WAVE REPORT

The Forrester Wave™: Anti-Money-Laundering Solutions, Q2 2025

The 15 Providers That Matter Most And How They Stack Up

Apr 8, 2025 • 22 min read

Andras Cser
Vice President, Principal Analyst

With contributors:
Merritt Maxim, Faith Born and Christine Turley

Share

In our evaluation of anti-money-laundering (AML) providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps you select the right one for your needs.

Productized Risk-Scoring Models, Case Management, And Reporting Matter

AML remains one of the most critical areas for financial institutions (FIs) in their quest to repel financial crime. FIs use AML solutions to sanction screen customers and transactions, to check for adverse media exposure and politically exposed persons (PEPs), and to monitor transactions to detect possible money laundering and terrorist financing. In 2025, AML requirements are further complicated by regulators' focus on enhanced due diligence (EDD), beneficial ownership of accounts and funds, and a focus on alternative (crypto, peer-to-peer) payments.

AML customers using this evaluation to inform a purchase decision should consider:

1. **Built-in, productized support and risk-scoring models for core transaction types.** Vendors like to say that “a payment is a payment” — as long as the AML solution captures and looks at payment attributes. But customer organizations tell Forrester that they need AML solutions that help with risk-scoring rules and machine learning (ML) models for various types of payments. As AML solutions transition to the cloud, built-in, reusable, consortium data-driven knowledge, such as money launderers’ names and organizations, is becoming the norm.
2. **Versatile and orchestrated queue and case management.** Once the AML solution identifies a potentially risky transaction and generates an alert, the path to a human investigator should be easily defined. Visual workflow designers, generative AI (genAI)-based routing, and investigation copilots are relevant here. Case management must have flexible workflow options, easy ways of looking at the history of various entities (customers, email addresses, account numbers in confirmed money laundering cases), customized investigator workspaces, and features for manual and automatic reassignment of cases.
3. **Operational and regulatory reporting.** Although AML vendors publish their reporting schema and recommend that the FIs use business intelligence tools such as Microsoft Power BI or Tableau, productized and built-in operational reporting (how effective risk-scoring rules and AI models are, how well investigators perform their jobs) is an essential AML solution requirement. AML solutions can never have enough canned reports. Leading AML providers increasingly offer copilots driven by genAI and large language models

where business users can use natural language prompts to define one-time or permanent tabular and graphical reports and dashboards.

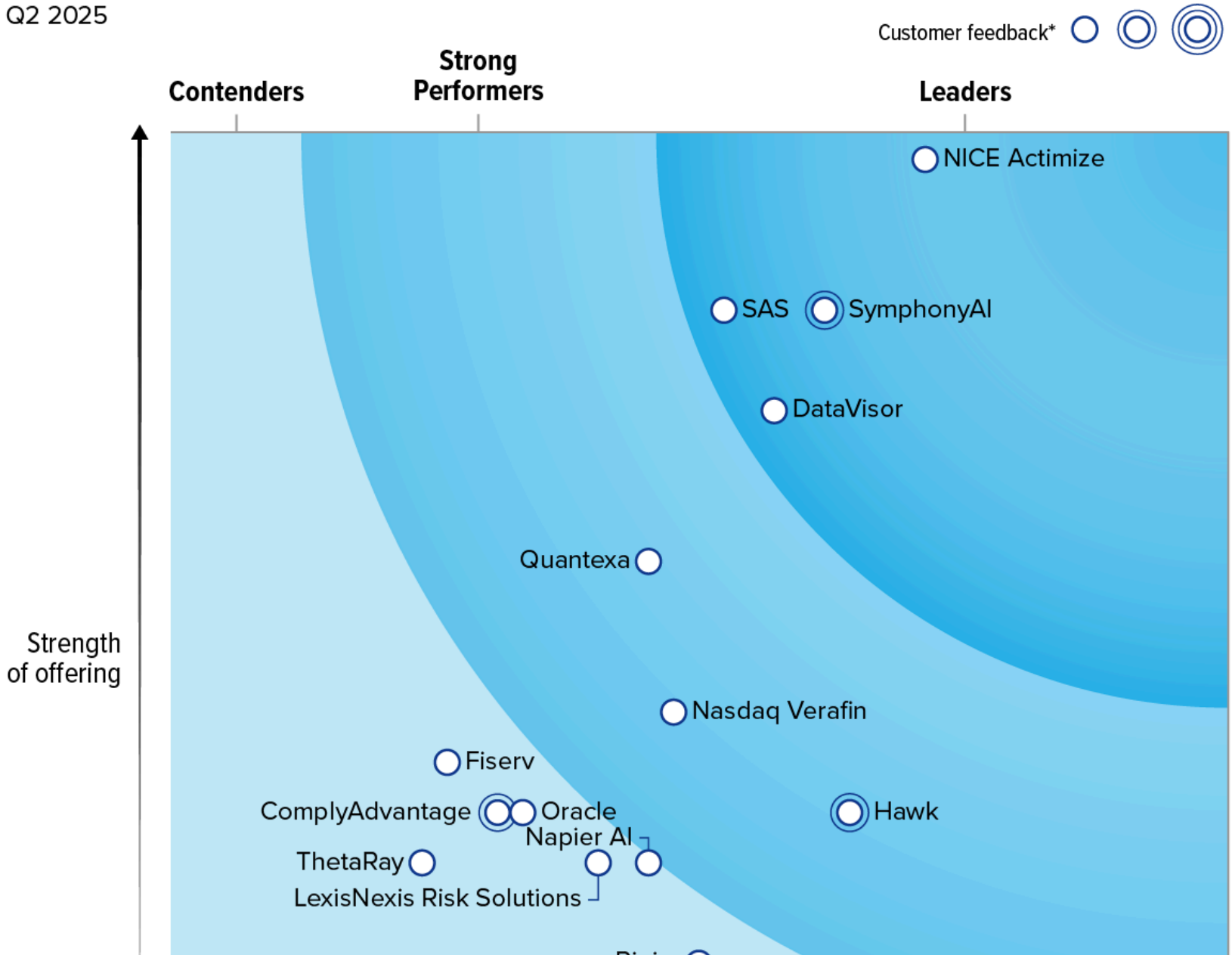
Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, and Contenders (see Figures 1 and 2). We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt the findings based on their priorities using Forrester's interactive provider comparison experience.

