality, and performance.

SAS achieved high marks in this category. Client ratings of the vendor's service and support, responsiveness, ability to deliver on promises, and cost-to-value ratios were the primary drivers of the ratings in this category, along with the vendor's position on key support items, such as providing 24/7 support, having a dedicated point of contact, facilitating customer advisory boards, and offering global/localized support.

For many vendors, the overall scores indicate that client service remains a huge opportunity to achieve a competitive advantage, especially as the competition among solutions continues to escalate.

Product Features

Today's financial crime machine learning platforms are expected to enable sophisticated rule and model development, testing, validation, and deployment. Bringing a more integrated AI approach, leading solutions enable an agile orchestration of machine learning techniques and facilitate integration across disparate systems and data sources:

- Solutions should enable and support a diverse repository of both supervised and unsupervised modeling approaches, as well as multiple languages, techniques, and libraries. By investing significantly in R&D, leading vendors continually augment their portfolio of machine learning algorithms and modeling capabilities.
- To ensure quality model performance and minimize and prevent model deterioration, continuous learning capabilities are embedded to automatically retrain, tune, and deploy models when degradation is detected.
- Capabilities for ingesting, wrangling, aggregating, and enriching data are a must; doing them exceptionally well is a major differentiator.
- Solutions must also be able to clearly articulate how financial crime detection schemas operate and mitigate evolving financial crime risk. Extensive documentation, record-keeping, and audit trails are table stakes.
- A key differentiator among platforms is the nature, breadth, and depth of intelligent automation embedded across the product suite.
- Some vendors complete their offerings with rich data sets and risk and identity intelligence.
- Many solutions enable citizen data scientists and other business users to design, write, build, test, and deploy machine learning models, without significant data science expertise. Robust UIs, guided workflows, drag-and-drop tools, and reporting capabilities empower users with full control of the end-to-end model development process.

SAS edged out the rest with the highest score in this category.

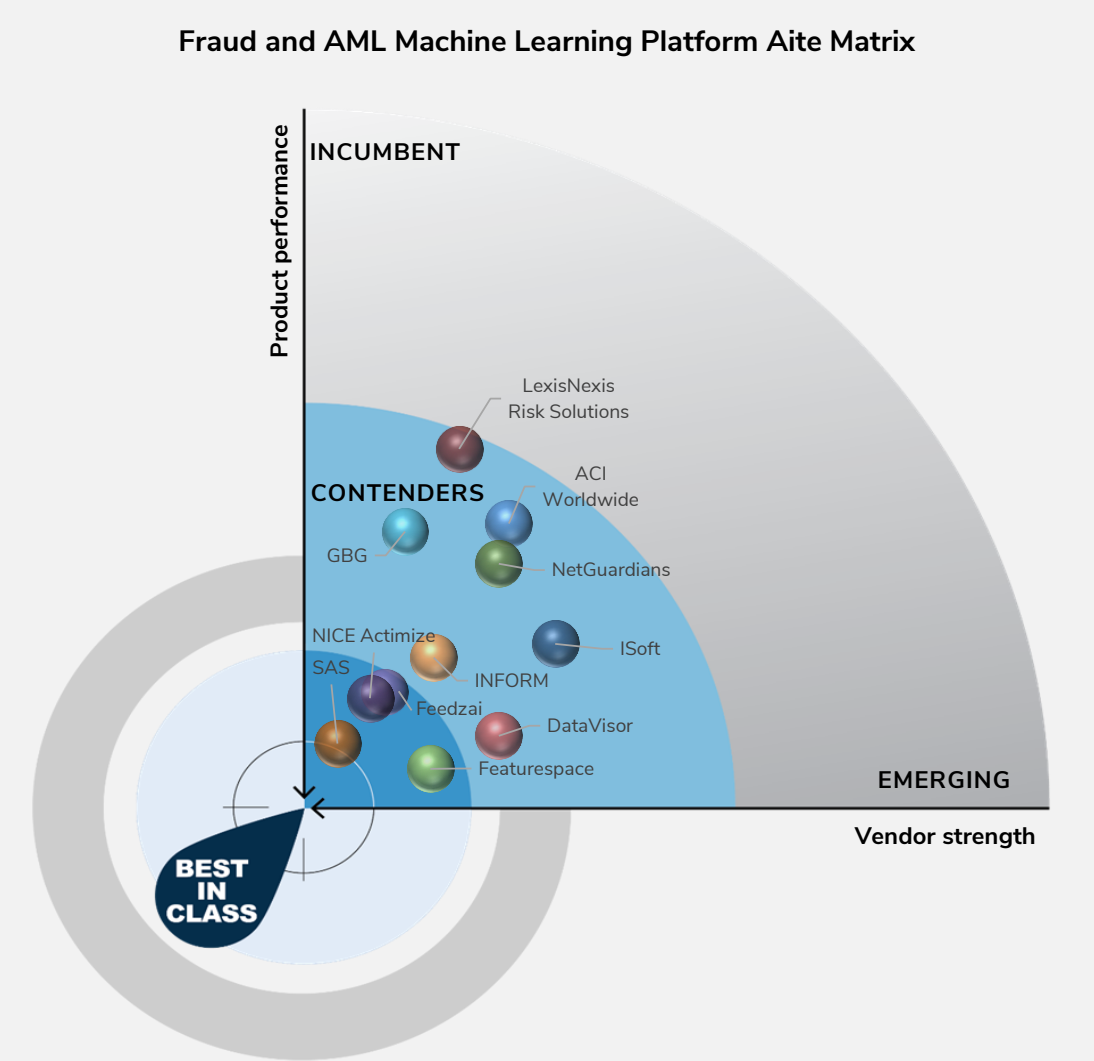
THE AITE MATRIX RECOGNITION

To recap, the final results of the Aite Matrix recognition are driven by three major factors:

