KuppingerCole Report

LEADERSHIP COMPASS

By John Tolbert

June 15, 2021

Fraud Reduction Intelligence Platforms

This report provides an overview of the market for Fraud Reduction Intelligence Platforms and provides you with a compass to help you to find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing Fraud Reduction Intelligence Platform solutions.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

Fraud is a major cost to businesses worldwide. Multiple reporting sources estimate that total related cybercrime costs will reach $10.5 trillion by 2025. Fraud has been exacerbated by the Covid pandemic. Banking, finance, payment services, and retail are some of the most frequent objectives of fraudsters, as expected. However, insurance, gaming, telecommunications, health care, cryptocurrency exchanges, government assistance agencies, travel and hospitality, and real estate are increasingly targeted as cybercriminals have realized that most online services trade in monetary equivalents. Moreover, after years in the sights of cybercriminals, banking and finance in general are better secured than other industries, so fraudsters attack any potentially lucrative target of opportunity. Fraud perpetrators also continually diversifying and innovating their Tactics, Techniques, and Procedures (TTPs).

The most prevalent types of fraud businesses and government agencies experience today are:

Account Takeover Fraud (ATO) - occurs when fraudsters use breached passwords and credential stuffing attacks to execute unauthorized transactions. Additional means for account takeover fraud are malware attacks (man in the middle and man in the browser) as well as the use of Remote Access Tools via Trojan or social engineering scams.

New Account Fraud (NAF) – also called Account Opening (AO) Fraud, often happens as a result of using stolen identities or assemblages of personal information to create a synthetic digital ID, and can be more difficult to detect but has advantages for attackers. This type involves gathering complete sets of or bits of PII (Personally Identifiable Information) on legitimate persons to construct illegitimate accounts. Educational, financial, and medical records can be sources of PII used for assembling fake accounts, which are then often used to abuse promotions and instant loans and/or used as mule accounts to move money around.

Other common fraud types that are encountered include:

SIM Swap Fraud – a SIM swap is a special type of ATO involving a change within Mobile Network Operator's (MNO's) device mapping database that points a phone number to a specific SIM card installed in customer phones. SIM Swap Fraud occurs when malicious actors convince MNO employees to associate victims' mobile phone numbers with the fraudsters' devices. Fraudsters may try to get information directly from victims or may buy victim info on the dark web in order to set the stage for these kinds of attacks. In this sense, it is a special kind of ATO fraud that relies upon social engineering and/or insider fraud.

Insider Fraud - includes not only financial theft by employees, contractors, or partners, but also the theft of intellectual property (IP), which may include customer information from CRM systems

Screen Scraping – programmatically scraping information entered into web forms by consumers and sending to other web services. This technique is (unfortunately, because it is insecure) sometimes used for legitimate purposes.

Inventory Skimming or Depletion – perpetrated largely by bots that buy up a retailer's inventory to re-sell.

Fraudulent Insurance Claim Submission – insurance agents' and brokers' credentials are captured and used to authorize fraudulent insurance claims.

Real Estate Escrow Mis-Direct – real estate agents' credentials are captured and used to send emails to customers to have them transfer large sums (down payments) to fraudsters' accounts. These transfers are usually unrecoverable and can be devastating to home buyers.

Banking Overlays – malicious apps that look like login screens for mobile banking apps, designed to harvest credentials and hijack transactions.

Travel Site Overlays - malicious apps that look like login screens for mobile travel apps, designed to harvest credentials and hijack transactions.

The chief mitigation strategies against these types of fraud employ real-time risk analytics and decisioning. Risk-based Multi-Factor Authentication (MFA) can eliminate a substantial portion of ATOs by increasing authentication assurance levels. Risk-based MFA often evaluates credential intelligence, device intelligence, user behavioral analytics, and behavioral/passive biometrics. To decrease NAF/AO/Synthetic Fraud, increasing identity assurance at registration and authentication time with identity vetting services is recommended. Bot detection and management can also be helpful at cutting other types of fraud.

Risk-based MFA and transaction processing solutions operate optimally when integrated with or informed by Fraud Reduction Intelligence Platforms (FRIPs). FRIPs provide to risk-based MFA and transaction processing systems the information needed to make more accurate decisions on whether or not transactions should execute. FRIP solutions generally provide up to six major functions:

- Identity proofing/vetting
- Credential intelligence
- Device intelligence
- User behavioral analysis
- Behavioral/passive biometrics
- Bot detection & management

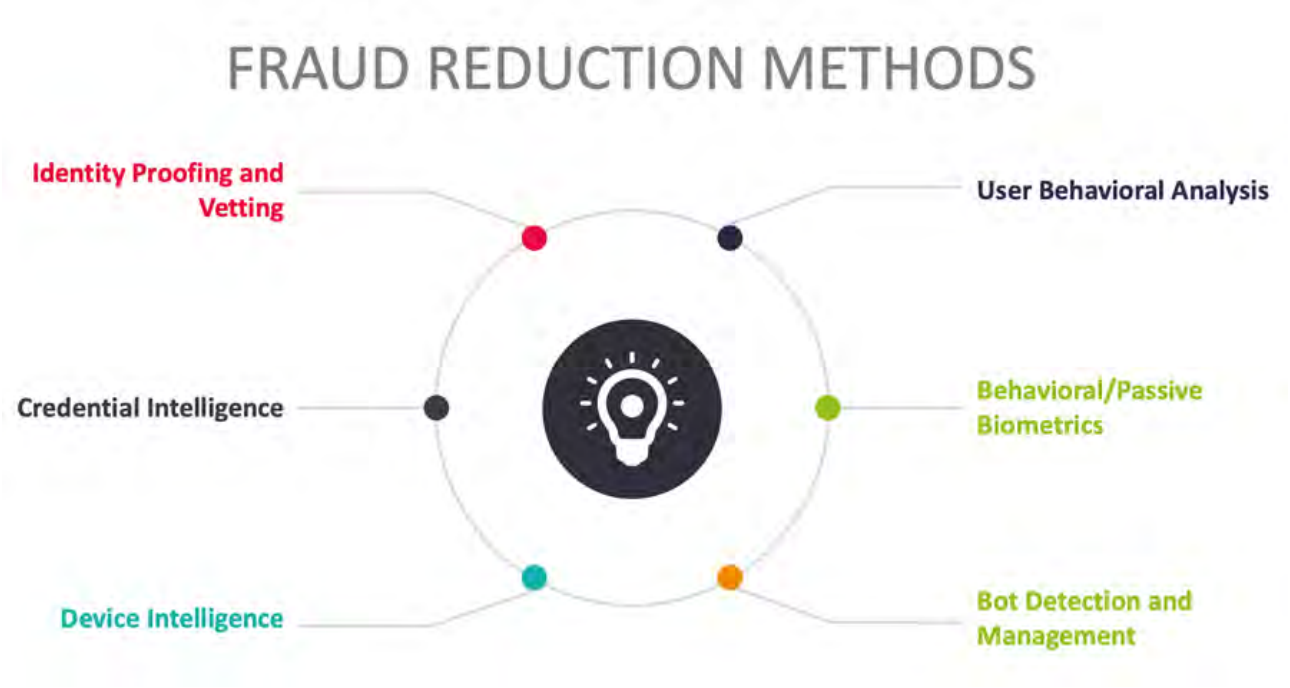


Figure 1: KuppingerCole

This report covers solutions that aggregate multiple fraud intelligence sources and provide advanced analytics services for customer organizations to augment their applications with the goal of reducing costly fraud.

1.1 Highlights

- Fraud Reduction Intelligence Platforms are increasingly sought after by consumer facing businesses in all industries. Account takeovers and new account fraud has been rising for years but has been exacerbated by the Covid pandemic.
- More FRIP solutions incorporate identity proofing directly and/or allow customers to extend identity vetting by enabling connections to 3rd-party authoritative attribute providers. The most innovative platforms offer remote identity verification apps and/or SDKs.
- Compromised credential intelligence is not ubiquitously used. Most vendors use credential intelligence from among their customer bases but sharing and consumption of external sources is not common.
- User behavioral analysis capabilities are expanding and getting more detailed in terms of transaction level attributes.

- Device intelligence, as a key indicator of fraud, is more widely collected and used effectively by FRIP service providers.
- Behavioral biometrics are catching on as more FRIP vendors provide built-in capabilities or partner with specialists to add this to their portfolios. Behavioral biometrics are a leading driver of innovation in the FRIP market.
- Bot detection capabilities are essential, and this is reflected by the fact that most vendors in this space now have at least basic bot detection functions. Advanced bot management is not commonplace yet within FRIP solutions.
- The product leaders are ID Dataweb, Transmit Security, Experian, BioCatch, OneSpan, IBM, Broadcom, and Arkose Labs.
- The innovation leaders are ID Dataweb, BioCatch, IBM, Transmit Security, Experian, OneSpan, and Arkose Labs.
- The market leaders are Broadcom, Experian, Neustar, Outseer (RSA), IBM, OneSpan, and Transmit Security.

1.2 Market Segment

The Fraud Reduction Intelligence Platform market is mature and growing, with some vendors offering full-featured solutions providing comprehensive functionality addressing each of the major methods listed above to support millions of users and billions of transactions across every industrial sector. As will be reflected in this report, the solutions in this space are quite diverse. Some vendors have about every feature one could want in a FRIP service, while others are more specialized, and thus have different kinds of technical capabilities. For example, some vendors are highly adept at device intelligence, including detailed histories of devices and information provided by working relationships with MNOs, but may not offer bot detection & management. Others excel at user behavioral analysis and passive biometrics, but don't do identity proofing. In general, identity proofing and vetting is quite specialized and is not built-in to all FRIP services. Many FRIP vendors allow customers to outfit their instances with identity vetting capabilities by enabling API callouts to 3rd-party ID vetting services, and then processing the results at transaction time.

Furthermore, KuppingerCole research indicates that the particular market segments that vendors choose to target often have a direct effect on the type of features available in their FRIP solutions. Some vendors specialize strictly in preventing fraud in financial transactions. Others are more general purpose, offering their services for insurance, health care, gaming, etc.

1.3 Delivery models

In the Fraud Reduction Intelligence Platform market, solutions are generally offered as SaaS. It's a consumable service, not usually something that customers would need or want to run in-house. For these SaaS offerings, the licensing model is often priced per volume of transactions. Some may offer discounts or refunds for low-scored results (i.e., missed fraud detections) that lead to chargebacks or other fraud.

1.4 Required capabilities

We are looking for comprehensive solutions that provide at least 4 of the 6 major areas of functionality areas. These are typically the requirements that customers pose to prospective vendors in RFPs:

- **ID Proofing** – verification that the proper user subject is issued digital credentials, often validated against government-issued ID credentials. Identity proofing and vetting services tend to be localized to specific regions or countries. FRIP solutions generally call out via APIs to one or more ID Proofing services rather than building this functionality directly into their FRIP. Some vendor services have built-in ID proofing functions.
- **Credential Intelligenc**e - information about prior usage of digital credentials, to answer questions such as "has this credential known to have been recently compromised?" or "has this credential been used for fraud at other sites?"
- **User Behavioral Analysis (UBA)** – examination of past user activities to determine if the current transaction request is within normal parameters. For example, "is the requested amount and recipient typical of what this user has successfully transacted before?" or "does the request originate with similar environmental attributes as prior transaction requests?". Environmental attributes may consist of data points such as time/day, IP, cyber threat intelligence, geo-location, geo-velocity, Wi-Fi SSIDs, and others. Longer storage periods allow for larger volumes of data to be evaluated, increasing accuracy and effectiveness.
- **Device Intelligence** - includes device hygiene (OS patch versions, anti-malware client presence, and RAT detection), device history and reputation, location history, IP reputation, MNO carrier information (IMSI, IMEI, etc.). MNO identifers, such as the IMEI and IMSI, in conjunction with UBA and Behavioral Biometrics (see next), can enable FRIP services to detect SIM swap attacks. Some services may include consumption of other 3rd-party sources of information.
- **Behavioral/Passive Biometrics** – the ability to analyze metrics of users' physical interaction with devices for comparison against registered samples. For desktop/laptop computers, this may involve

downloading JavaScript from the customer site to capture information on keystroke and mouse usage; for mobile devices, this may involve building a mobile app using a special SDK that allows for collection of information on screen pressure, swipe analysis, gyroscopic orientation, etc.