THE FORRESTER WAVE™

Anti-Money-Laundering Solutions

Q2 2025



*A halo indicates above-average customer feedback. A double halo indicates that the vendor is a Customer Favorite.

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 1 - Forrester Wave™: Anti-Money-Laundering Solutions, Q2 2025

	Forrester's weighting	ComplyAdvantage	DataVisor	Fiserv	Hawk	LexisNexis Risk Solutions	Napier AI	Nasdaq Verafin	NICE Actimize
Current offering		2.40	4.00	2.60	2.40	2.20	2.20	2.80	5.00
Data integration	10%	1.00	3.00	3.00	1.00	3.00	3.00	1.00	5.00
Administrator management	10%	1.00	3.00	3.00	3.00	3.00	1.00	1.00	5.00
Watchlist management and screening	10%	3.00	5.00	3.00	5.00	3.00	3.00	3.00	5.00
Rules-based risk scoring and alerting	10%	5.00	5.00	3.00	3.00	3.00	3.00	3.00	5.00
AI/ML-based risk scoring	10%	1.00	3.00	1.00	3.00	1.00	1.00	3.00	5.00
Support for transaction types	10%	5.00	5.00	1.00	5.00	1.00	1.00	5.00	5.00
Queue definitions and alert routing	10%	3.00	3.00	3.00	1.00	3.00	3.00	3.00	5.00
Case management	10%	1.00	3.00	3.00	1.00	1.00	3.00	3.00	5.00
Third-party integrations	10%	3.00	5.00	5.00	1.00	3.00	1.00	1.00	5.00
Reporting	10%	1.00	5.00	1.00	1.00	1.00	3.00	5.00	5.00
Strategy		2.20	3.30	2.00	3.60	2.60	2.80	2.90	3.90
Vision	15%	1.00	1.00	1.00	3.00	1.00	3.00	5.00	5.00
Innovation	15%	1.00	5.00	1.00	5.00	1.00	3.00	3.00	3.00

Innovation	15%	1.00	5.00	1.00	5.00	1.00	3.00	3.00	3.00
Roadmap	15%	1.00	5.00	1.00	3.00	3.00	5.00	3.00	3.00
Partner ecosystem	15%	5.00	1.00	3.00	5.00	5.00	3.00	1.00	3.00
Adoption	10%	1.00	1.00	3.00	5.00	3.00	1.00	5.00	5.00
Pricing flexibility and transparency	5%	1.00	3.00	1.00	1.00	3.00	1.00	1.00	5.00
Community	15%	5.00	5.00	3.00	1.00	1.00	3.00	3.00	5.00
Supporting services and offerings	10%	1.00	5.00	3.00	5.00	5.00	1.00	1.00	3.00

	Forrester's weighting	Oracle	Quantexa	Ripjar	SAS	Shufti	SymphonyAI	ThetaRay
Current offering		2.40	3.40	1.80	4.40	1.60	4.40	2.20
Data integration	10%	1.00	5.00	1.00	5.00	3.00	5.00	1.00
Administrator management	10%	1.00	5.00	1.00	5.00	1.00	5.00	1.00
Watchlist management and screening	10%	5.00	3.00	1.00	3.00	3.00	3.00	1.00
Rules-based risk scoring and alerting	10%	3.00	1.00	1.00	5.00	1.00	3.00	1.00
AI/ML-based risk scoring	10%	1.00	3.00	3.00	5.00	1.00	5.00	5.00
Support for transaction types	10%	1.00	3.00	1.00	3.00	1.00	3.00	3.00
Queue definitions and alert routing	10%	3.00	3.00	3.00	3.00	1.00	5.00	1.00