- Vendor-provided information based on Aite-Novarica Group's detailed Aite Matrix RFI document
- Participating vendors' client reference feedback or feedback sourced independently by Aite-Novarica Group
- Analysis based on market knowledge and product demos provided by participating vendors

Figure 9 represents the final Aite Matrix evaluation, highlighting the leading vendors in the market.

FIGURE 9: FRAUD AND AML MACHINE LEARNING PLATFORM AITE MATRIX



Source: Aite-Novarica Group

Best-in-Class Vendor: SAS

SAS provides a cohesive, open, elastic, and scalable platform that enables high-performing advanced analytics, machine learning model development and deployment, and real-time decisioning across a diverse set of fraud and AML use cases. The SAS platform supports the end-to-end data mining process and empowers a simple, powerful, and automated engine to handle tasks across the analytics life cycle from data engineering to model development, visualization, and deployment, to ongoing monitoring and optimization.

BEST IN CLASS: SAS

Founded in 1976, SAS has been a long-standing leader of risk and data analytics for over 45 years. With customers in over 145 countries, SAS provides solutions and services focusing on customer intelligence, risk management, fraud prevention, and AML compliance. SAS' financial crimes solutions use advanced data analytics to monitor payments, nonmonetary transactions, and events, enabling businesses to identify and respond to unwanted and suspicious behavior in real time. Privately owned, SAS is dedicated to a company culture that emphasizes being a good corporate citizen.

Aite-Novarica Group's Take

Through its Financial Crimes Analytics solution, SAS aspires to build an enterprise decisioning platform that can solve a diverse array of fraud and AML problems and deliver actionable insights along the customer journey. Leveraging SAS Viya, an elastic and scalable cloud platform, the SAS Financial Crimes Analytics solution serves as a cohesive, open, high-performance platform for integrating advanced analytics and open-source languages with flexible deployment options. It is designed to provide robust end-to-end analytics life cycle support from data engineering to model development, visualization, and deployment, to ongoing monitoring and optimization.

It is an environment that can be used to build machine learning algorithms (supervised and unsupervised), such as clustering, Random Forest, logistic regressions, neural networks, deep learning, gradient boosting, and Bayesian kriging. SAS Financial Crimes Analytics provides a simple, powerful, and automated way to handle all tasks in the analytics life cycle. The SAS Financial Crimes Analytics solution enables significant out-of-the-box machine learning applications as well as automated ML. While providing robust model explainability and interpretability across the end-to-end model management and governance process, the SAS Financial Crimes Analytics solution can deliver high model performance by continuous model monitoring as well as identifying when models require retraining.

The SAS Financial Crimes Analytics solution empowers analytics team members of all skill levels with a simple, powerful, and automated way to handle all tasks in the advanced analytics life cycle. By supporting multiple use cases, the SAS Financial Crimes Analytics solution can support those firms wanting to replace existing financial crime systems as well as those looking to supplement and augment their current systems. SAS' adaptive learning capability enables clients' data scientists or data analysts to build

custom machine learning models themselves. The solution provides a suite that helps with feature identification and creation of machine learning models using a variety of algorithms, then facilitates side-by-side comparisons of model performance using the client's historical data.

In-market use cases for SAS' machine learning models include application and identity fraud, payment fraud (these support functions such as scoring for risk identification and mitigation), dynamic segmentation, scenario replacement, alert scoring for prioritization, and hibernation.

Basic Firm and Product Information

- **Headquarters:** Cary, North Carolina
- **Founded in:** 1976
- **Number of employees:** 13,939
- **Ownership:** Privately owned
- **Global business footprint:** The company has offices in the U.S., Canada, Europe, the Asia-Pacific, Latin America, the Middle East, and Africa.
- **Key product names:** SAS Financial Crimes Analytics
- **Target customer base:** FIs, issuing processors, acquiring processors, and merchants
- **Number of machine learning clients:** 120
- **Global footprint:** The company has clients all around the world.
- **Modeling:**
  - Canned and custom models
  - Vendor-developed and maintained models
  - Support for import of external models
  - Up to 50,000 transactions per second supported
  - Automated feature generation functionality
- **Implementation options:** On-site and cloud
- **Product version frequency schedule:** Minor releases are published quarterly, and major releases are published annually.