- **Bot Detection** – evaluation of pertinent cyber threat intelligence on botnet activities, request context behavior, and behavioral biometrics to determine on a per-session basis whether a real user vs. bot is requesting the action.

Most vendor solutions that utilize these methods employ various Machine Learning (ML) algorithms to process the vast amounts of data required to detect and classify anomalies in order to determine accurate risk scores and help customer applications make informed decisions.

Solutions not meeting our general inclusion criteria but nevertheless strongly focusing on specific types of fraud reduction are mentioned separately in our “Vendors to watch” chapter. Consequently, we did not impose any additional restrictions on vendors, such as a minimum number of customers or revenue caps – both large international companies and small but innovative startups were invited to participate. KuppingerCole does not charge vendors to participate in Leadership Compass reports.

Evaluation Criteria Key Features

- Solutions which interoperate with authoritative attribute sources for ID proofing, generally via APIs
- Solutions which can draw from both in-network and out-of-network sources for compromised credential intelligence and effectively use that information for transaction-time analyses without impeding customer business (for example, high false positive rates)
- Solutions which can build a baseline of normal activity per user and compare it in real-time to incoming transaction requests; or those which interoperate with 3rd-party sources of user behavioral analysis
- Solutions which can harvest device intelligence from in-network and/or consume 3rd-party device intelligence sources
- olutions which enable customers to deploy behavioral/passive biometrics capabilities by use of JavaScript or vendor-provided SDKs and process collected passive biometrics data within their risk analysis engine
- Solutions which can granularly build policies to evaluate business-relevant environmental attributes
- Solutions that utilize the above-mentioned types of information and offer customer administrators flexible and automated response actions such as
    - Permit
    - Deny

    - Re-authenticate
    - Step-up / out-of-band authorization
    - Place holds on accounts
    - Set monetary limits on transaction amounts by account or account type
    - Throttle transactions per period and per user
    - Approve/prohibit IP addresses and ranges
- Solutions which generate dashboards and reports for customers including the following standard types:
    - Total number of dismissed, detections, case open and close events, etc.
    - Regional activities
    - Source/destination aggregation
    - Fraud types detected
    - Location/fraud type trend analysis
    - Chargeback events per period, rates, and reasons
    - Fraud rates benchmarked per industry
    - Others as needed per industry or general use case

Additional and related features will be considered as innovations and benefits but not absolute functional requirements in this analysis:

- Solutions which can adequately identify bot-generated activities and present customer administrators with appropriate management options for proactively handling these kinds of activities. Sessions suspected of being manipulated by bots can be handled differently than those believed to be initiated by real users. For example, customers usually can set policies to deny, throttle, or redirect bot traffic while giving priority to real users. This collection of features is not found in all FRIP solutions.
- Geographic and industry-specific compliance regimes and certifications, such as but not limited to AML, GDPR, KYC, OFAC, PCI-DSS, PEPs, PSD2, etc.
- OLAs or service guarantees that provide relief to customers in cases where missed fraud detections or false positives decrease customer revenue
- Support for relevant standards such as OAuth and Global Platform Secure Element (SE) and Trusted Execution Environment (TEE) standards
- Integration with national e-IDs and passports issuers and validators

- Support for advanced use cases outside of only the financial and payments sectors, including but not limited to insurance, retail, media, travel and hospitality, etc.

The criteria evaluated in this Leadership Compass reflect the varieties of use cases, experiences, business rules, and technical capabilities required by KuppingerCole clients today, and what we anticipate clients will need in the future. The products examined meet many of the requirements described above, although they sometimes take different approaches in solving the business problems.

The following are our standard criteria against which we evaluate products and services:

- overall functionality and usability
- internal service security
- size of the company
- number of customers and end-user consumers
- number of developers
- partner ecosystem
- licensing models

Each of the features and criteria listed above will be considered in the product evaluations below.

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

Figure 2: The Overall Leaders in Fraud Reduction Intelligence Platforms

IBM is in the highest position in the Overall Leader rating for Fraud Reduction Intelligence Platforms. Experian, Transmit Security, OneSpan, and BioCatch are grouped just to the left in the Overall Leader chart. Broadcom, Arkose Labs, Outseer (RSA), and ID Dataweb round out the Overall Leaders in this iteration of

the FRIP Leadership Compass.

The top Challengers are HID Global, Group-IB, Kaspersky, and Neustar. ThreatMark and Cleafy debut on the left side of the Challenger section.

There are no Followers in LC FRIP this year.

Overall Leaders are (in alphabetical order):

- Arkose Labs
- BioCatch
- Broadcom
- Experian
- IBM
- ID Dataweb
- OneSpan
- Outseer (RSA)
- Transmit Security

2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.

Figure 3: The Product Leaders in Fraud Reduction Intelligence Platforms

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

Fraud Reduction Intelligence Platforms are ideally composed of six distinct sets of capabilities as described in chapter 1. Not all vendor solutions contain the complete mix of FRIP functions. However, the vendors with the most coverage of FRIP functions have risen to the top of the Product Leader chart in this Leadership Compass.

In the top tier of Product Leadership, we find ID Dataweb and Transmit Security. Both ID Dataweb and

Transmit Security cover all aspects of FRIP in breadth and sufficient depth to justify their positions at the top of the chart.

Next, we see BioCatch and OneSpan. Both appear high in the product leadership chart because of their relative completeness and strength of components within their solutions. BioCatch bases their solution on their industry leading behavioral biometrics with advanced cognitive analysis. In addition to the core set of features, OneSpan has a high-security SDK and remote identity verification app. Experian appears next and has good features in all functional areas of FRIP minus credential intelligence.

IBM, Broadcom, Arkose Labs, HID Global, Kaspersky, and Outseer (RSA) are also product leaders. IBM, Broadcom, and Outseer (RSA) are long established stalwarts in this market. Arkose Labs is a more recent entrant in the FRIP market but has quickly developed an engaging solution around user-friendly CAPTCHA mechanisms and advanced bot detection and management. HID Global is leveraging their identity proofing and identity management capabilities for fraud protection. Kaspersky is a global cybersecurity leader offering fraud prevention services.

Group-IB, Neustar, ThreatMark, and Cleafy are the challengers. All the challengers appear in the top half of the challenger area. Their feature sets differ in terms of areas of functional coverage, but overall the entire challenger field is quite strong.

There are no followers in this section of the Leadership Compass on Fraud Reduction.

Product Leaders (in alphabetical order):

- Arkose Labs
- BioCatch
- Broadcom
- Experian
- HID Global
- IBM
- ID Dataweb
- Kaspersky
- OneSpan
- Outseer (RSA)
- Transmit Security

2.3 Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

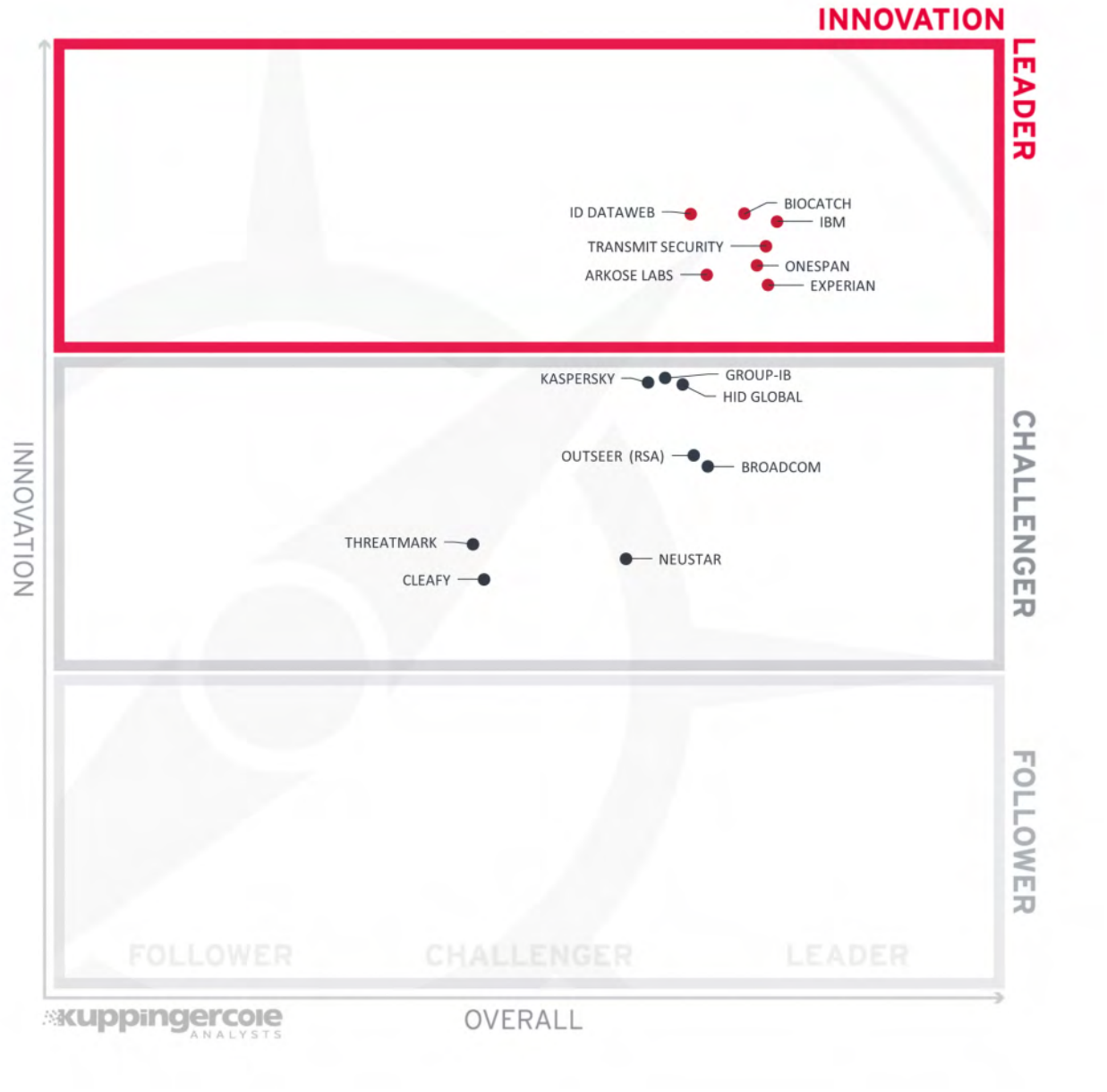


Figure 4: The Innovation Leaders in Fraud Reduction Intelligence Platforms

Innovation in FRIP manifests in several ways. Given the disparity in some of the features defined and technology requirements for delivering them, innovation is embodied by the ability to combine these different kinds of functions. However, the ability to provide these different functions in a unified way is quite challenging. Thus, we see that ID proofing is not provided by all vendors. Another example is bot management. Basic bot detection is a requirement for FRIP, but advanced bot management, which is offered by some vendors, is an innovative discriminator.

Innovation also means going above-and-beyond the basic features. Examples may include mobile SDKs that leverage the TEE and facilitate remote document verification; pulling 3rd-party credential and device

intel; sophisticated and granular risk analytics engines; regulatory compliance features; and the effective use of multiple ML algorithms and trained detection models.

ID Dataweb, BioCatch, and IBM are at the top in Innovation Leadership, with Transmit Security, OneSpan, Arkose Labs, and Experian also appearing in the top section. ID Dataweb expertly combines all fraud reduction intelligence features into their AXN platform, which is also highly extensible. BioCatch is a technological trailblazer in behavioral biometrics and cognitive analysis. IBM's Trusteer excels at device intel and UBA. Transmit Security provides quality capabilities in all areas of FRIP. OneSpan protects its remote identity verification app and SDK with app shielding technology. Experian offers innovative and thorough identity vetting options as well as deep transaction analysis. Arkose Labs is setting trends with its easy-to-use bot deterrent CAPTCHAs.