Case management	10%	5.00	5.00	5.00	5.00	1.00	5.00	1.00
Third-party integrations	10%	1.00	1.00	1.00	5.00	3.00	5.00	3.00
Reporting	10%	3.00	5.00	1.00	5.00	1.00	5.00	5.00
Strategy		2.30	2.80	3.00	3.10	3.00	3.50	1.90
Vision	15%	3.00	5.00	3.00	3.00	5.00	5.00	3.00
Innovation	15%	1.00	1.00	5.00	3.00	1.00	5.00	1.00
Roadmap	15%	1.00	3.00	1.00	3.00	1.00	3.00	3.00
Partner ecosystem	15%	3.00	3.00	5.00	1.00	3.00	3.00	1.00
Adoption	10%	1.00	3.00	5.00	1.00	3.00	3.00	1.00
Pricing flexibility and transparency	5%	3.00	5.00	3.00	5.00	3.00	3.00	3.00
Community	15%	5.00	1.00	1.00	5.00	5.00	1.00	1.00
Supporting services and offerings	10%	1.00	3.00	1.00	5.00	3.00	5.00	3.00

Scores are on a scale of 1 (below par relative to others evaluated) to 5 (superior relative to others evaluated).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2 - Forrester Wave™: Anti-Money-Laundering Solutions Scorecard, Q2 2025

Leaders

NICE Actimize

NICE Actimize's solution is a purpose-built AML and fraud management platform with built-in and easy-integration, customer-provided models.

1. **Strategy.** NICE Actimize excels in migrating its offerings to the cloud. Its use of genAI across all areas for AML and its collaboration with global regulators, as well as establishing extensive partnerships with regulators, elevate the vendor's vision above others. Strong adoption-boosting strategies include ongoing free health checks and model/library updates. Partner ecosystem support is on par.
2. **Capabilities.** NICE Actimize's data integration capabilities and schema setup and mapping both use genAI and are intuitive. Its rules-based transaction risk scoring is powerful and ahead of the competition. Data scientists can choose from a catalog of built-in, productized AI and ML risk-scoring models for transaction monitoring. However, the solution has its admin and data scientist users interact with multiple policy administration interfaces, including the unified data management Windows application GUI Windows, ActOne, Senzing, XSight AML Monitor, and others — each detracting from usability and administrative efficiency. This may be problematic for medium- and small-sized FIs.
3. **Customer feedback.** Reference customers mentioned that having access to the highest levels of management at NICE helps them keep projects on track. The vendor's proven track record in implementing AML projects is a plus. While the vendor offers early-adopter

support, some customers received defective updates without adequate vendor quality assurance testing, but the vendor fixed these defects quickly.

4. **Forrester's take.** The solution is a great fit for enterprises looking for a combined AML and fraud management (FRAML) solution on-premises or in the cloud.

   View NICE Actimize's detailed scorecard.

SymphonyAI

SymphonyAI is in the process of revamping the NetReveal portfolio it acquired from BAE Systems and Sensa. The vendor supports an incubation framework where select, early-adopter customers can preview new AML solution capabilities, including vertical- and domain-specific features.

1. **Strategy.** SymphonyAI's innovation strategy is ahead of the crowd; the vertical AI focus for delivering industry-specific solutions, the prototype previews by customers, agile releases, and customer advisory board organization cadence are strong. A healthy ecosystem of supporting products and services includes broad and deep consulting as well as professional services support for migrating AML capabilities to the cloud. However, community build-out and maintenance strategies lack differentiation.
2. **Capabilities.** Permissions and role management for admins shine. AI- and ML-based risk scoring of transactions is above par, and the vendor offers a rich selection of productized

ML algorithms. Risk-score explanations for investigators in case management are integrated. However, rules-based risk scoring lacks rule versioning, and entity risk-scores management in watchlist management is less powerful than the other Leaders in these areas. Watchlist management lags other Leaders with managing entity risk scores.

3. **Customer feedback.** Customers mention that the vendor is dependable and transacts in an ethical way. However, project scoping could improve — the unforeseen costs that arise during implementation are too unpredictable and high.
4. **Forrester's take.** The solution is a good fit for organizations that require broad, out-of-the-box support for ACH and wire transactions and are willing to experiment with genAI for watchlist-screening, name-matching, and summarizing investigations.

   View SymphonyAI's detailed scorecard.

SAS

SAS expanded its synthetic data generation capabilities by acquiring Hazy in November 2024. Forrester expects that this acquisition will accelerate the adoption of large data models and other genAI techniques in SAS' Financial Crime Compliance portfolio.

