datos INSIGHTS

April 2025

Beyond Point Solutions: Orchestrating the Future of Fraud Prevention

Jim Mortensen and Gabrielle Inhofe

This report provided compliments of:

ALLOY

April 2025

Beyond Point Solutions: Orchestrating the Future of Fraud Prevention

Jim Mortensen and Gabrielle Inhofe

Table of Contents

List of Figures

List of Tables

Introduction

FIs face mounting pressure to prevent fraud across an expanding array of payment types, channels, and threats while maintaining as frictionless a customer experience as possible. The difficulty of managing multiple point solutions, data providers, and risk assessment tools has accelerated the demand for fraud orchestration platforms, which can coordinate these various components effectively and build more detailed pictures of customers and their risk profiles. The increasing speed of business and transactions, along with a rapid evolution of fraud tactics and regulatory requirements, adds further complexity to an already challenging landscape, requiring solutions that can adapt quickly.

Fraud orchestration can mean different things and apply to a variety of use cases. In general, these platforms serve as central hubs for managing fraud-prevention strategies, enabling FIs to implement sophisticated, multilayered approaches to risk assessment and fraud detection. These platforms coordinate the interaction between various tools, data sources, and decision engines while providing unified case management and reporting capabilities. The platforms must integrate seamlessly with existing bank infrastructure while maintaining strict performance requirements. They enable intelligent routing of transactions to appropriate verification and authentication services based on risk level, cost considerations, and business rules.

This report examines a cross-section of third-party vendors and their fraud orchestration solutions, understanding their capabilities, deployment models, and product roadmaps. It reviews how each solution coordinates multiple fraud-prevention services and provides flexibility to adapt to emerging threats and changing business requirements. The report's insights will help FIs better understand the fraud orchestration market, how to differentiate the different types of solutions, and how to develop a centralized fraud management strategy that works best for them.

Methodology

The report draws on data collected directly from 13 participating vendors and through interviews with 19 fraud-prevention executives regarding their organization's needs and plans regarding fraud and orchestration capabilities. The participating vendors included ACI Worldwide, Alloy, DataVisor, Demyst Data, Experian, Featurespace, FICO, GBG, LexisNexis Risk Solutions, NICE Actimize, Provenir, Transmit Security, and TransUnion.

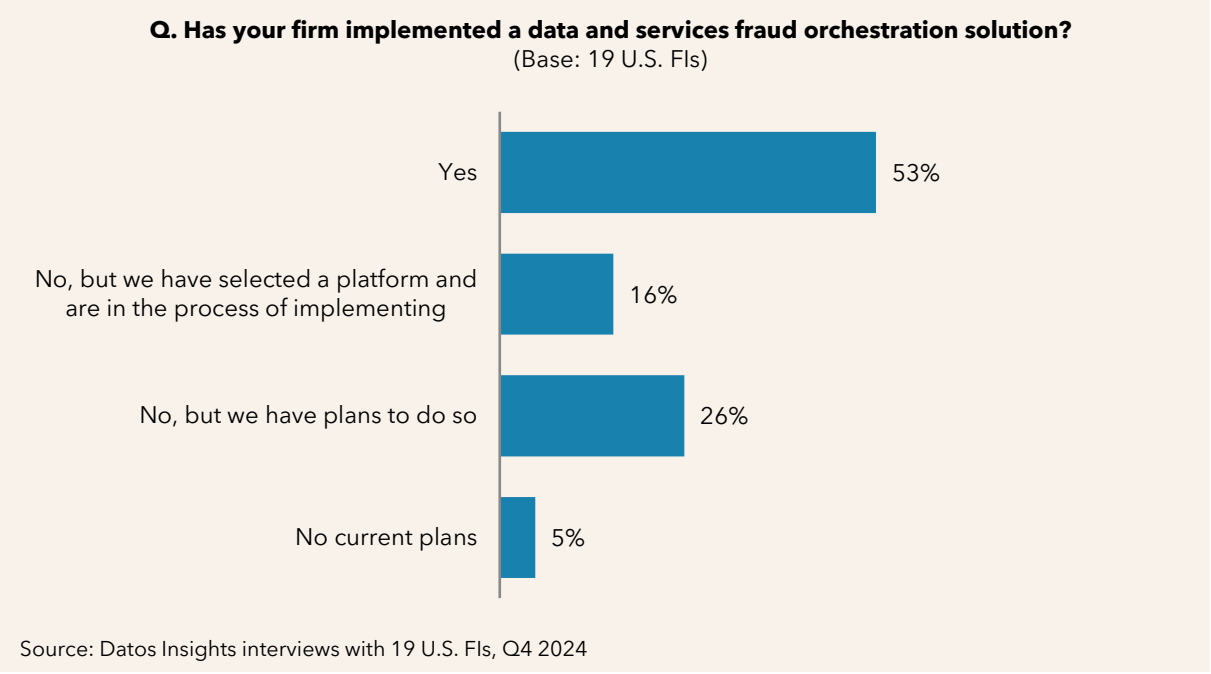
Each profiled vendor completed a detailed questionnaire and presented a product demonstration.