Group-IB, HID Global, and Kaspersky appear just below the leader bar in the Challenger section, followed by Outseer (RSA) and Broadcom. ThreatMark, Neustar, and Cleafy appear in the lower half of the Challenger area. In order to appear in the Challenger section, each of these companies have products with highly innovative elements that differ somewhat in terms of focus and depth of innovation in each area. For a more complete description, see each company's entry in chapter 5 below.

There are no Followers in Innovation in this version of the Leadership Compass.

Innovation Leaders (in alphabetical order):

- Arkose Labs
- BioCatch
- Experian
- IBM
- ID Dataweb
- OneSpan
- Transmit Security

2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions or entities evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies.

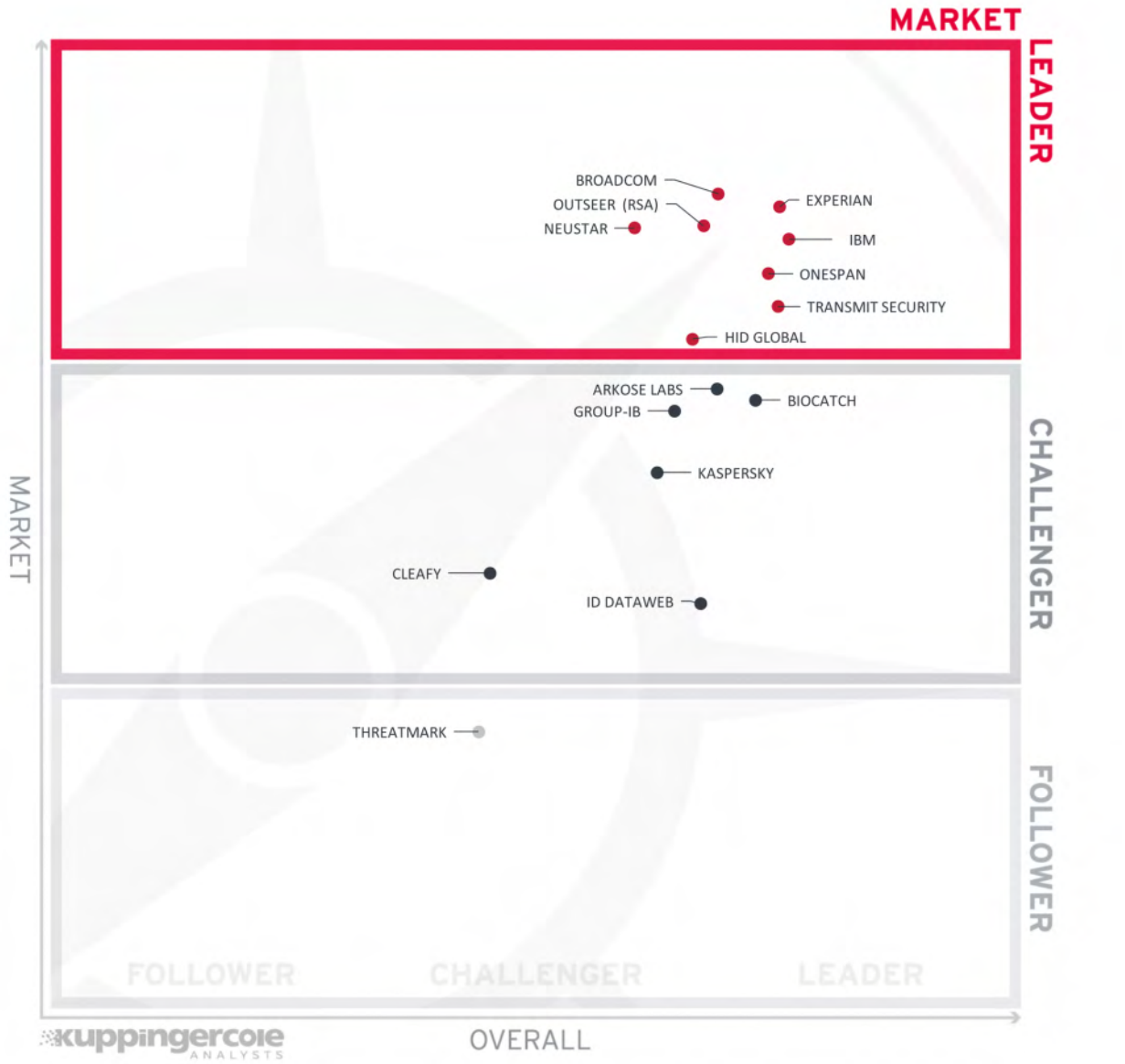


Figure 5: The Market Leaders in Fraud Reduction Intelligence Platforms

Broadcom, Experian, Outseer (RSA), Neustar, and IBM are in the highest echelon of market leadership. They have been in the fraud prevention business for a comparatively long time and have garnered a large customer base. Similarly, OneSpan appears in the market leader ranks, just underneath the top five. Transmit Security is an anti-fraud specialist with a shorter history; however, they have grown rapidly and continue to expand. HID Global is a global market leader in IAM with rich and expanding fraud reduction technologies.

Arkose Labs, BioCatch, Group-IB, and Kaspersky are top market challengers. Each have compelling services and have been experiencing growth in this business-critical sector. ID Dataweb and Cleafy are in

the lower half of the Market Leadership chart, and are likely to see opportunities for expanding their market share.

ThreatMark is at the top of the Follower block. As a fairly recent entrant to the FRIP market, they have not yet captured a share of the market that is commensurate with their capabilities.

Market Leaders (in alphabetical order):

- Broadcom
- Experian
- HID Global
- IBM
- Neustar
- OneSpan
- Outseer (RSA)
- Transmit Security

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

3.1 The Market/Product Matrix

Figure 6: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership. All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

The Market/Product Matrix compares product strength to market position. The Market Champions are Broadcom, Experian, HID Global, IBM, OneSpan, Outseer (RSA), and Transmit Security. These vendors have the strongest alignment between product capabilities and uptake by customers.

Neustar appears in the top center box above the line and is doing very well in terms of market share.

Arkose Labs, BioCatch, Kaspersky, and ID Dataweb are in the middle right box below the line. They have the most potential for growth based on the fortitude of their services.

Group-IB is in the center of the graph and are positioned on the line. Cleafy is in the bottom of the center square, with room to grow.

ThreatMark is in the bottom center box with a fairly strong service and more than adequate ability to acquire a larger share of the market.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

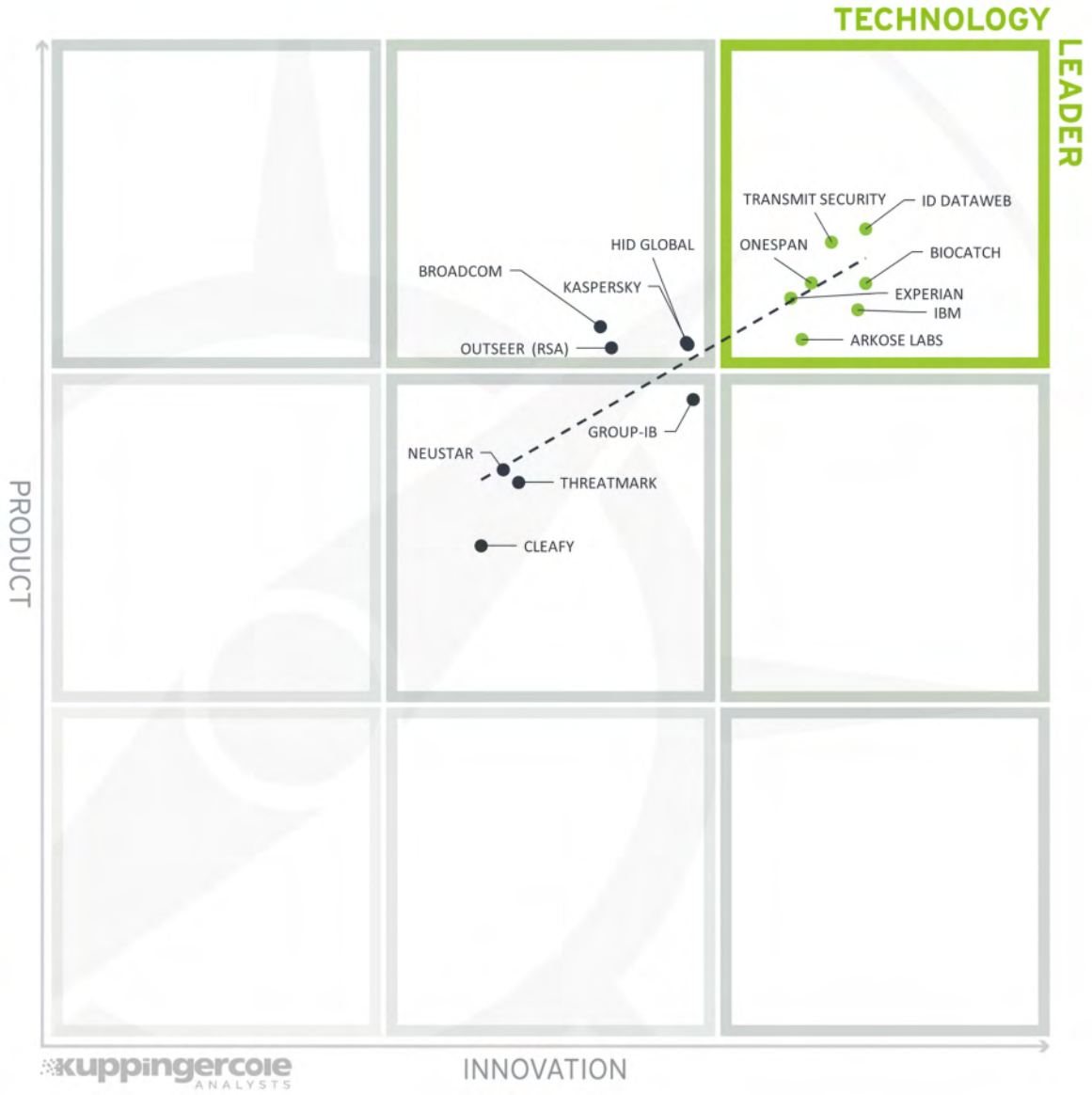


Figure 7: The Product/Innovation Matrix

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The Technology Leaders in FRIP are ID Dataweb, Transmit Security, OneSpan, BioCatch, Experian, IBM, and Arkose Labs.

Broadcom, HID Global, Kaspersky, and Outseer (RSA) are found in the top center box with strong products and median amount of innovation.

Neustar is in the center square and on the line. Group-IB, ThreatMark, and Cleafy also are in the center

square but below the line.