1. **Strategy.** The vendor offers a strong framework for quantifying the ROI of its AML solution for its potential and existing customers. SAS's vision includes transaction monitoring that includes segmentation logic, anomaly detection, and ML-based detection as well as genAI

inclusion into productized copilots. Roadmaps promise model-driven customer risk rating, increased depth of cash activity risk scoring, and better scenario tuning and optimization processes. Community-building strategies are ahead and include blogs and focused user communities. Its AML risk-scoring strategy and developer help is on par, with GitHub source code being made available. However, partner ecosystem management and adoption-boosting strategies are behind.

2. **Capabilities.** The vendor's managed cloud services have been rapidly gaining adoption. Rules-based risk scoring and alerting is comprehensive: Customers can define thresholds, what-if scenarios, and segmentation strategies. The vendor's name resolution module offers a built-in cultural affinity AI model. Its reporting is powerful and provides more types of built-in reports than do many other vendors. Built-in, productized support for common payment transaction types (peer-to-peer, automated clearing house [ACH], wire, etc.) is on par. Productized watchlist source integration and configuration requires more effort and is more complex than that of other vendors.
3. **Customer feedback.** Customers mention that SAS dedicates extra effort and energy to maintaining meaningful bidirectional communication with them and keeping the conversation technical and not sales heavy. However, customers mentioned that the deployment requires existing internal resources with SAS programming skills, and full build-out is more expensive (both from the licensing and from the labor cost perspective) than with other vendors' solutions.

4. **Forrester's take.** The solution is a great fit for enterprises with existing SAS and data science skills that require cutting-edge, AI/ML risk-scoring strategies for highly efficient AML processes.

   View SAS's detailed scorecard.

DataVisor

DataVisor has been broadening its third-party tool integration ecosystem to include core banking platforms, fraud management tools, CRM solutions, and others.

1. **Strategy.** The vendor's innovation strategy and roadmap are ahead of the competition. They feature AI-assisted alert and case review and report generation, and they use AI and customizable knowledge entity risk graphs to highlight risk indicators. The vendor plans to continue cocreating with its customers and partners. However, partner and adoption-boosting strategies lag others. DataVisor's vision falls short relative to peers in migration support and the use of AI agents.
2. **Capabilities.** The vendor closely follows regulatory changes with improved regulatory reporting features. Watchlist management was better than others, along with third-party integrations and reporting. The offering is extremely strong in entity risk-score definitions, updates, and management, including on-demand periodic customer watchlist risk rescoring. However, while the vendor offers a selection of supervised ML algorithms, it lags in the administration of unsupervised ML algorithms. SAML- and OIDC-based admin

authentication integration requires assistance from DataVisor implementation or professional services teams. The solution currently offers no copilots in case investigation.

3. **Customer feedback.** Customers like the heuristic rule definition flexibility that the solution provides as well as the ability to define granular report access policies. However, they find the solution's learning curve to be steeper than that of other competitive solutions. Only one of DataVisor's reference customers responded to Forrester's outreach for this evaluation.
4. **Forrester's take.** The solution is a great fit for organizations that require end-to-end AML tools offering fraud management capabilities, such as account takeover, and do not mind dealing with a less user-friendly power tool.

   View DataVisor's detailed scorecard.

Strong Performers

Quantexa

Quantexa has been pioneering entity risk scoring and automatic discovery and corroboration of data in AML. As a result, it achieved $100 million in annual recurring revenue in 2024 after acquiring Aylien in its first quarter of 2023. The company's valuation reached $2.6 billion, and the vendor expects to invest an additional sum of $155 million in AI by 2027.

1. **Strategy.** Quantexa's AML product vision is ahead of other vendors' vision and focuses on risk-scoring scale while keeping its solution open and extensible. Flexible deployment form factors, such as hybrid cloud and on-premises deployments, are also central to its vision. Roadmaps are on par and include additional AML case management workflow templates, discovering entity relationships from unstructured data, as well as expanding financial crime typologies. However, community build-out strategies miss opportunities.
2. **Capabilities.** Quantexa's solution offers a genAI-based "assist" copilot that helps investigators with contextual, natural language guidance. Data integration provides strong schema setup and mapping; it also allows client administrators to use AI to improve the quality of input data into the solution. Admin user permission management is robust, with explicit capabilities to define permissions and scope of predefined and custom admin roles. Case management is also highly functional: It provides a copilot for investigation and regulatory report filing. However, rules-based risk scoring lags in terms of ease of use (many features lack GUI administration), what-if scenarios, and rule versioning. Third-party integrations and API access to AML policies are also behind.
3. **Customer feedback.** Customers said that the vendor's product quality has been improving, and they enjoy cocreating and collaborating with the vendor. However, customers find that the vendor's heavy focus on complex entity risk identification means that rule tuning and other basic capabilities can suffer.
4. **Forrester's take.** The solution is a nice fit for financial organizations that require out-of-the-box entity risk discovery and management in payment transaction monitoring.