The market continues to mature as vendors invest in enhanced capabilities while maintaining focus on scalability, flexibility, and ease of use. Organizations evaluating orchestration solutions should carefully assess their specific needs against provider capabilities while considering factors such as deployment options, integration requirements, and support for future growth.

The Market

Financial services organizations face mounting pressure to prevent fraud while maintaining operational efficiency in an increasingly digital environment. The changing face of fraud threats compels organizations to iterate their fraud strategies more frequently so that they can respond swiftly with a high degree of certainty. However, this need for constant adaptation presents significant operational challenges that many firms struggle to overcome, particularly as fraudsters exploit gaps between different payment systems and channels. As a result, most FIs have either already implemented some sort of orchestration solution or are planning on doing so in the near future (Figure 1).

Figure 1: Orchestration Solution Plans



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

Fraud Strategy Management Challenges

Large and small institutions face several substantial barriers when attempting to implement or modify fraud-prevention strategies. Table A summarizes fraud strategy management considerations that FIs face in an increasingly complex market.

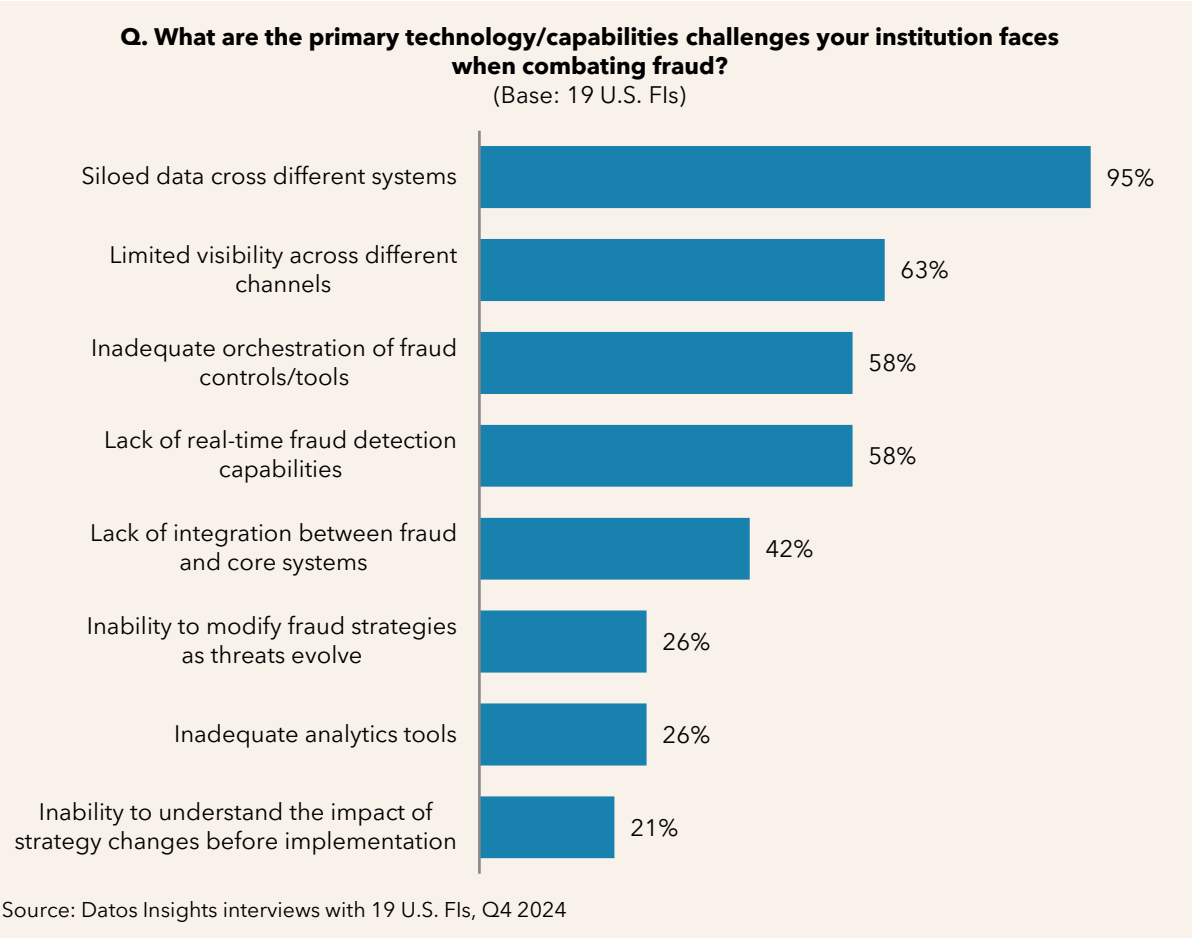
Table A: Fraud Strategy Management Considerations