All surveyed vendors appear reasonably close to the line, demonstrating that constant innovation is a true necessity for producing effective services in the Fraud Reduction Intelligence Platforms market.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

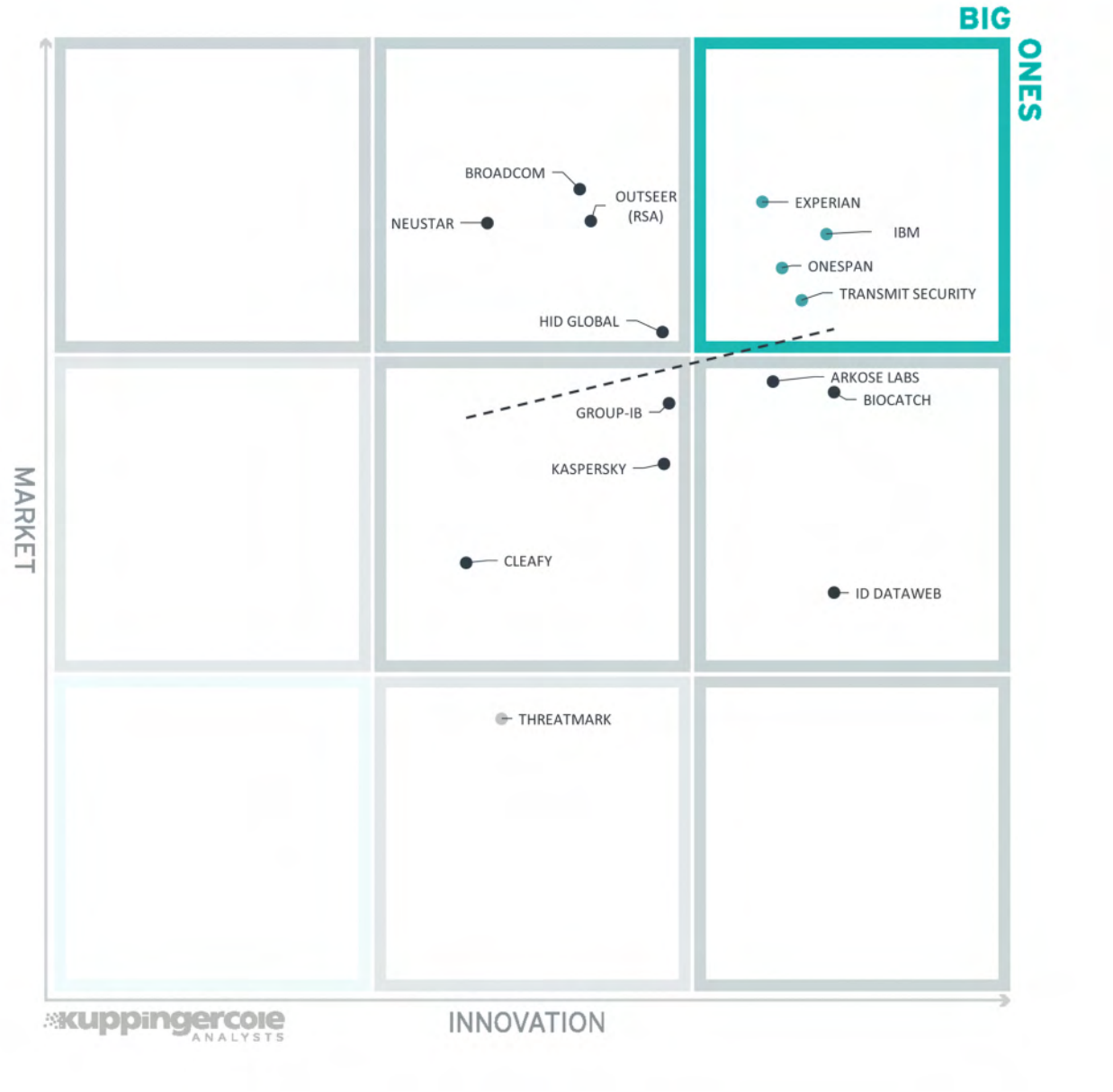


Figure 8: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

The Big Ones in FRIP are Experian, IBM, OneSpan, and Transmit Security. Broadcom, Outseer (RSA), Neustar, and HID Global are to the left of the Big Ones in the top center square. All seven of these vendors are showing excellent market performance for their investments in innovation.

Arkose Labs, BioCatch, and ID Dataweb are in the center right, below the Big Ones. They have highly

innovative products that are likely to fuel their future growth.

Group-IB and Kaspersky are in the center box just below the line. Cleafy also appears in the center box but much lower. The fact that they all are below the line but right of the midpoint of the chart suggests that a greater market position is possible due to their innovative solutions.

ThreatMark is found near the top of the lower center box and has similar opportunities for improving their market position.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Fraud Reduction Intelligence Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Product	Security	Functionality	Interoperability	Usability	Deployment
Arkose Labs Detect and Enforce	positive	positive	neutral	positive	strong positive
BioCatch Platform	strong positive	positive	neutral	strong positive	strong positive
Broadcom Arcot Payment Security Devision	strong positive	positive	positive	positive	strong positive
Cleafy Platform	positive	positive	weak	positive	neutral
Experian CrossCore	positive	positive	strong positive	strong positive	strong positive
Group-IB Fraud Hunting Platform	positive	positive	neutral	positive	positive
HID Global Adaptive Authentication Platform	strong positive	positive	neutral	positive	positive
IBM Security Trusteer	strong positive	strong positive	positive	positive	strong positive
ID Dataweb AXN	strong positive	strong positive	strong positive	strong positive	positive
Kaspersky Fraud Prevention	positive	positive	positive	positive	positive
Neustar Digital Authentication	strong positive	neutral	neutral	positive	positive
OneSpan	positive	strong positive	positive	strong positive	positive
Outseer (RSA) Fraud Manager; 3D Secure and Fraud Action	positive	positive	neutral	positive	neutral
ThreatMark Anti-Fraud Suite (AFS)	positive	positive	neutral	positive	neutral
Transmit Security FlexID	strong positive	strong positive	strong positive	strong positive	positive
Legend		critical	weak	neutral	positive	strong positive

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Arkose Labs	●	●	●	●
BioCatch	●	●	●	●
Broadcom Inc.	●	●	●	●
Cleafy	●	●	●	●
Experian	●	●	●	●
Group-IB	●	●	●	●
HID Global	●	●	●	●
IBM	●	●	●	●
ID Dataweb	●	●	●	●
Kaspersky	●	●	●	●
Neustar	●	●	●	●
OneSpan	●	●	●	●
Outseer (RSA)	●	●	●	●
ThreatMark	●	●	●	●
Transmit Security	●	●	●	●
Legend	● critical	● weak	● neutral	● positive	● strong positive

5 Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC FRIP, we look at the following eight categories:

- ID Proofing - This category rates the quantity, quality, and jurisdictional variety of integration and interoperability capabilities for identity proofing and vetting as defined in Chapter 1. Many FRIP services programmatically query specialty 3rd-party identity vetting services. ID Proofing is not merely performing transaction time comparisons to templates created at registration time. Rather, this metric considers both built-in functions and configurable callouts to authoritative attribute providers.
- (Compromised) Credential Intel - This category rates the capabilities for obtaining updated information about the status of credentials used in transactions, from both within the vendor customer ecosystem and from external sources.
- UBA – This category assesses the capabilities with regard to processing historical information about the subject user and past transactions to determine baseline profiles for analysis against current request contexts to identify and classify anomalous behavior. Examples of common UBA parameters include frequency/time of logins, failed login patterns, transaction types and amounts, transaction frequency/patterns, exceptions for known travel, and user profile changes.
- Device Intel - This category is the combination of device intelligence parameters including device fingerprint, type, health assessments, device and IP reputation, etc., as described in Chapter 1. FRIP services commonly draw upon multiple sources. Some of the vendors examined below provide these functions to other FRIP vendors.
- Behavioral Biometrics – This measures the presence and sophistication of behavioral biometrics within the solution. Behavioral biometrics is generally implemented as JavaScript downloaded to consumer browsers and information collected from mobile devices by vendors' SDKs. Behavioral

biometrics can create profiles on users based on their interaction with keyboards, mice, and touchscreens as well as certain device specific parameters.

- Bot Detection - This category considers the ability of vendor solutions to analyze traffic in real-time to identify whether it is initiated by legitimate users or bots. For this report, bot detection capabilities are recommended, and products with comprehensive bot management functions will be noted as innovative.
- Risk Engine - This category represents the collection of functions provided by the vendor for receiving the various forms of intelligence, processing the sets of relevant information, and providing usable outputs for customer applications and infrastructure. Features considered here include complexity and customizability of policies, depth and granularity of available output options, rationale provided to customers for individual transaction processing decisions, and the use of Machine Learning algorithms and detection models in assessing intelligence sources and other input. The usability of analyst and policy manager interface is reflected in this category as well.
- Scalability - Some solutions have massive scalability while others do not. Picking the right size vendor is an important consideration in RFPs. Not everyone needs the biggest and most scalable solutions. But if your business does, then understanding the scalability comparison and factors examined will be of paramount interest. The most scalable solutions are usually those which are based on micro-services architectures. This rating is influenced by many factors including number of customers, consumers, deployment models, multi-cloud utilization, geographic distribution, SLAs, and maximum number transactions per second. Availability is a related measure, in that, truly scalable systems must have very high availability. Guaranteed uptimes range from 99% to 99.999%, with 99.5% being the median value.

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services may have gaps in certain areas, while are strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations of Fraud Reduction technologies.

5.1 Arkose Labs

Arkose Labs is a well-funded startup established in 2017 out in San Francisco. Their solution is focused on reduction of the most common fraud types, covering the majority of finance, retail, gaming, etc. use cases, as well as inventory hoarding, screen scraping, loyalty card abuse, and fake reviews. It does not feature call center integration. The service is hosted in AWS and Azure data centers covering all regions of the globe. Licensing is per-transaction, and there are fixed cost options available.

Arkose Labs Detect and Enforce relies on a combination of proprietary UBA techniques in lieu of identity vetting. It does not support lookups against 3rd-party identity vetting services. In-network compromised credential information informs the risk engine, and external sources can be configured via APIs. For UBA, all the common data points are evaluated, with the exception of transaction amounts and known travel. Arkose Labs uses multiple standard and in-house developed supervised ML detection algorithms for classification as well as a mix of unsupervised ML models for anomaly detection.

Device intelligence functions include device type, custom fingerprinting techniques, various IP reputation sources, and computation of geo-velocity. Device health is not assessed. Arkose Labs' behavioral biometrics implementation considers gyroscopic analysis and uses JavaScript to pull keyboard/mouse/touchscreen interaction characteristics. Mobile environmental attributes are not evaluated. The solution includes highly innovative and user-friendly CAPTCHA challenges for not only identity risk analysis but also for bot detection. Customers can work with Arkose Labs Technical Account Managers to create detailed policies for advanced bot management.

The risk analysis engine outputs verdicts with textual justifications which are only visible to customers. Customers work with Arkose Labs Technical Account Managers to define policies and weightings of risk factors within policies. Dashboards and reports show fraud types detected by groups, location/type trend analysis, session flows, throughput rates of legitimate vs. suspicious vs. fraudulent traffic. Key exchange is used for API authentication.

Arkose Labs is a well-funded and growing startup that has attracted major global customers, which attests to their ability to scale up as needed. Detect and Enforce are SSAE 18 SOC 2 Type 2 compliant, and they are targeting mid-year for FIPS 140-2 certification for crypto components. The solution excels at bot detection and management and has adequate UBA and device intel capabilities. Connections for ID proofing, support for more API authentication standards such as JWT and SAML, and device health and additional behavioral biometrics attributes would strengthen the offering. Organizations of any size looking for hosted fraud reduction services that need coverage for financial, retail, and gaming use cases should consider Arkose Labs Detect and Enforce solution.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●●