View Quantexa’s detailed scorecard.

Hawk

Hawk received its series B funding, allowing it to grow its banking client customer base. The vendor has announced a new product every year for the last five years and the majority of its customers expand their platform use.

1. **Strategy.** Hawk’s innovation is ahead of the competition: The vendor uses regional expert groups that meet three times annually and capture customer feedback via surveys, end-user testing, and support. The vendor invests a disproportionately high 40% of its revenue into R&D. Partner ecosystem and adoption-boosting strategies are also strong: Hawk offers self-configuration with no-code UI and uses metrics to optimize performance and expand modules. However, its community-building strategies lag others, as do its pricing and ROI calculations transparency.
2. **Capabilities.** Watchlist management is highly configurable, as evidenced by rich functionality for what-if scenarios, champion-challenger list management, configurable entity risk scores, and perpetual know-your-customer (KYC) processes. Productized support for common transaction types like SWIFT or crypto and the built-in tenant management are also nice. However, the solution lags in data integration, queue definitions, and alert routing. Role-based access controls for AML admins are inconsistent.

Case management and reporting also lack functionality like queue management and automatic alert assignments to investigators.

3. **Customer feedback.** Customers mentioned that the sales process is adequate and using the solution is intuitive. Customers unanimously said the vendor fulfills its promises, is competent, delivers consistent quality, and acts ethically. However, they also mentioned that the vendor's professional services bench depth is inadequate and the bulk editing of cases is challenging.
4. **Forrester's take.** The solution is a good fit for small financial services firms that require customer screening, transaction screening, and transaction monitoring from a single, end-to-end solution and do not mind developing some extra operational reports themselves.

View Hawk's detailed scorecard.

Nasdaq Verafin

Verafin was one of the first AML vendors to offer a purely cloud-based solution — benefitting from consortium data and highly repeatable decision-making logic. Beyond core AML, the company has a long history of detecting human trafficking from payment and non-payment transactions.

1. **Strategy.** Verafin's AML vision is one of the strongest across the vendors in this evaluation. Its strength is its shared consortium information as well as targeted typology analysis

developed in collaboration with customers and regulators. Strong adoption-boosting strategies include a module-by-module, gradual rollout as well as extensive customer success operations. While ongoing optimization, support, upgrades, and other services are built into the subscription price, it can be markedly higher than that of competitors. However, partner ecosystem management strategies and supporting services and offerings lag.

2. **Capabilities.** Verafin uses Naïve Bayesian networks (called agents) in decisioning that can build on each other. The number of built-in, productized models that support key transaction types (P2P, ACH, wire, crypto) is higher than with other competitors. Reporting offers the useful customization of built-in reports and dashboards. However, data integration capabilities, admin user management, and third-party system productized integrations are behind.
3. **Customer feedback.** Customers mention that the ability to identify high-risk accounts and develop targeted monitoring activities is powerful, and the vendor's interactions with its customers are respectful. However, Verafin's routing of technical support and product defect tickets to the right engineer or developer can result in longer-than-expected resolution times.
4. **Forrester's take.** The solution is a great fit for organizations that require a cloud-based AML solution and do not mind paying a higher price for bundled solution support and maintenance.

View Nasdaq Verafin's detailed scorecard.

Contenders

Napier AI

Fueled by its focus on regulatory compliance using explainable, auditable, and ethical AI, Napier AI achieved a large mindset growth with financial services clients. Napier AI's AML solution is modular, with microservices that allow for API-first, orchestrated implementations.

1. **Strategy.** Napier AI's roadmaps are ahead of the competition and feature entity resolution and network analytics that build on structured and unstructured data. Enhancing ML with dynamic learning and testing that results in better decision automation is also part of future development plans. However, its adoption-boosting strategies are below par and pricing lags in transparency. Supporting services and offerings lack the depth and breadth offered by other vendors, such as extended own and third-party product ecosystems.
2. **Capabilities.** Queue definitions and alert routing are on par and offer customizable routing policies (workflows for workgroups) and the bulk management of alerts. GenAI provides a

copilot with recommendations and guidance for investigators. Data integration is on par, and reporting features customizable dashboards; however, the solution lacks genAI-driven reports and detailed insight into the efficiency of AI risk-scoring algorithms. Administrative users' permissions management and productized support for various transaction types are below par.

3. **Customer feedback.** Customers like the bang for the buck — its high performance-to-price ratio — that the solution offers; however, they expressed concerns about the product's transaction risk-scoring response times under load.
4. **Forrester's take.** The solution is a nice fit for organizations that require end-to-end solutions with hands-off and managed AI-based risk scoring and that don't mind working with a smaller vendor.

   View Napier AI's detailed scorecard.