- **Pricing structure:** Pricing is based on a tiered approach tied to a firm's total assets. An additional fee may be charged for custom model development services and support.
- **Percentage of revenue invested in R&D:** More than 15%

Key Features and Functionality Based on Product Demo

- Leveraging Jupyter Notebooks, users can access SAS analytics and employ coding interfaces, visual interfaces, or open-source languages.
- Low-code/no-code UI supports the end-to-end data mining and machine learning development process.
- The workflow manager component enables solution users to test and compare analytical models with a web-based interface that supports ongoing model performance, efficiency, and governance.
- Leveraging a behavior-based approach, unsupervised techniques define and segment different customer groups, enabling different thresholds under transaction monitoring scenarios for each customer group.
- Auto-tuning can be used to automatically adjust the hyperparameters to the best values. SAS hyperparameter tuning minimizes or maximizes the chosen objective function primarily by using the preferred method that includes genetic algorithms, grid search, random sampling, Latin hypercube sampling, or Bayesian kriging.
- By aggregating alerts together, the solution can continually risk rate customer behavior to target the riskiest activities.
- Using a combination of visual interpretability reports and explanations in simple language from embedded natural language generation capabilities, the SAS Financial Crimes Analytics solution ensures transparency with explainable AI and machine learning models. For increased model efficiency, the solution integrates model retraining within the model pipeline processing environment.
- The SAS Business Orchestration Services platform can act as a central platform for integrating, managing, and designing complex and real-time strategies with internal and external data as well as third-party service providers.

- Out-of-the-box entity resolution capabilities facilitate creation of single customer views from disparate data sources.

Top Three Strategic Product Initiatives Over the Past 12 to 18 Months

- To improve advanced analytics (with a focus on digital and merchant use cases), integrated more data sources (e.g., device and behavior information) for session and authentication monitoring (including identity fraud)
- To enhance analyst and user experience, updated the capabilities for forensic searches and discovery, authoring, alert triage, and distribution to mobile experiences
- Enhanced exploration, KPI dashboards, and operational management through elevated visualizations and user interfacing

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

- The vendor will increase integration of machine learning capabilities (e.g., dynamic alert scoring, behavior monitoring, dynamic segmentation, and automated triage). SAS will emphasize the administration and management of the model life cycle within its Financial Crimes Analytics solution.
- It will increase integration of robotic processing automation to drive efficiency in operations, including automated data collection, adaptive workflows, NLP, NLG, and visualization.
- It will implement choice and control strategies to deploy SAS Financial Crimes Analytics in a cloud-native architecture that consumes open-source analytics and leverages containers.

Client Feedback

SAS continues to bring a strong reputation for advanced analytics, and client references are complimentary of the strength of the management team as well as SAS' reputation in the market. One bank client noted that SAS is always available and accessible, especially when issues and challenges arise, and its advisory and support services are of the highest quality.

Clients are pleased with solution performance and ease of integration with existing technology ecosystems. One bank client complimented SAS' robust platform, which facilitates all required AML model risk governance and testing mandates, as well as its very transparent infrastructure, which is able to document all change management across all environments in a single environment. Another bank client has introduced dynamic segmentation, alert risk scoring, and hibernation into its AML transaction monitoring program. Customized to fit the bank's needs and requirements, deployment reduced false positive alerts as well as optimized investigation practices. Another client commended the SAS predictive risk score for new fraud trends and patterns and transaction processing power.

Table C displays SAS' strengths and improvement opportunities.

TABLE C: KEY STRENGTHS AND IMPROVEMENT OPPORTUNITIES—SAS

STRENGTHS	IMPROVEMENT OPPORTUNITIES
Superior model performance	More real-time adaptive learning scoring
Excellent support and advisory services	An improved UI (although the client expected that enhanced functionality will come with a planned upgrade)
Ease of implementation and integration	Easier upgrade cycles, especially when attempting to integrate new functionality

Source: Aite-Novarica Group

CONCLUSION

Despite the variety of barriers to adoption that have kept many FIs' machine learning ambitions less than optimally realized, investment in these platforms has remained and is forecast to continue its robust growth. The benefits of applying machine learning risk models to fraud and AML use cases have created a thriving market that is only expected to grow as the dimensions and sophistication of criminal enterprises expand.

- Much benefit can be realized from the flexibility afforded by machine learning platforms, largely in terms of expansion into future use cases as well as their capacity to streamline and consolidate shared overlapping elements of the financial crime control framework.
- It's important that firms understand, as objectively and honestly as possible, their strategic approach to maturing their financial crime control framework. Firms must focus on the solution providers that are well-positioned to meet their particular needs and circumstances not only in the present but also in a manner that won't restrict the capacity and potential for developing and expanding into more robust analytical capabilities in the future.
- FIs must be cautious about overestimating the degree to which their data science capabilities will mature in such a way that will enable them to optimize the benefits of developing and deploying their own risk models as opposed to leveraging the capabilities and offerings provided by third-party solution providers.

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group 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. The quality of our research, insights, and advice is driven by our core values: independence, objectivity, curiosity, and integrity.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Trace Fooshée
+1.857.406.3515
tfooshee@aite-novarica.com

Charles Subrt
+1.617.338.6037
csubrt@aite-novarica.com