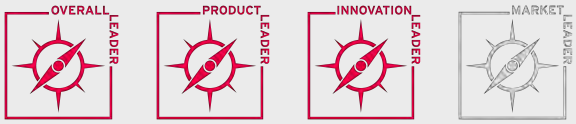
Strengths

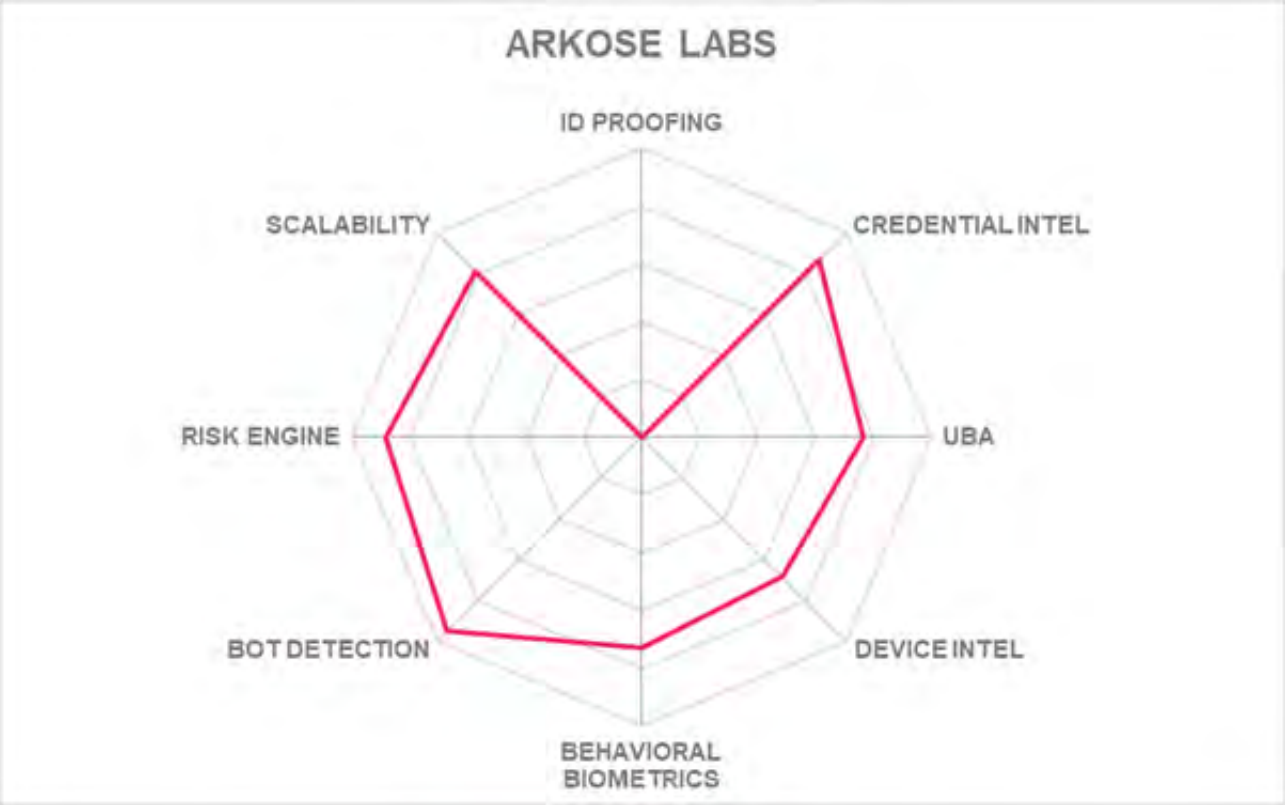
- Highly functional and user-friendly CAPTCHAs
- Good array of unsupervised ML algorithms for anomaly detection
- Mix of open source and proprietary supervised ML algorithms for behavioral analysis and device intelligence
- Strong device fingerprinting and detection of device outliers, such as randomized device identity attributes
- Advanced, policy-based bot management available
- Quick integration with customer apps

Challenges

- Integration with identity proofing services is not present but is on the roadmap
- Policy creation and maintenance currently requires vendor assistance
- Device health and environmental attributes are not evaluated
- Additional standards-based API authentication methods are needed

Leader in




ARKOSE LABS
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.2 BioCatch

BioCatch is a well-funded, late-stage venture-backed FRIP service provider that was founded in Tel Aviv in 2011. They have offices around the world and are focused on risk reduction for financial industry customers. Use cases they address include Account Opening Fraud Protection, Account Takeover Fraud Protection, Social Engineering Fraud Detection, Mule Account Detection, Business Email Compromise (BEC) Detection, and enabling PSD2/SCA compliance. Their service is hosted in Microsoft Azure across APAC, EU, and NA regions. Licensing is priced annually per transaction volume in most cases, but also by active users for ATO protection.

BioCatch deploys JavaScript on browsers and mobile SDKs to collect behavioral biometrics and perform cognitive analysis, which allows their solution to discover behavioral anomalies and criminal indicators including low familiarity with subject PII, high application fluency, excessive deleting, copy/paste activity, etc., even at the time of account opening. This is their method for vetting identities. BioCatch does not support integration of 3rd-party identity vetting services, compromised credential intelligence, or remote document validation. The UBA capabilities are comprehensive for financial use cases, covering transaction details and known travel, which are not ubiquitously offered by FRIP solutions. Moreover, BioCatch stores up to 3 years of user profile data to enhance UBA.

For device intel, BioCatch evaluates most expected parameters such as device and IP reputations. BioCatch's device health assessment is limited to inventorying other installed apps on users' devices. BioCatch does access IMEI and SIM info for consumer mobiles and can use this to detect SIM swap attacks. Their implementation of behavioral biometrics takes full advantage of all available sensors on modern mobiles as well as all ascertainable environmental attributes. Device intel and behavioral biometrics enhance BioCatch's UBA and form the basis of their patented and highly effective bot detection capabilities.

The risk engine uses multiple ML detection models, is accessible to customers via API, and can return not only risk scores but also detailed rationales for decisions. BioCatch supports HTTP, JWT, and mutual authentication for APIs. The Rule and Case Manager and Analyst Station interfaces are intuitive. Enforcement actions are customizable beyond the basic allow/deny/step-up. Basic reports and dashboard are present, but customers must work with BioCatch Professional Services to define additional reports if needed. The service employs standard web application and network layer protection for high availability. Event data can be passed to customer SIEMs via APIs but not CEF or syslog standards, and the solution does not have connectors for ITSMs.

BioCatch is ISO 27001 and SSAE SOC 2 Type 2 certified. The BioCatch suite offers protection against not only the common fraud types but also enables compliance with AML, KYC, OFAC, PEP, PSD2, and 3DS2 regulations and standards. The solution is scalable and globally distributed. A multi-cloud strategy would further enhance scalability and availability. BioCatch's solution is highly innovative, particularly with regard to the cognitive analysis afforded by the behavioral biometrics features. Financial companies that need to reduce fraud should definitely take a look at BioCatch's offering.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●●
Deployment	●●●●●

BioCatch

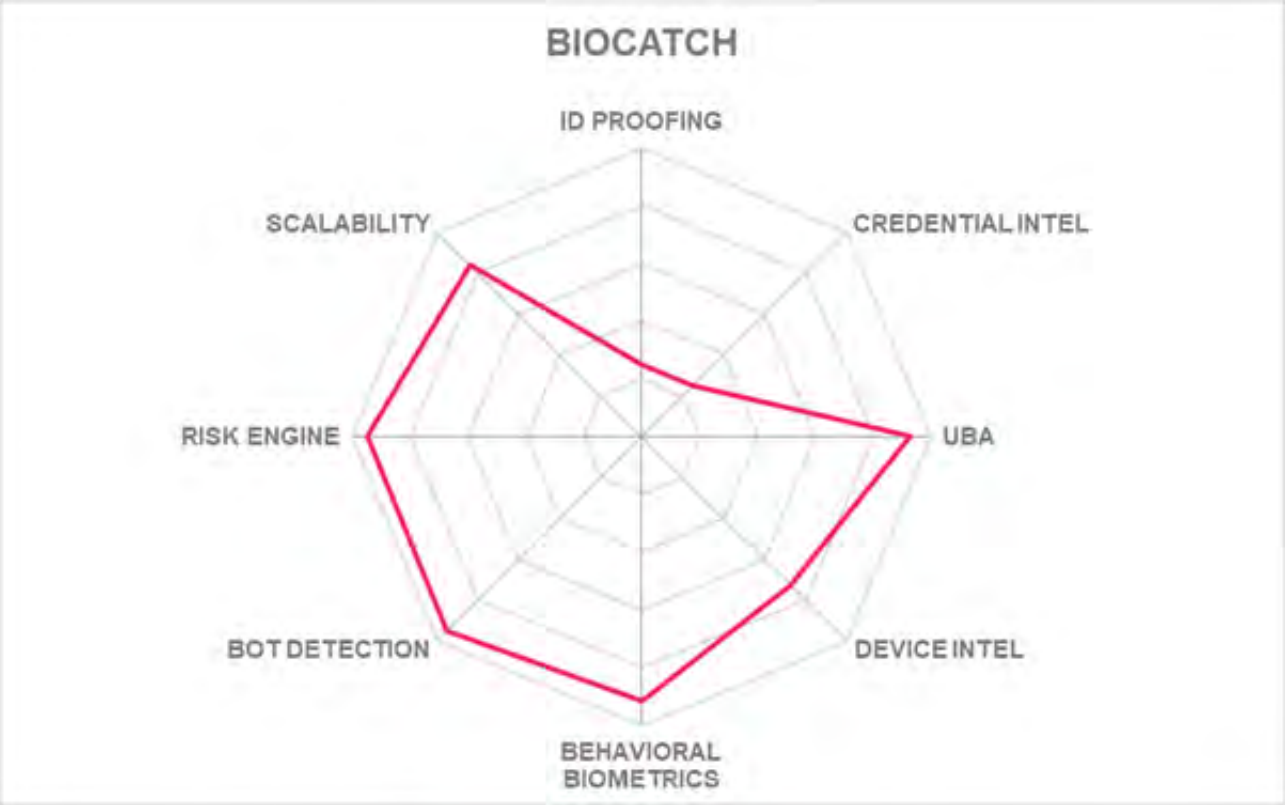
Strengths

- Full range of behavioral biometrics
- Cognitive analysis discovers fraud types that other solutions might miss
- Excellent implementation of ML algorithms for not only detecting anomalies but accurately classifying malicious behavior
- Admin user-friendly interface for policy authoring
- High performance multi-regional cloud deployment with data localization
- APIs allow inclusion of 3rd-party threat intelligence feeds
- Can detect SIM swaps and social engineering voice scams

Challenges

- Additional 3rd-party credential intel and device/IP reputation feeds would add value for customers
- Identity proofing limited to analysis of user behavior at registration time
- Device health assessments limited to installed apps inventories, with jailbreak check on the roadmap
- No connectors for ITSM or SIEM but can be configured over APIs

Leader in


BIOCATCH
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.3 Broadcom Inc.

Broadcom's entry in this market originated with Arcot Systems, a 3DS pioneer acquired by CA Technologies in 2010. Broadcom, a global IT vendor, has assimilated Symantec as well as CA Technologies. Their "Arcot Network" solution offering comprising Arcot for Issuers and Arcot for Merchants are heavily used by credit card issuers, processors, merchants, and banks. The Digital Banking product has been rolled into The Arcot Network as of 2021. Broadcom has functionality in the areas of device intel, passive biometrics, and UBA. It is designed to support 3DS and PSD2. The solution is SaaS-based and is hosted within both their own facilities and Google Cloud at US locations. Broadcom offers licensing contracts with unlimited numbers of transactions.

Broadcom does not support identity proofing integrations or document verification but does utilize in-network credential intelligence. Broadcom's UBA functions assess standard user actions as well as detailed analysis of transaction amounts, types, history for both CNP EMV 3DS and non-CNP transactions such as account transfers. Up to five years of UBA history can be stored without association to PII or PCI data.

Their device intelligence capabilities take into consideration device fingerprint, type, IMEI number, IP reputation, geo-location, and geo-velocity. Device health assessment requires 3rd-party apps. The combination of device data plus UBA and other device intel enables Broadcom to discover and alert on SIM swap attacks. Broadcom uses a mix of unsupervised ML for detection and supervised ML for classification, including advanced algorithms designed in-house. Broadcom supports a variety of third-party JavaScript integrations to harvest keystroke dynamics, and partners with other companies for EMV 3DS SDKs for passive biometrics. Rudimentary bot detection is possible via UBA and IP address reputation inisghts. Call center integration is not directly available.

Customers can configure their own rules for risk analysis and apply different weights to variables as their businesses require. Action code results are permit, deny, step-up, log, and alert. Recommendations for actions and rationales are provided to customers. Basic case information is tracked in reports. Broadcom can integrate with customer case management systems. The risk engine is addressable via API, with JWT, OAuth2, OIDC, and SAML for authentication. Transaction information can be passed to customer SIEMs.