LexisNexis Risk Solutions

LexisNexis Risk Solutions has been expanding its KYC, watchlist management, AML, and identity verification portfolios aggressively in the past five years. The vendor focuses on alert reduction, screening, and AML orchestration and workflow implementation.

1. **Strategy.** LexisNexis Risk Solutions has one of the largest AML support services and complementary offerings ecosystems. The vendor offers adjacent solutions in identity

verification (including public records, email, and document verification) and customer due diligence. Its partner ecosystem and nurturing strategies are also ahead. However, its AML vision, innovation, and community-building strategies as well as its current use and plans for use of genAI are weak compared with that of other vendors.

2. **Capabilities.** Its rule-writing capabilities shine. The solution provides admin rights management, watchlist management (the built-in integration choices for commercial watchlists are broad), and rules-based risk-scoring capabilities. Productized integrations with its own ThreatMetrix and identity verification (IDV) solutions are strong and easy to configure. However, some of the data integration configuration is not exposed to end-user client administrators, and case management and reporting also lag.
3. **Customer feedback.** Customers conclude that LexisNexis Risk Solutions is competent and ultimately dependable. However, the vendor's bench depth is limited, which curtails its ability to implement on time and deliver timely fixes to product defects. Proactive, timely, and transparent communication can also be an issue.
4. **Forrester's take.** The solution is a good fit for organizations that require consolidation for their IDV, watchlist management, customer screening, and transaction-monitoring stacks and have internal resources to consolidate policy management and, in some cases, build centralized operational reporting.

View LexisNexis Risk Solutions' detailed scorecard.

Ripjar

Ripjar received additional series B investment from Long Ridge Equity Partners, and the Dow Jones also expanded their investment. Ripjar also expanded sales, marketing, and demand generation coverage in Europe and North America.

1. **Strategy.** Its innovation strategies excel, as evidenced by the vendor's unwavering disruption of its own products to continually evolve them, and the vendor builds in-house expertise to support this. However, Ripjar does rely on deep cocreation with customers as other vendors do. It's weaker than other vendors at defining and following up on roadmaps, and its supporting services and offerings are as well.
2. **Capabilities.** Ripjar's adverse media screening features are powerful. Case management is very versatile, with useful genAI-based copilots to guide the investigation process. Investigators can easily prioritize their workload and customize the look and feel of their case screens. In its on-par AI- and ML-based risk scoring, Ripjar's predictive and behavioral analytics show promise, as the solution applies AI on top of structured and unstructured data. However, the solution falls short in data integration, administrative user permissions and roles management, rules-based risk scoring, and productized support for transaction types. Its third-party integration and out-of-the-box reporting also lag.
3. **Customer feedback.** Customers feel that Ripjar increasingly fulfills its promises and generally cares about its customers. However, they don't fully understand the direction of

the vendor's long-term AML product development. Only one of Ripjar's reference customers responded to Forrester's outreach for this evaluation.

4. **Forrester's take.** The solution is a good fit for organizations that require their AML vendor to 1) enjoy the regulator's trust and 2) provide a one-stop AML offering to its clients.

   View Ripjar's detailed scorecard.

Oracle

Oracle AML and Financial Crime Compliance Management consists of sanctions screening, case management, and AML transaction monitoring. The solution offers a unified data model as well as investigation and regulatory and operational reporting.

1. **Strategy.** Community-boosting strategies are ahead, as evidenced by Oracle's strong online user community and discussion boards. Its product vision and partner ecosystems are on par with those of other vendors. Oracle has been pushing the migration of its financial crime-fighting portfolio from on-premises deployments to software-as-a-service (SaaS) delivery. However, its innovation, concrete AML product roadmaps, communication to clients, and adoption-boosting strategies lag others.
2. **Capabilities.** Oracle's watchlist management capabilities are strong. Case management — user screen customization, alert visualization, workload management — is ahead of the competition. GenAI-based chatbots provide investigators with enhanced alert and case

narratives. Oracle is focused on behavioral models (to augment heuristic rules) and claims to reduce false-positive rates. However, data integration, admin management, and productized support for typical payment transaction types are weak.

3. **Customer feedback.** Customers appreciate the long-standing, 20-year presence of the vendor in the AML space. However, Oracle's long-term commitment to AML and relatively low levels of visible AI/ML innovation are concerning. Oracle did not provide reference customers for this evaluation.
4. **Forrester's take.** The solution is a good fit for multinational financial services firms that use a broader set of Oracle solutions, including the vendor's FLEXCUBE core banking solution, and that require global product implementation and ongoing support.

View Oracle's detailed scorecard.

ComplyAdvantage

In cryptocurrency monitoring, ComplyAdvantage offers fiat-to-crypto and crypto-to-fiat currency transactions monitoring, while it partners with Elliptic for crypto-to-crypto transaction monitoring.