Consideration	Implications
Data integration challenges	Consolidating data across products and channels presents significant obstacles. Information often exists in disparate formats with varying quality levels, complicating efforts to build comprehensive customer profiles.
Digital channel growth	The shift toward mobile and online transactions continues. Organizations can apply device data and behavioral patterns from digital channels to strengthen fraud detection while maintaining customer experience.
Digital identity management	Organizations face growing complexity in managing digital identities across multiple touchpoints. This drives demand for solutions that can coordinate an array of identity verification tools and apply appropriate verification steps based on risk level and transaction context.
Increased sophistication and complexity of fraud attacks	The tools available to fraudsters continue to advance, making detection more challenging. Organizations need expanded risk signal monitoring and verification capabilities for effective mitigation.
Understanding the customer's behaviors	Organizations aim to leverage customer behavior data to customize authentication requirements. This requires understanding transaction history and interactions across channels to consider individual customer patterns to accurately assess risk and determine the appropriate treatment.
Resource optimization	FIs face pressure to maximize fraud-prevention capabilities while minimizing vendor relationships and IT costs. This drives consolidation from multiple point solutions toward comprehensive platforms from fewer providers.
Advanced analytic technologies	The increasing capabilities and declining costs of artificial intelligence (AI) and ML technology enable solution providers to deliver enhanced fraud detection across multiple risk signals.
Regulatory changes	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.

Source: Datos Insights

Data integration, in particular, presents a significant hurdle for financial services firms: 95% of institutions surveyed indicated that siloed data was a primary challenge, and 63% reported having limited visibility across different channels (Figure 2).

Figure 2: Technical and Capability Challenges in Fraud Prevention



Source: Datos Insights interviews with 19 U.S. FIs, Q4 2024

Most organizations store customer data across multiple systems, often in different formats and with varying levels of quality. Payment data might reside in one system, while customer authentication history lives in another, and device fingerprinting data in a third. This fragmentation makes it difficult to build comprehensive customer risk profiles or implement sophisticated fraud-prevention strategies that require real-time access to multiple data sources.

IT resource limitations often create bottlenecks as well, with new systems requiring extensive resources, detailed business cases, and extended lead times. Even after approval, projects frequently face delays of three to six months before reaching the top of the IT queue. The vendor management process layers on more complexity, as internal

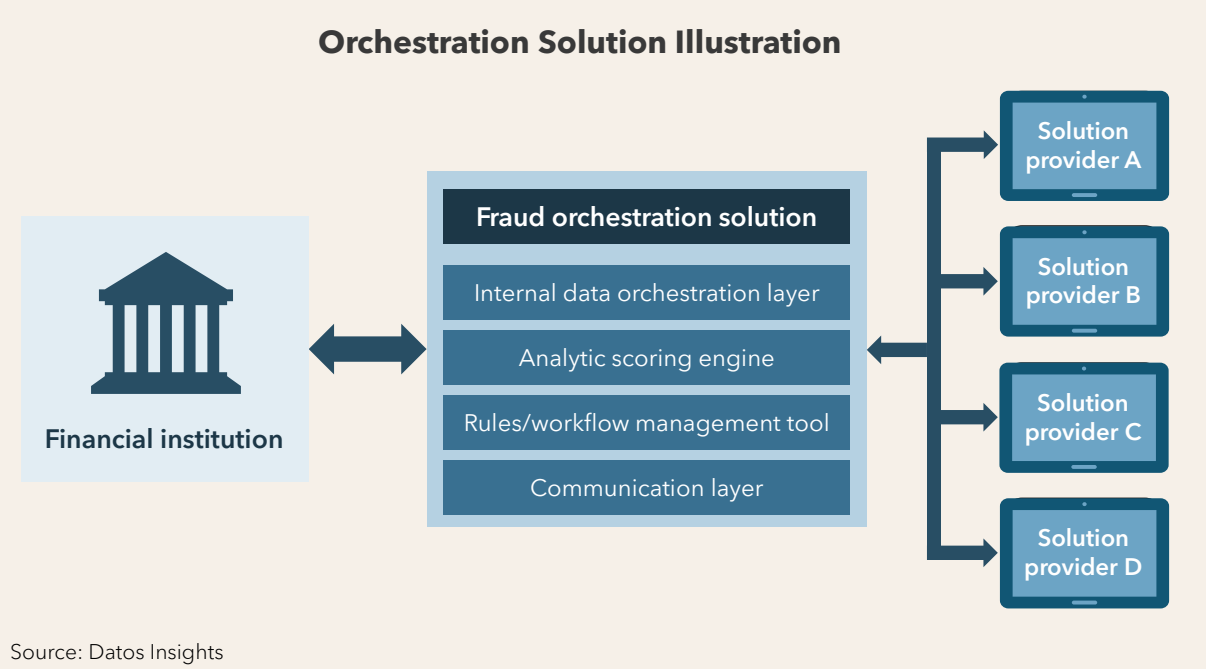
vendor risk management typically adds additional time to the cycle. This extended timeline proves particularly challenging when organizations need to respond rapidly to emerging fraud threats.