Broadcom is PCI-DSS and SSAE 18 SOC 2 Type 2 certified. The Arcot for Digital Banking platform offers customers scalability and support for complex use cases in this area as well as for other industries. Broadcom offers one of the highest uptime SLAs in the FRIP space. The solution has excellent internal platform security. Enhancing passive biometrics and including support for identity proofing, credential intelligence, and bot detection would extend the solution for other use cases. Companies looking for proven FRIP solutions particularly in the payment services sector should review Broadcom Arcot Network capabilities.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●

BROADCOM

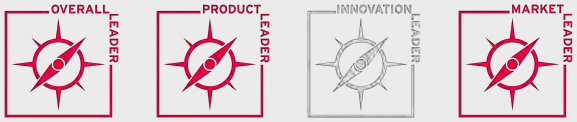
Strengths

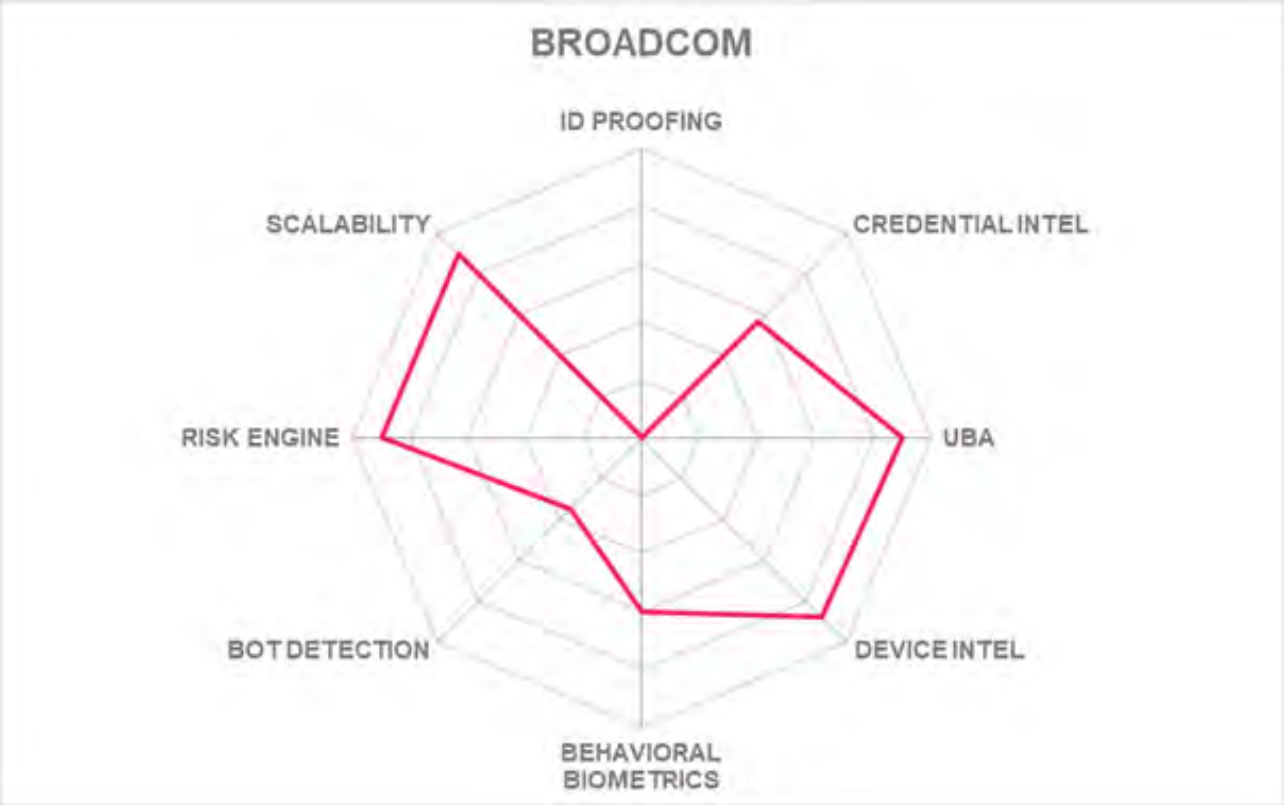
- UBA tailored for most types of financial transactions
- Long default data retention period
- Advanced ML detection algorithms
- SIM swap detection supported via 3rd-party integrations
- Unlimited transactions licensing plans for enterprise customers
- Detailed device fingerprinting techniques
- High uptime SLA and fast implementations

Challenges

- No identity proofing integration
- Does not integrate with 3rd-party compromised credential intel
- Device health assessment requires 3rd-party apps
- Bot detection capabilities are limited

Leader in




BROADCOM
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.4 Cleafy

Cleafy was established in 2014 in Milan. In 2017, it became part of the Moviri Group, a global software and professional services company with offices in Italy and the US. Cleafy offers agentless endpoint protection as well as anti-fraud services. The service is multi-tenant SaaS running on GCP, with full elasticity planned for later in 2021, and hosting locations can be chosen by customers. Cleafy is focused on PSD2 compliance. Licensing is by the number of active users per year and by Cleafy modules selected.

Cleafy does not link to identity proofing services or perform document verification. The Platform utilizes in-network compromised credential intelligence, and customers could configure other sources if needed. The UBA functions examine all relevant attributes, including transaction details and up to 60 days of history.

Cleafy relies on JavaScript and mobile SDK to collect device intelligence, which spans the full range of discoverable attributes. Cleafy has special emphasis on accurate malware detection by behavioral analysis, which helps clients meet PSD2 requirements. IP reputation information comes from MaxMind, and other feeds could be evaluated at customer's discretion. The JavaScript and SDK components also function as behavioral biometrics, analyzing keyboard/mouse usage, gestures, network information, and SIM data if accessible via device OS. The combination of UBA and behavioral biometrics allow for bot detection. Advanced bot management is not required by their target customers.

All behavioral data passes through ML detection models for anomaly discovery and classification. More advanced proprietary ML detection models are slated for inclusion in 2021. The risk engine offers maximum flexibility: customers can write their own detection criteria and create action types based on risk factors they can define; the detection models can then be trained on customer provided data. The analyst interface has a modern look making it easy to operate. Reports are available, and customers can create ad hoc queries which can be turned into automatable and schedulable reports. Customer access is via protected APIs, which can be rate-limited. JWT, OAuth2, and SAML are not supported for service authentication. Ingested data is not signed or encrypted. Event information can be sent to SIEMs over syslog.

Cleafy is a small but growing revenue-positive and debt-free vendor. Their cloud strategy should allow them to scale to meet customer load demands. They are pursuing ISO 27001/27018, PCI-DSS, and SOC 2 compliance in 2021. Cleafy Platform has some highly innovative features, particularly in the analyst interface, with regards to customizing detection policies and actions. Though the solution is missing a few features of the broader FRIP landscape, organizations in the finance and payments business that need a tweakable policy GUI and risk engine and advanced malware detection for PSD2 should explore the Cleafy Platform.

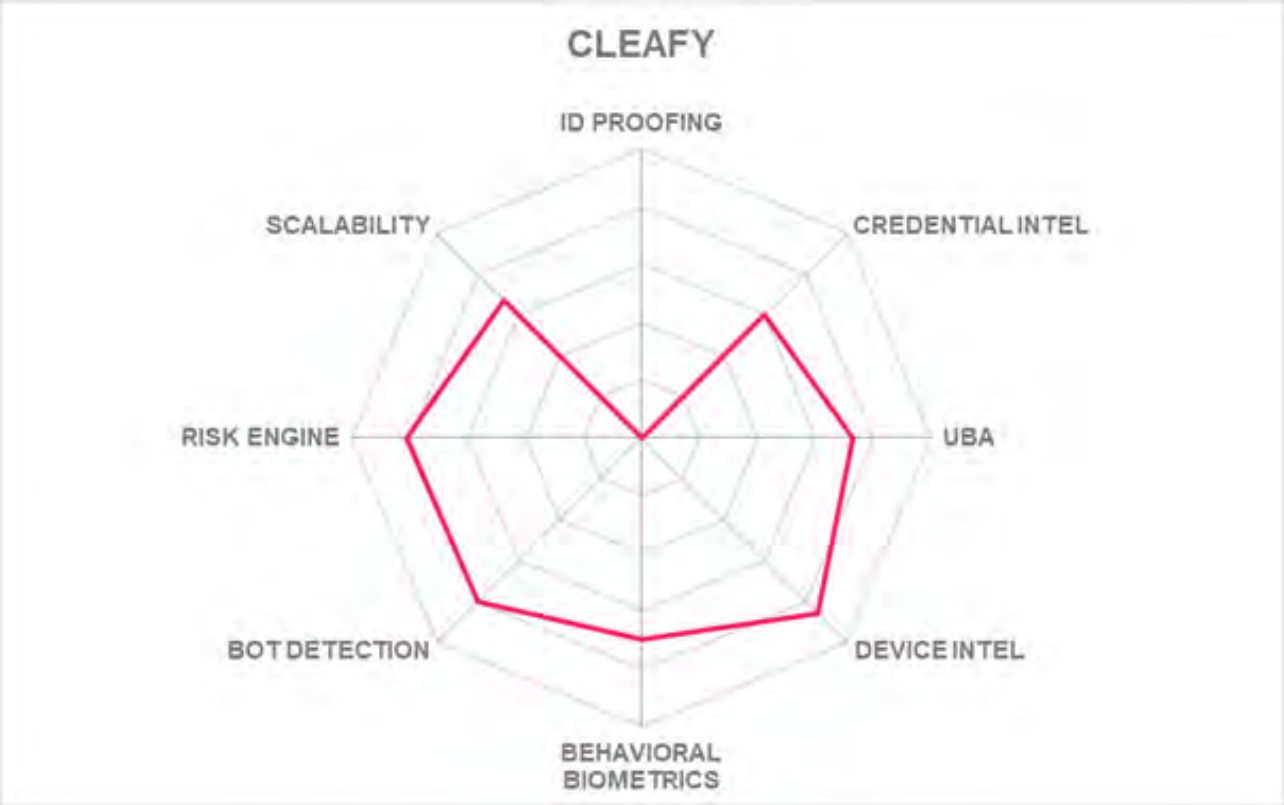
Security	●●●●○
Functionality	●●●●○
Interoperability	●●○○○
Usability	●●●●○
Deployment	●●●○○

Strengths

- Fast deployments
- Sophisticated malware detection by behavioral analysis
- Good implementation of UBA
- Highly flexible and configurable fraud risk engine

Challenges

- Connectors for ID proofing and external credential intel would allow the platform to serve other use cases
- Needs support for JWT, OAuth2, and SAML for API authentication
- Ingested data should be signed and encrypted to prevent tampering
- Small but growing vendor


CLEAFY
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.5 Experian

Experian was founded in 1996 and is headquartered in Dublin. It is one of the “Big Three” credit rating agencies, processing information on over one billion people worldwide. It provides credit history information to financial institutions, and analytics and marketing information for other customers. For fraud prevention, Experian has CrossCore, which addresses identity proofing, UBA, device intelligence, behavioral biometrics (via partners), and bot detection. CrossCore is designed to aggregate various fraud sources to consolidate decisioning for Experian customers at both account opening and transaction time. Additionally, Experian supports AML, KYC, OFAC, and PEP compliance. CrossCore runs as SaaS in globally distributed data centers in their own facilities, AWS, Azure, Cloud9, and Oracle Cloud. Licensing models are based on per-login/transaction per time period and fraud use case types covered.

As an authoritative attribute provider, Experian offers comprehensive identity proofing services, with bi-directional links to various government agencies and financial institutions and partnerships with vendors of app-based remote document verification with liveness detection functions, behavioral and traditional biometric capabilities, email verification, alternative identity data, and mobile verification solutions. Partners include Acuant, Daon, IDfy, Mitek, Onfido, eMailage, Ekata, BioCatch, GDC, Boku, and RapidID. Compromised credential intelligence integration is under consideration. Experian performs detailed UBA, looking at parameters such as login patterns, profile changes, cross-account activities, shopping cart data, time zone vs. clock settings, etc.

CrossCore pulls in device intelligence data points from multiple sources. Adding direct device health assessments would be useful. Advanced behavioral biometrics capabilities are available through integration with BioCatch and Daon. Behavioral biometrics plus signatures enable bot detection.

Experian applies open-source, proprietary, and 3rd-party ML detection models against these data sources to make real-time risk decisions. The risk engine itself is not directly exposed via APIs. Customers can select data sources, assign priorities, and apply conditional logic for their specific use cases in the well-constructed Workflow Manager. CrossCore outputs verdicts, recommendations, and rationales rather than risk scores. The Event Viewer portal facilitates investigations by allowing analysts to see results of individual steps and tests per transaction. Experian secures the service using a WAF, enforces rate limiting on APIs, and has DDoS protection. Data export to SIEMs is not available. JWT, OAuth2, and SAML are supported for API authentication.