1. **Strategy.** Look for partner ecosystem build-out and management strategies: Dedicated partner contact managers, cocreation with partners, and quick partner onboarding are the key strong points here. Community-building methods are powerful and include better-

than-average peer exchanges, customer events, webinars, and white papers. However, the vendor's vision, innovation strategies, roadmaps, adoption, and supporting services and offerings are below par and lack an entity risk focus, typologies improvements, and model governance.

2. **Capabilities.** ComplyAdvantage provides valuable insights to its customers on customer outcomes, including abandonment rates. Rules-based risk scoring and alerting are strong and sport threshold management, what-if scenarios, and version control. Productized support for payment transaction types includes solid support for textual SWIFT message risk scoring and screening and cryptocurrency. However, the solution lags in data integration, admin user permission management, AI/ML-based risk scoring, case management, and reporting.
3. **Customer feedback.** Customers mention that ComplyAdvantage communicates openly and clearly, goes to great lengths to build real client relationships, and puts out exceptionally good documentation. However, it sometimes needs guidance from its customers on exact regulatory requirements.
4. **Forrester's take.** The solution is a good fit for tier three or four FIs that want one solution to cover their customer screening, payment screening, and transaction-monitoring needs.

View ComplyAdvantage's detailed scorecard.

Fiserv

Fiserv has been selling its AML solution as part of its large “department store for banking” concept. Forrester expects that there has been slow growth of the vendor’s large install base and that the vendor will update its FCRM AML solution with new capabilities and user interfaces.

1. **Strategy.** Fiserv’s vision, innovation, and roadmap lag those of other vendors; they lack genAI, perpetual KYC improvement, and the use of semantic data for risk scoring. Broad integration with partner solutions, extensive professional services support, and roadmaps that focus on user-friendly interfaces help with customer adoption. But plans to support non-fiat currency-based payments (peer-to-peer, cryptocurrencies) are also weak, and proactive investigations supported by entity risk scoring are missing. Pricing is less transparent than that of other vendors. ROI justification has been complex and hard for customer organizations.
2. **Capabilities.** The solution’s marketplace of third-party integrations (watchlists, consortium data) is ahead of the competition. Being a large “department store” provider for financial services institutions explains deployments of a larger scale than other vendors in this evaluation. Data integration, rule management, and queue and case management are on par. However, AI- and ML-based risk scoring, productized risk-scoring support for payment transactions, and reporting are weak. Customization is not intuitive and usually requires engagement from the vendor’s implementation services.
3. **Customer feedback.** Customers generally like the one-stop-shopping experience the vendor offers but have reported challenges with 1) extensive implementation timelines, 2)

risk-scoring response times, and 3) data integration with core banking solutions. Fiserv did not provide reference customers for this evaluation.

4. **Forrester's take.** The solution is a good fit for firms with a deep existing relationship with Fiserv and where traditional, batch, and rule-based risk scoring is adequate.

   View Fiserv's detailed scorecard.

Shufti

Shufti uses its proprietary data, integrates with hundreds of watchlists, and has one of the largest PEP databases. The vendor's pedigree is in physical identity document verification, which it uses in electronic KYC processes.

1. **Strategy.** Shufti's product vision surpasses its competitors' and includes aligning with global AML regulations, reducing compliance risks, and streamlining workflows. Strong community-building strategies include a healthy mix of user group meetings, publications, and regulatory body engagement. Partner ecosystem and adoption-boosting strategies are on par, and per-transaction pricing, while unpublished, is internally standard. However, innovation and roadmaps fall behind the competition.
2. **Capabilities.** Shufti's third-party integrations are on par and offer robust watchlist and PEP list choices. The vendor's integration with its own physical identity document verification (PIDV) solution is promising, while integration with third-party case management solutions

only focuses on Salesforce. However, administrative user permissions management and role-based access control are weak, with a minimal administrative role structure. Multitenancy management is not exposed to end-user organizations. Rules-based risk scoring, AI/ML risk scoring (especially the customization options available for end-user admins), queue and case management, and reporting are below par.

3. **Customer feedback.** Customers are generally satisfied with Shufti's dependability and its attentiveness: Sales reps are responsive, professional, and courteous. However, customers expressed concerns about integration times being too long as well as the high labor costs of manual investigations because of inaccurate solution decisions. Shufti's reference customers did not respond to Forrester's outreach for this evaluation.
4. **Forrester's take.** The solution is a good fit for organizations that require an integrated PIDV, customer sanctions, and a PEP screening solution and have other vendor solutions for transaction monitoring.

   View Shufti's detailed scorecard.

ThetaRay

ThetaRay's focus on turning compliance into a competitive business agility benefit plays an essential role in its use of genAI. Identity resolution, low-/no-code AML orchestration, and collaborative AI models for sharing threat intelligence are central to the vendor's approach to AML.