Organizations must also ensure that alerts from any number of point solutions integrate cohesively rather than adding to the workload. Many institutions operate with multiple vendor-provided fraud-prevention solutions, each generating unique alerts and potentially requiring separate investigation workflows. Without advanced risk evaluation capabilities, fraud teams become overwhelmed with duplicate alerts and struggle to prioritize investigations effectively. This challenge becomes more acute as organizations add new channels and payment types, each requiring its own set of controls and generating additional alerts.

The Orchestration Solution Approach

The orchestration solution model is a response to these challenges, offering a more integrated approach to fraud prevention (Figure 3).

Figure 3: Orchestration Solution Illustration



Source: Datos Insights

Orchestration platforms enable FIs and other organizations to connect to a range of different solution providers through a platform with capabilities that integrate internal data sources, analytically assess risk, and determine the best course of action to take. This

approach puts fraud-prevention teams in control of their risk processes and provides the ability to adapt quickly, which is critical in the world of fraud prevention.

The solutions support the integration of multiple point solutions, either native to the provider or through third-party integrations. The following breakdown outlines the primary features and functionality of an orchestration model:

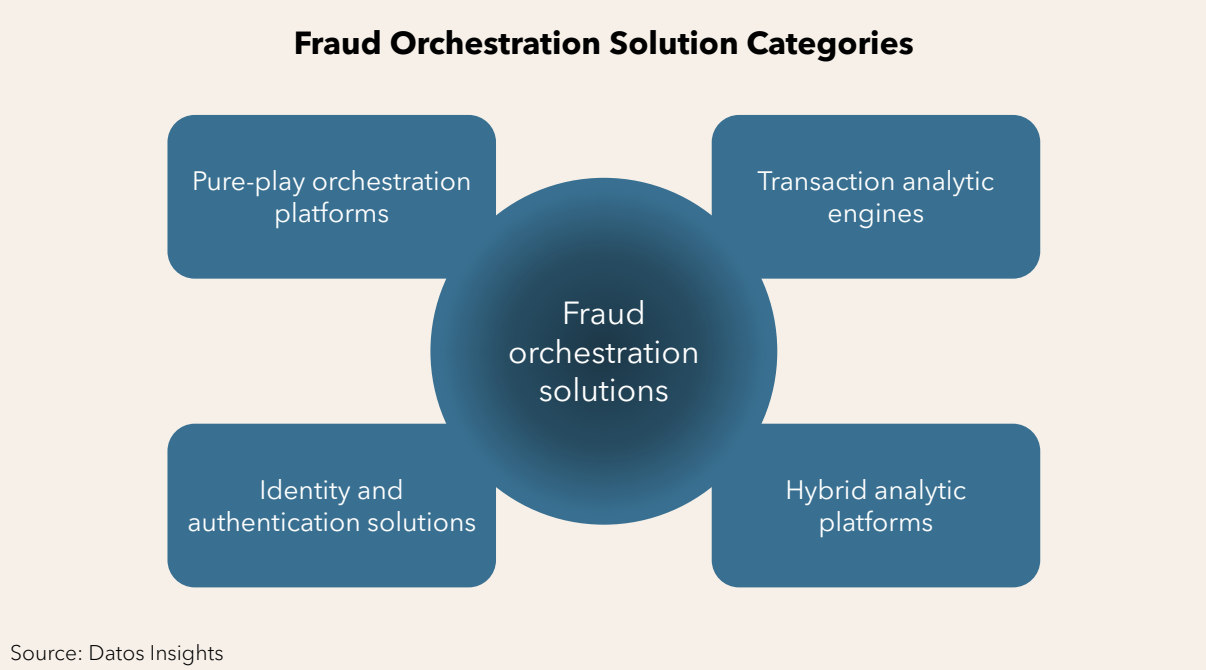
- Organizations integrate into vendor solutions through APIs, typically through a public or private cloud implementation, enabling strategy management without constant technology resource demands and delays in the IT queue. This approach allows fraud teams to test and implement new vendors, capabilities, models, or rules without requiring extensive IT support.
- They incorporate data integration layers that facilitate the combination of external solutions and internal customer data to support effective decisioning. This capability proves particularly valuable for real-time fraud prevention, where decisions must be made in milliseconds based on data from multiple sources.
- They incorporate ML-based risk engines and support custom model deployment while also providing multitenant capabilities and geographic customization. The quality of ML tools varies with the solution provider's focus and evolution.
- They provide sophisticated workflow design through graphical, drag-and-drop interfaces to allow for no-code development.
- Nearly all include capabilities for executing A/B testing of different vendors, models, and strategies, allowing organizations to optimize their fraud-prevention approach based on actual results.
- These platforms often include broad point solution marketplaces with centralized contracting. In these cases, providers maintain vendor relationships, allowing clients to operate under a single contract and reduce vendor management overhead. This marketplace approach can substantially lower implementation time compared to traditional point solution integration.

Fraud Orchestration Solution Types

The fraud orchestration market encompasses several solution types based on the core competencies of the vendors and their evolution. The main categories are pure-play orchestration platforms that coordinate third-party services, transaction analytics engines

that focus on pattern detection, identity and authentication solutions positioned that validate individuals and interactions, and hybrid platforms that combine orchestration with native analytics capabilities (Figure 4).