Experian’s CrossCore is highly scalable, handling millions of transactions per day. They have obtained certifications for HIPAA, ISO 27001 and 22301, PCI-DSS Level 1, and SSAE SOC 2 Type 2. Experian is trusted by governments and financial institutions around the world as an authoritative attribute provider. CrossCore’s technical capabilities for fraud reduction are well-suited for detecting account opening and ATO fraud. Beyond their native identity proofing, device intelligence, network analysis, and transactional risking capabilities, through partnerships, they add strong features in document verification, behavioral biometrics, and bot detection. Organizations looking for FRIP services with a global reach should consider Experian CrossCore.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●

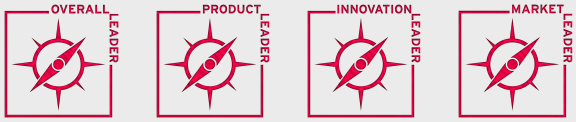
Strengths

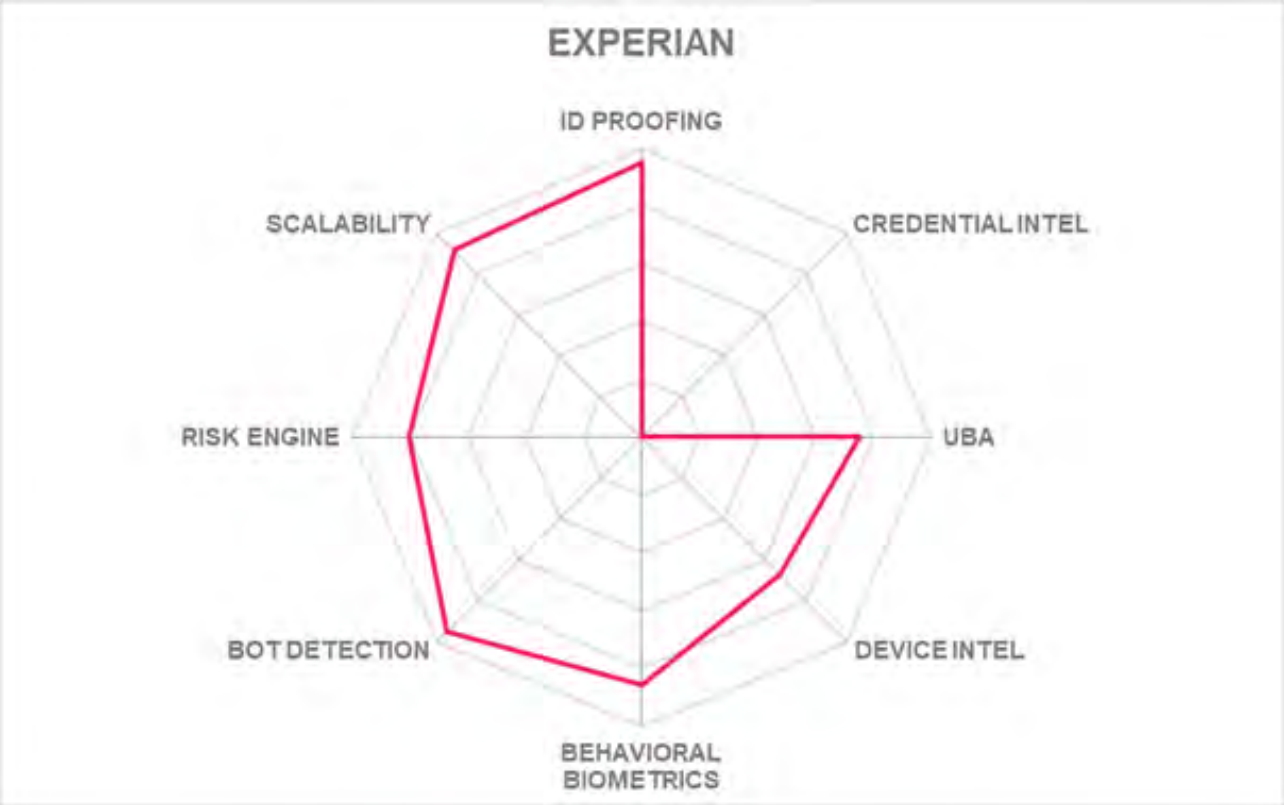
- Internationally recognized authoritative attribute provider
- Integration with document verification, device intel, and behavioral biometrics suppliers
- Highly configurable policy and decisioning engine
- Ideally positioned to detect account opening fraud
- Technical partnerships enable ATO, SIM swap, and bot detection
- Support for AML, KYC, OFAC, and PEP compliance
- Digital identity protection services

Challenges

- Compromised credential intelligence services are not present but under consideration
- Comparatively long deployment times
- More complex licensing model factors in fraud type use cases
- Device health assessment would enhance device intelligence

Leader in




EXPERIAN
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.6 Group-IB

Privately held Group-IB was founded in 2003 in Moscow, but its global HQ is in Singapore. Beyond FRIP services, Group-IB offers threat intelligence, threat hunting, and anti-piracy products. Fraud Hunting Platform (FHP) has functionality in compromised credential and device intelligence, UBA, behavioral biometrics, and bot detection. Partnership with Sumsub adds identity proofing capabilities. Customers can also utilize their services with customization to aid in AML, KYC, OFAC, PSD2, and 3DS2 compliance. Their services are hosted in their own facilities in APAC and EU regions. Options for deploying at customer sites or on customer private clouds are available. Licensing costs depend on the number of active users per contract period.

Group-IB partners with Sumsub for identity proofing services including remote ID verification, biometric analysis with liveness detection, AML/KYC and KYB (Know Your Business) compliance. Credential intelligence comes from in-network sources as well as Telesign and RU FS-CERT. Group-IB's UBA functions scrutinize logins, navigation patterns, history, and transaction details.

FHP uses JavaScript and a mobile SDK to deliver device intel and behavioral biometrics components. Group-IB's device intelligence capabilities are comprehensive, covering detailed device fingerprints, device health evaluations, external and internal IP reputation sources, and mobile platform-dependent data where permitted. Likewise, FHP's passive biometric implementation assesses all available parameters, such as keyboard/mouse, touchscreen, swipe, gesture, and network factors. Behavioral biometrics plus embedded pixels can be used to detect bot activities and alert customers so that their applications can handle them appropriately. Group-IB offers full traffic proxy options for customers who want comprehensive bot management. Their behavioral biometrics functions can identify users across multiple devices and detect when a known user gets a new device. SIM swap detection is possible based on not only subscriber information, but in cases where that is not available, can proceed using behavioral biometrics alone. All analytic operations are powered by their proprietary clustering, gradient boosting, and supervised ML detection models. Call center integration with phone-to-web session mapping is available.

New rules for the risk engine are typically configured by Group-IB with customer input. FHP is moving to a direct customer management model. Customers can have various data sources included in policy evaluations and customize the priority of risk factors and result codes. Customer dashboards include a wide variety of standard metrics such as fraud types and locations. The fraud analyst interface provides several primary visualizations to facilitate investigations and includes a detailed timeline view with per-entry risk ratings and historical analysis for comparison to current sessions. Application integration utilizes APIs, which only supports OAuth2 authentication currently. FHP can send to SIEMs and they have connectors for ArcSight, MaxPatrol, QRadar, and Splunk.

Group-IB reports high utilization and thus good scalability, but their standard SaaS SLA uptime is comparatively low. Group-IB offers their services in private cloud deployments to give customers more control, the highest possible uptime, and lowest latency performance for those who need or prefer those options. Group-IB attests that their service is ISO 27001, PCI-DSS, and SOC 2 Type 2 compliant. Updating

API authentication methods to adhere to additional secure standards would be beneficial. Strong authentication for administrators is needed. Allowing customers to create rules directly will likely improve usability for advanced clients. Their partnership with Sumsub adds advanced identity proofing functions. Fraud Hunting Platform's strengths in UBA, device intel, and behavioral biometrics warrant consideration from enterprises looking for FRIP solutions, particularly in the EMEA and APAC regions where they are most active.

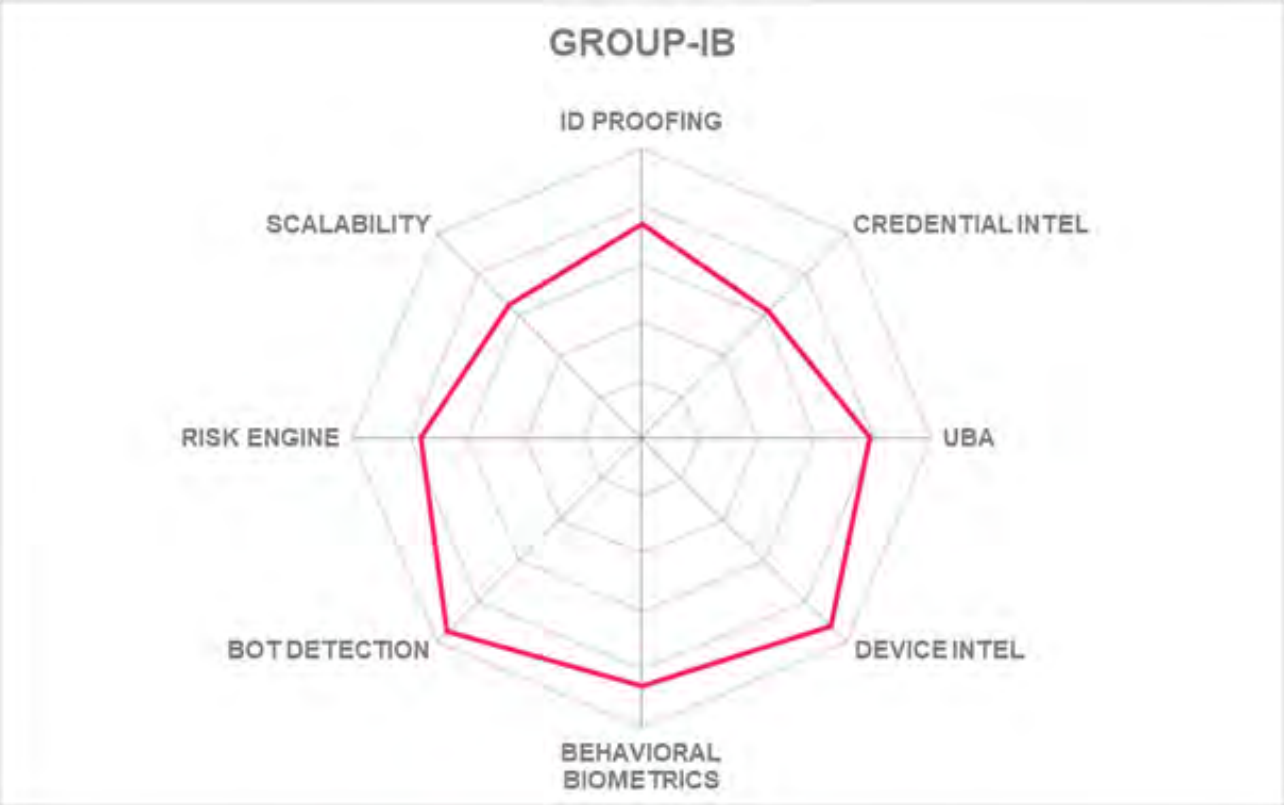
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○

Strengths

- Exhaustive device intel capabilities
- Good selection of behavioral biometrics attributes examined
- Advanced bot management available
- Sophisticated array of ML detection models
- Cross-channel UBA builds complex user profiles across multiple browsers and devices
- Transaction detail analysis
- Excellent fraud analyst interface promotes efficient investigations

Challenges

- Customers are currently limited to rule scoring adjustments and must work with Group-IB to create new rules; full direct customer management expected late 2021
- Support for additional API authentication standards needed
- Comparatively low uptime guarantee SLA


GROUP-IB
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.7 HID Global

HID Global is a subsidiary of ASSA ABLOY Group AB of Stockholm. HID Global's US headquarters is in Austin, TX. HID Global has IAM solutions, and makes physical access controls systems, RFID tags and readers, biometric readers, smart cards, passports and some national identity cards, card readers, and mobile apps capable of remote identity verification. Their intersection of IAM, biometrics, and SDK allows them to perform identity card issuance for several organizations. The Adaptive Platform offers fraud prevention components including ID proofing, credential and device intelligence, behavioral biometrics, UBA, and bot detection. It can be installed locally or in IaaS, and their SaaS is hosted in AWS in both EU and NA regions. Licensing is per registered user, and per-transaction options are available.