1. **Strategy.** The vendor has been a pioneer in using AI and ML for AML risk scoring, but its heurist scoring vision is weak relative to the Leaders in this market. Important AML vision points include 1) allowing customers to work with incomplete or inconsistent data, 2) integrating legacy systems, and 3) helping customers deal with regulatory uncertainty and changes. Pricing transparency and flexibility are on par, largely because the solution is available on the Azure marketplace. However, the vendor's innovation strategy, partner management and retention, customer adoption, and community-building strategies are below par.
2. **Capabilities.** The solution excels in AI- and ML-based risk scoring with powerful use of proprietary algorithms and continuous learning. Reporting and dashboarding offer ahead-of-the-pack data visualization tools. The accuracy of decisioning is strong. However, data integration, admin user permissions management, watchlist management, rules-based risk scoring, and queue and case management lag the competition.
3. **Customer feedback.** Customers generally like the vendor's willingness to jointly work on product improvements in adapting to new money-laundering methods but mention that implementation can be challenging, and that ease of use and intuitiveness of the admin graphical user interface should improve. ThetaRay did not provide reference customers for this evaluation.
4. **Forrester's take.** The solution is a good fit for organizations looking for accurate risk scoring in transaction monitoring, even if it means paying a higher-than-average price.

View ThetaRay's detailed scorecard.

Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

Vendor	Product evaluated
ComplyAdvantage	ComplyAdvantage Mesh, Financial Crime Risk Intelligence
DataVisor	DataVisor AML Platform V2.1
Fiserv	Financial Crime Risk Management
Hawk	Hawk AML Solution Suite
LexisNexis Risk Solutions	LexisNexis Risk Solutions
Napier AI	Napier AI Continuum
Nasdaq Verafin	AML Compliance & Management
NICE Actimize	NICE Actimize Anti-Money Laundering Solutions Suite
Oracle	Oracle Financial Crime and Compliance Solutions
Quantexa	Quantexa Contextual Monitoring for AML
Ripjar	Labyrinth Screening (UBS/JB - v 24.1, Dow Jones - Bespin v31)
SAS	SAS Anti-Money Laundering
Shufti	User Identification and Authentication and Business Identification and Risk
SymphonyAI	NetReveal Transaction Monitoring, NetReveal CDD, NetReveal Name Screening, NetReveal Transaction Screening, Sensa Investigation Hub, Entity Resolution, SensaAI for AML, SensaAI for Sanctions
ThetaRay	Transaction Monitoring, Customer Risk Assessment, Watchlist Screening

	(Transaction & Customer Screening)

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.
Figure 3 - Evaluated Vendors And Product Information

Evaluation Overview

We evaluated vendors against three categories:

1. **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering.
2. **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies, including elements such as vision and innovation.
3. **Customer feedback.** A halo on a vendor's marker indicates above-average customer feedback relative to the other evaluated vendors. A double halo indicates outstanding customer feedback: We consider the vendor to be a Customer Favorite. As part of this evaluation, we speak with up to three customers of each vendor. We also consider customer input from our previous research.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

1. **Broad, enterprise-level native AML functionality.** The vendor natively provides all core AML functions for this space including watchlist management, sanctions screening, transaction monitoring, investigation, and reporting and has a demonstrated track record for supporting large enterprises.
2. **An AML solution that is available for purchase as a standalone product.** The product has its own SKU and pricing. It is not solely available as a free feature within a larger portfolio.
3. **Substantial AML revenue.** The vendor had at least $10 million in AML product revenue from the AML solution in the last four fiscal quarters.
4. **Mindshare among Forrester's enterprise clients.** Forrester clients frequently mention the product as one they are considering or shortlisting prior to a purchase. We have heard about the product from our clients in the form of inquiries, advisories, consulting engagements, and other interactions over the past 12 months. Other vendors frequently mention this vendor as a competitor in the market.

Other Notable Vendors

The Forrester Wave evaluation is an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market and additional vendors that Forrester considers to be notable for enterprise clients in our corresponding report: The Anti-Money-Laundering Solutions Landscape, Q4 2024.

Supplemental Material

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos and briefings, and interviews with customers (vendors may provide up to three reference customers; we also consider feedback from other customers we've spoken with). We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by January 17, 2025, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with our vendor review policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. We score vendors that met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation in accordance with our vendor participation policy and publish their positioning along with those of the participating vendors.

Fiserv, Oracle, and ThetaRay declined to participate in the full Forrester Wave evaluation process. For vendors that are not full participants, Forrester uses primary and secondary research in its analysis. For example, we might use public information, data gathered via briefings, and independently sourced customer interviews to score the vendor. We may ask the vendor for an abbreviated briefing and/or to provide reference customers. We may also rely on estimates to score vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the integrity policy posted on our website.

About Forrester Reprints https://go.forrester.com/research/reprints/

© 2025. Forrester Research, Inc. and/or its subsidiaries. All rights reserved.