Figure 4: Solution Categories



Source: Datos Insights

Each solution type offers different advantages for specific use cases, though the boundaries between categories continue to blur as vendors expand their capabilities and fraud-prevention needs evolve. Vendors often combine elements from multiple categories, but understanding these core solution types helps FIs evaluate options based on their specific needs.

Pure-Play Orchestration Platforms

Pure-play orchestration platforms provide workflow management and decisioning capabilities without native fraud detection. These solutions focus on integrating and coordinating third-party data sources, verification services, and fraud detection tools through a single platform. The platforms typically offer no-code or low-code environments for building verification workflows and decision flows. Pure orchestration solutions emphasize flexibility and vendor-agnostic integration capabilities. Their value proposition centers on reducing integration complexity and enabling organizations to optimize their use of third-party services.

Transaction Analytics Engines

Transaction analytics engines focus on processing a high volume of payment and nonpayment transactions to detect fraud patterns and anomalies. These solutions typically employ ML models and rules engines purpose-built for specific transaction types like payments, account opening, or account takeover. The analytics engines excel at real-time processing and pattern recognition across large transaction volumes. Transaction analytics providers often maintain consortium databases that help identify patterns across their client base. These solutions generally offer strong performance for their targeted use cases but may require additional tools for comprehensive fraud prevention.

Identity and Authentication Solutions

Identity and authentication solutions concentrate on validating customer identities and ensuring account access security. These platforms typically combine identity verification capabilities like document validation and biometrics with ongoing authentication methods such as behavioral biometrics and device fingerprinting. The solutions often include fraud detection specific to account opening and account takeover scenarios. Identity-focused providers generally maintain identity networks or consortium data specific to identity verification and authentication patterns.

Hybrid Platforms

Hybrid platforms combine orchestration capabilities with native fraud detection and analytics. These solutions offer built-in transaction monitoring and fraud detection while also supporting the integration of third-party services and data sources. Hybrid solutions aim to reduce the total vendor count by providing core fraud-prevention capabilities while maintaining flexibility to add specialized third-party services. Their approach balances the benefits of pre-integrated fraud detection with the adaptability of pure orchestration platforms.

Key Functionality

Fraud orchestration platforms have evolved significantly to address the growing complexity of financial crime. These solutions now incorporate advanced capabilities across deployment, processing, integration, and analytics to support enterprise-scale operations. As FIs work to balance fraud prevention effectiveness with operational efficiency and customer experience, orchestration platforms deliver core functionality that helps organizations achieve these objectives:

- Cloud deployment options now dominate the market, with most vendors offering flexible implementation models, including public cloud, private cloud, and hybrid approaches. This shift enables FIs to maintain performance at scale while adapting to changing infrastructure requirements and regulatory obligations.
- Real-time processing capabilities have become table stakes, with leading solutions processing thousands of transactions per second while maintaining low response times. These performance levels demonstrate the maturity of orchestration platforms in handling enterprise-scale deployments across multiple channels and use cases.
- Point solution integration capabilities continue to expand, with providers offering hundreds of prebuilt connectors to third-party data sources and services. This expansion enables FIs to implement new capabilities quickly.
- ML model management capabilities now support parallel model deployment and testing across multiple model types, including proprietary, custom, and third-party models. This flexibility allows organizations to leverage various analytical approaches while maintaining consistent governance and monitoring.
- Low-code/no-code interfaces are becoming standard features as providers seek to empower business users in strategy management and model development. These capabilities reduce dependence on technical resources while enabling fraud teams to respond more quickly to emerging threats.
- Device intelligence and behavioral biometric capabilities are increasingly embedded within orchestration platforms rather than requiring separate point solutions. This integration improves fraud detection effectiveness while reducing implementation complexity and maintaining consistent customer experiences.
- Cross-channel visibility and unified case management help organizations identify fraud patterns that might otherwise go undetected when channels are monitored in isolation. These capabilities enable more efficient investigation processes while improving detection rates across different payment types and channels.

The maturation of these platforms reflects the financial services industry's need for comprehensive, scalable fraud-prevention capabilities. These solutions have advanced beyond basic integration and workflow management to provide advanced analytics and channel-agnostic fraud detection. FIs evaluating orchestration platforms should assess

how these key capabilities align with their specific operational requirements, risk-management objectives, and technology infrastructure.

Fraud Orchestration Market Sizing

Datos Insights estimates the fraud orchestration solution market at about US$2.094 billion in 2024 (Figure 5). This market sizing focuses specifically on fraud orchestration capabilities and associated integration services, excluding, to the extent possible, revenue from other risk-management functions. Additionally, the market estimate considers primarily enterprise-level deployments, as smaller implementations often rely on fraud-prevention capabilities embedded in their core processing or payment platforms.

Figure 5: Fraud Orchestration Solution Market Size

Source: Datos Insights

The market is expected to grow consistently to US$3.662 billion in 2028, representing a compound annual growth rate of 15%. This growth trajectory reflects increasing demand for solutions that can coordinate multiple fraud-prevention tools and data sources. The market size also assumes substantial ongoing investment by FIs and other organizations in modernizing their fraud-prevention infrastructure. The 2024 baseline of US$2 billion demonstrates that orchestration has moved beyond early adoption to become an established market segment.

Provider and Key Functionality

Datos Insights looked at Alloy, which offers fraud orchestration capabilities.

Table B: Orchestration Solution Providers

Provider	Product name	Headquarters	Founded	Employee count
Alloy	Alloy Platform	New York	2015	250

Source: Datos Insights, Solution Providers

This vendor represents different approaches to orchestration with the same objective of preventing fraud through the integration of internal and external data sources, the application of advanced analytics, and the ability to leverage identity, authentication, and other risk services.

Platform Functionality

Table C provides an overview of core functionality, high-lighting key differentiators in risk coverage and technical capabilities.

Table C: Orchestration Platform Key Functionality

Solution provider	Risk areas	Analytic capability	Self-service integration	Native data consortium	Embedded finance
Alloy	• Fraud/AML • Compliance • Credit	• ML • Rules engine	■	■	■

Source: Datos Insights, solution providers

Key: ■ = Yes, ☐ = No, ◪ = Via a partner, ○= Plans to/will offer in the future

The functionality comparison reveals some variation in orchestration, with most providers supporting multiple risk types and offering ML capabilities. The following highlights key observations:

- Self-service integration capabilities, which allow users to directly add point solution providers, are present in roughly half of the solutions, resulting in some differences in approaches to implementation and configuration.
- Native data consortia are widely available across providers, demonstrating the importance of shared intelligence in fraud prevention.
- About half the providers offer embedded finance capabilities, which allow nonfinancial companies to integrate financial services directly into their products while the provider manages the related risk. Several others report plans to add these capabilities to their platforms, pointing toward a trend in the market.

Deployment Models

Deployment flexibility represents a key consideration for organizations evaluating orchestration platforms, as shown in Table D. The comparison examines support for public cloud, private cloud, on-premises, and hybrid deployment models across providers. AWS emerges as the dominant public cloud platform, though some providers support multiple cloud services. Most providers offer multiple deployment options to accommodate varying client requirements.

Table D: Orchestration Platform Deployment Models Supported

Solution provider	Public cloud	Private cloud	On-premises	Hybrid
Alloy	■	□	□	N/A

Source: Datos Insights, Solution Providers

Key: ■ = Yes, □ = No

Cloud deployment dominates the orchestration platform landscape, with AWS serving as the primary public cloud provider. While most vendors support multiple deployment models, implementation approaches vary considerably. While public cloud represents the standard offering, several providers maintain on-premises capabilities for organizations with strict data residency requirements. Hybrid deployments bridge these approaches, enabling firms to maintain sensitive data on-premises while leveraging cloud capabilities for other functions.

Identity and Authentication Capabilities

Identity verification and authentication capabilities represent critical components of orchestration platforms as FIs face increasing pressure to prevent account takeover fraud while maintaining streamlined onboarding processes. The ability to coordinate multiple verification methods—from document scanning to behavioral biometrics—enables FIs to apply risk-appropriate authentication without creating unnecessary friction.

Table E examines how orchestration providers deliver these capabilities, distinguishing between native functionality and partner-provided services across key verification methods, including document verification, personally identifiable information (PII) validation, bank account verification, behavioral biometrics, device intelligence, and mobile phone owner verification.

Table E: Identity and Authentication Capabilities

Solution provider	Document verification	PII verification	Bank account verification	Behavioral biometrics	Device intelligence	Mobile phone owner verification
Alloy	◪	◪	◪	◪	◪	◪

Source: Datos Insights, Solution Providers

Key: ■ = Native, ◪ = Via partner, ○ = Plans to/will offer in the future, □ = No or N/A

Device intelligence and PII verification emerge as core competencies among orchestration providers, with over half offering these capabilities natively. In contrast, bank account verification and mobile phone owner verification remain largely partner-dependent functions across the market. This reveals many providers focus internal development on capabilities that benefit from direct integration with their risk engines while partnering for functions requiring specialized infrastructure or regulated data access.

Alloy Profile

Alloy, founded in 2015 and headquartered in New York, provides an end-to-end identity risk-management platform for FIs. With approximately 250 employees and operations across North America, Europe, the Middle East, Africa, Latin America, and Asia-Pacific region, Alloy serves nearly 700 banks, credit unions, and fintech companies. The company has raised over US$210 million in funding through Series C, backed by investors including Bessemer Venture Partners, Lightspeed, Avenir, Canapi, Eniac, Avid, Primary, and Felicis Ventures.

The company's orchestration capabilities are distinguished by its extensive network of prebuilt integrations with approximately 250 solution partners. Alloy's platform allows FIs to manage identity risk throughout the customer life cycle while maintaining strict data privacy and regulatory compliance. This approach enables clients to leverage multiple data sources and services through a single integration point, providing comprehensive risk signals across onboarding and ongoing monitoring use cases.

Table I provides summary information for Alloy.

Table F: Alloy Fraud Orchestration Solution Overview

Category	Description
Product name and original release date	Alloy Platform, serving as an orchestration solution since 2015
Primary target market	• Banks, credit unions, and fintech companies across various sizes • Solution providers such as Banking-as-a-Service providers, program managers, sponsor banks, core banking processors, and digital account opening solution vendors
Existing client base	Nearly 700 FIs, including banks, credit unions, and fintech companies
Geographic coverage	Local in-market platform coverage across North America, Europe, the Middle East, North Africa, Latin America, and Asia-Pacific regions, with data-source coverage spanning 195 markets
Deployment options	Software-as-a-Service (SaaS) platform hosted on AWS cloud services

Category	Description
Current deployment mix	Multitenant SaaS platform; no on-premises or private cloud installations

Source: Alloy, Datos Insights

Solution Overview

Alloy's platform provides comprehensive risk-management capabilities across three primary verticals: fraud, compliance, and credit. The solution supports both origination and ongoing monitoring use cases, allowing organizations to manage risk throughout the customer life cycle. Unlike traditional point solutions focusing on specific risk types or channels, Alloy's platform provides an integrated view of customer risk across multiple touchpoints, including digital onboarding, account maintenance, external account linking, and ongoing account activity.

The platform supports various identity verification and risk assessment use cases:

- Banking transaction monitoring (card issuing, acquiring)
- Digital account opening
- Account maintenance monitoring
- External bank account linking verification
- Business identity verification
- Document verification

Key Components and Features

The platform's architecture enables organizations to implement components based on their specific needs while maintaining the ability to expand capabilities over time. Key components include the following:

- **Journey orchestration:** A visual workflow builder that allows organizations to create complex, multistep identity verification and risk assessment processes without coding

- **SDK integration:** Provides prebuilt front-end components for document verification, step-up authentication, and device fingerprinting that can be easily integrated into client applications
- **Testing suite:** Enables organizations to test and validate rules, perform A/B testing, and analyze the impact of policy changes before deployment
- **Investigation tools:** Provides case management capabilities for reviewing alerts and investigating potentially suspicious activity
- **Custom model integration:** Allows organizations to incorporate ML models or third-party models into decision workflows

The key features of the solution provide comprehensive risk management across all channels and touchpoints:

- **Real-time processing:** The platform processes API requests with response times ranging from 300 to 1,500 milliseconds, depending on workflow complexity. The multitenant architecture enables automatic scaling to handle increased volume.
- **Policy management:** Organizations can create and modify risk policies through a no-code interface that supports simple and complex decisioning logic using the following tools:
  - Visual workflow editor for building and testing rules
  - Version control and audit trails for policy changes
  - Role-based access control for policy management
  - Testing capabilities, including backtesting and A/B testing
- **Flexible integration options:** Supports multiple integration methods, such as REST APIs, native SDKs for web and mobile, batch processing, and webhooks for case management integration.
- **Analytics and reporting:** Provides insights into policy performance and operational metrics such as application approval rates and manual review rates, alert and investigation metrics, data-source-performance analytics, and custom reporting capabilities.

Data Providers and Risk Solution Services

Alloy maintains an extensive network of prebuilt integrations with 232 solution partners. The platform follows an "open ecosystem" approach, allowing organizations to leverage both existing vendor relationships and new services through Alloy's reseller agreements. Rather than requiring specific vendor relationships, Alloy enables organizations to select and combine services based on their specific use cases and risk factors. Table J provides an overview of Alloy's data and point solution offerings.

Table G: Alloy, Available Data and Fraud Solution Services

Service/data type	Service/data	Native/ partner	Partners
Identity verification	Document scanning and authentication	◪	BluCognition, CLEAR, GBG IDology, IDVerse, Inscribe, Ocrolus, Onfido, Persona, Socure, SumSub, Trulioo, Veriff, Vouched
	Selfie/liveness verification	◪	Onfido, Socure, Veriff, Vouched
	PII verification	◪	Mastercard Identity, Equifax, GBG IDology, LexisNexis Risk Solutions
	Business identity verification	◪	Middesk, Trulioo, D&B
	Email reputation	◪	Mastercard Identity, SentiLink, SEON, Socure
Authentication	SMS OTP	◪	Prove, Twilio
	Mobile app push OTP	◪	Prove, Twilio
	Behavioral biometrics	◪	NeuroID, BioCatch
	Device intelligence	◪	LexisNexis Risk Solutions, Prove, Socure, TransUnion
Compliance	Global sanctions lists	◪	ComplyAdvantage, LexisNexis Risk Solutions, Socure, Coris, Moody's

Service/data type	Service/data	Native/ partner	Partners
	PEP lists	◪	ComplyAdvantage, LexisNexis Risk Solutions, Socure, Coris, Moody's
	Adverse media screening	◪	ComplyAdvantage, Quantifind, Coris, Moody's
Payment verification	Bank account validation authentication/ verification	◪	Early Warning Services, Plaid, LSEG, GBG
Credit underwriting	Traditional credit data	◪	Equifax, Experian, TransUnion
	Alternative credit data	◪	LexisNexis Risk Solutions, Prism Data

Source: Alloy, Datos Insights

Key: ■ = Native, ◪ = Via partner

Planned Enhancements

Alloy's product roadmap focuses on three strategic priorities: seamless implementation, optimized investigations, and proactive risk detection. The planned improvements reflect the company's focus on operational efficiency and advanced analytics capabilities. Table K provides an overview of the company's product roadmap.

Table H: Alloy, Product Roadmap

Time frame	Description
H1 2025	• Enhanced Workflow Editor 2.0 for improved policy management available for all customers • The Alloy Library for easier policy editing, shared global knowledge, and easier adoption of solutions from its partner network • ML and proprietary insights for investigations • Alloy for Embedded Finance–collaboration enhancements • Fraud Attack Radar for proactive detection of coordinated fraud attempts

Time frame	Description
H2 2024	• Enhanced integrations with digital banking platforms • Expanded data partnerships and SDK capabilities

Source: Alloy, Datos Insights

Datos Insights' Take

Alloy's orchestration platform provides comprehensive capabilities for managing identity, fraud, credit, and compliance risk throughout the customer life cycle. The solution's key strengths are its no-code workflow builder with built-in A/B testing and its extensive network of prebuilt integrations, which enables organizations to quickly implement and iterate on their risk-management strategies without requiring significant technical resources. This also allows their customers to be more responsive to evolving fraud risks and make changes with new data sources and tools to mitigate losses.

The platform's journey-based architecture provides flexibility in designing and implementing risk policies while maintaining consistency across channels and use cases. This approach is particularly valuable for organizations looking to standardize their risk-management practices while supporting various products or channels. The solution's testing capabilities, including backtesting and A/B testing, enable organizations to validate the effect of policy changes before deployment, reducing the risk of unintended consequences.

The general availability of Fraud Attack Radar in 2025 shows the company's commitment to proactive fraud detection. This capability, combined with Alloy's existing Entity Fraud Model, will provide organizations with both point-in-time and continuous risk assessment capabilities. The company's focus on investigation workflow optimization through enhanced case management and analytics capabilities addresses a critical operational need of most FIs. Also, the company's recent partnership with Q2 makes orchestration capabilities available more broadly.[1]

Alloy's focus on digital-first organizations has evolved to include embedded finance and sponsor banking relationships, as well as multichannel and multi-line-of-business risk management for enterprise banks, which serve complex enterprise structures. The platform supports various partnership models across multiple entities, with configurable

[1] "Q2 Holdings announces new partnership with Alloy," Markets Insider, January 22, 2025, accessed on February 4, 2025, https://markets.businessinsider.com/news/stocks/q2-holdings-announces-new-partnership-with-alloy-1034256336.

workflows and controls for each relationship type. This flexibility helps organizations maintain consistent controls and visibility when managing multiple brands or partner relationships, enabling them to scale their operations efficiently. For these and other reasons, the company has gained market share over the last few years in a relatively crowded field. Alloy is clearly a solution that should be considered by FIs looking to upgrade their risk frameworks, whether for fraud, credit, or compliance.

Conclusion

The orchestration solutions market demonstrates strong momentum as providers enhance their platforms to address evolving fraud threats and changing customer expectations. Core capabilities like real-time processing and rule management remain essential, but several key developments are shaping the market's future direction. As the market continues to evolve, organizations should evaluate providers based on their ability to address current needs while positioning them well for future requirements. Carefully consider factors such as scalability, flexibility of deployment options, breadth of prebuilt integrations, and strength of professional services support.

FIs should keep the following points in mind:

- **Explore how to use ML capabilities to optimize operational decisions beyond basic fraud detection.** Fraud strategists should evaluate platforms that enable automated strategy refinement while maintaining effective controls.
- **Consider orchestration platforms that integrate digital identity verification and authentication capabilities directly within the solution.** Organizations should look for approaches that reduce integration complexity while enabling risk-based authentication.
- **Evaluate consortium data-sharing capabilities when selecting an orchestration platform.** Fraud-prevention teams should examine how providers enable network intelligence benefits while maintaining data privacy and regulatory compliance.
- **Review cloud deployment track records when assessing orchestration providers.** FIs should examine performance metrics and scalability demonstrations in cloud environments that align with their infrastructure requirements.
- **Prioritize support for real-time payments and emerging payment types when evaluating orchestration platforms.** Potential buyers should assess how providers address fraud vectors across both traditional and new payment channels.
- **Look for vendor-agnostic approaches to third-party integration when selecting an orchestration platform.** Technologists should evaluate how platforms can incorporate existing fraud-prevention investments while supporting expansion based on evolving requirements.

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

Gabrielle Inhofe

ginhofe@datos-insights.com