HID Global provides identity assurance verification and credential issuance services. Government and enterprise customers can utilize HID Global for authoritative attribute lookups, remote document verification, and electronic credential assignment. For remote document proofing scenarios, users utilize the smartphone app to scan and register the authoritative documents, take selfies, and perform real-time biometric matching. The Authentication Platform utilizes in-network compromised credential intelligence, but external feeds are not yet considered. HID Global's UBA functions encompass full transaction history details. Per-tenant crypto keys are managed to promote maximum data security.

The use of JavaScript and the mobile SDK allows for collecting device intelligence and behavioral biometrics. Device intel capabilities cover the normal range of functions, including advanced fingerprinting. Device health is assessed by behavior. MNO subscriber and IMEI data are not gathered but SIM swaps can be detected with device fingerprinting and behavioral biometrics. Behavioral biometric features include keyboard/mouse, swipe/touchscreen, gyroscopic and light sensor analysis; these functions also provide basic bot detection. The Platform can determine if session activity is artificial in origin, then informs customers who can block or require step-up authorization.

HID Global's risk engine allows customers to prioritize risk factors. The score output ranges from 0-1000 with four major action recommendations. The policy authoring interface is flow-chart driven. The fraud analyst interface is very intuitive and includes a detailed timeline view to expedite investigations. The solution does not offer integration with 3rd-party ITSM or SIEM systems. Customer apps communicate via REST APIs. JWT, OAuth, OIDC, and SAML can be used for API authentication.

HID Global is a market leader in authentication solutions. Their focus is on B2C use cases in the finance and healthcare industries and providing G2C solutions for government agencies around the world. In fact, some implementation partners package HID Global Authentication Platform to serve as the consumer front-end for their "bank-in-a-box" offerings. HID Global attests and/or has certified on FIPS 140-2, ISO 27001, and SOC 2 Type 1. SOC2 Type 2 certification is in work. Inclusion of 3rd-party intelligence sources in the risk evaluation would strengthen the offering. The remote document verification for onboarding, strong identity proofing, and transaction level UBA features make HID Global worth considering as a FRIP solution for financial customers.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○

HID®

Strengths

- Identity proofing and strong credential issuance capabilities present, including some government IDs
- App for remote document verification
- Easy-to-use flow-chart style policy authoring and analyst interfaces
- Device intelligence and behavioral biometrics can be collected using secure SDK, including some uncommon attributes
- Transaction level UBA
- FIDO 2.0 and FIPS 140-2 certified components
- Incident response and site takedown services

Challenges

- Basic bot detection available but advanced management is not
- Internal-only compromised credential intelligence
- External sources of device and IP intelligence could be beneficial
- No ITSM integration

Leader in


HID GLOBAL
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.8 IBM

IBM is a global technology and consulting company headquartered in New York. IBM offers a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and information security. Trusteer is the service for fraud reduction. The integrated suite covers all aspects of FRIP except identity proofing. IBM offers industry-specific profiles and support for KYC and PSD2. Trusteer is hosted in AWS data centers around the world. Licensing options include per login, per contract period, and by numbers of active or registered users.

Trusteer does not support identity document verification or callouts to 3rd-party identity proofing services. The service uses in-network sources only for compromised credential intelligence. Trusteer does support integration with 3rd-party vendors for phone number intelligence and carrier data, email reputation, IP enrichment and reputation and other external threat intelligence sources. Trusteer has thorough UBA, assessing a wide range of user behaviors including transaction details and history.

Customers can use the secure mobile SDK, which collects the full gamut of device intelligence characteristics, including device health assessments, mobile malware detection, and IMEI/SIM and history from MNOs. Call center integration could be configured. The robust behavioral biometrics are delivered via JavaScript and the mobile SDK. Signature definition with customers combined with device intel and passive biometrics enables Trusteer to perform bot detection.
The risk engine is granular, allowing weighting of risk factors within policies, and is accessible by APIs. The risk engine outputs score from 0-1000, recommendations, and reason codes for customers. A single user interface serves as the starting point for both admins and analysts, allowing deep dives into incident investigation, report generation, and policy creation. The four major actions are allow, block, restrict, and authenticate. Basic reports are available, and cases can be managed within Trusteer itself, rather than external ITSM solutions. App integration and security infrastructure interoperability are possible via APIs. SAML can be used for API authentication. Trusteer can also be integrated with IBM QRadar.

IBM's security solutions are widely used across many enterprises and are known to be highly scalable. Trusteer services are ISO 27001 and SOC 2 Type 2 certified. Organizations with existing IBM security solutions in place may find it easy to add Trusteer for Fraud Reduction Intelligence purposes. Organizations that are looking to acquire or update FRIP services, particularly those that need strong device intel, behavioral biometrics, and UBA features, may want to consider IBM's strengths in these areas. Trusteer would benefit from integrations with 3rd-party identity proofing services and advanced bot management functionality.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●●

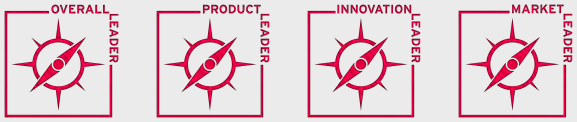
Strengths

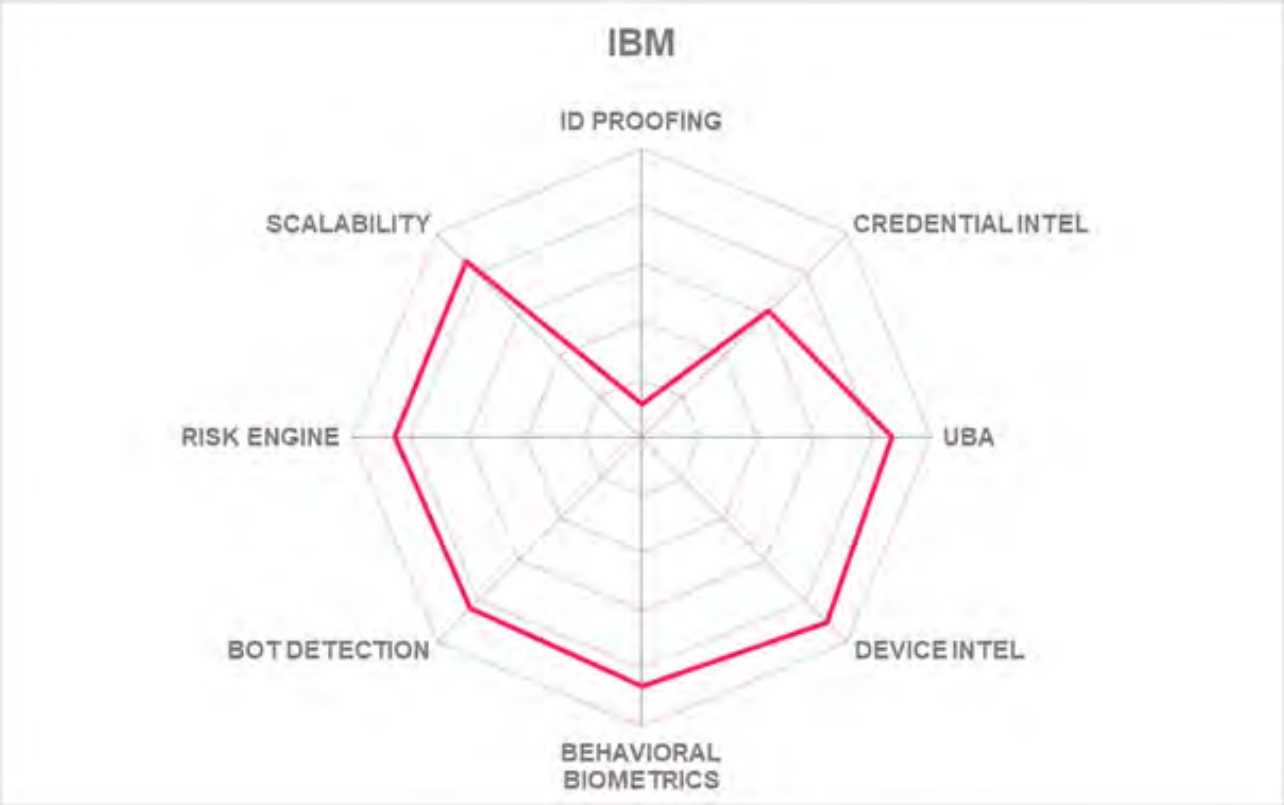
- Excellent UBA considering all pertinent attributes
- Comprehensive device intelligence features
- Malware detection functions aid compliance with PSD2
- Full spectrum of behavioral biometrics

Challenges

- Multiple licensing options may be perceived as complex
- Synthetic fraud detection would be improved by inclusion of identity proofing functions
- External credential intel not available
- Support for additional API authentication methods needed
- No ITSM integration

Leader in




IBM
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.9 ID Dataweb

ID Dataweb was founded in 2011 and is headquartered in Virginia. ID Dataweb is a late-stage startup that was initially backed by venture capital. AXN was originally designed to gather authoritative attributes for ID proofing for both government and commercial applications, but the solution now covers all aspects of fraud reduction. AXN also facilitates AML, KYC, LEI, OFAC, PEP, PSD2, and 3DS2.0 compliance. The solution is SaaS-based and is hosted in AWS. Licensing is a combination of number of active users and per-transaction fees, depending on the type of attribute services requested.

AXN offers comprehensive identity proofing services, integrating multiple government and private sector attribute sources and providing remote document verification with facial recognition. AXN solves many ID proofing use cases ranging from employment verification, supply chain management, medical license verification, student status validation, and criminal watchlist checks. ID Dataweb has a secure mobile SDK which leverages the Android TEE for building additional mobile ID proofing apps. AXN uses in-network credential intelligence, plus feeds from iovation and ThreatMetrix. AXN performs rules-based UBA without ML, but evaluates the continuum of user and transaction characteristics.

AXN's device intel capabilities span all major data types including device health assessments, malware detection, root detection, device fingerprinting, and IMEI/SIM data from MNOs. These features aid in PSD2 and 3DS2.x compliance and SIM swap detection. ID Dataweb has call center integration which can map calls with web sessions using their Mobile Match technology. Behavioral biometrics, delivered via the SDK and/or JavaScript, include keyboard/mouse, swipe/touchscreen, and gyroscopic analysis. Behavioral biometrics capacitate bot detection and management, including options for challenging, throttling, and redirecting bots.

AXN facilitates orchestration of identity attributes and risk factors for analysis. The admin interface allows policy authors to choose among multiple templates, select attributes per template, and set attribute values as thresholds for actions. Approve, Obligation, and Deny are the decision types rendered. The Obligation model allows organizations to customize resulting actions and reason codes as needed. AXN evaluation results are communicated via APIs, which can be authenticated and authorized via JWT, OAuth2, OIDC, and SAML; API gateways at the service level allow rate limiting, DDoS, and web attack protection. AXN can send event data to SIEMs over syslog.

AXN is ISO 27001 certified but has not yet gone for CSA or SOC 2. Given the architecture, the service should scale as needed. ID Dataweb is a smaller vendor but is trusted by some large global customers and is using self-funding for responsible growth. AXN offers one of the highest uptime SLAs among FRIP solutions. ID Dataweb has focused on integrating identity and transaction data sources to build one of the most comprehensive ID proofing services. The AXN service is feature-rich in the other areas of FRIP and is highly innovative. ID Dataweb is pursuing a path of responsible growth. Any organization, whether public or private sector, that needs excellent identity vetting and fraud reduction capabilities should put ID Dataweb on their consideration list for RFPs.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

iddataweb

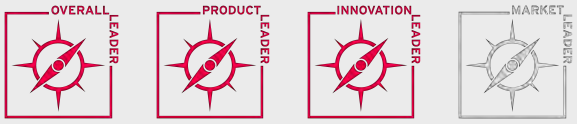
Strengths

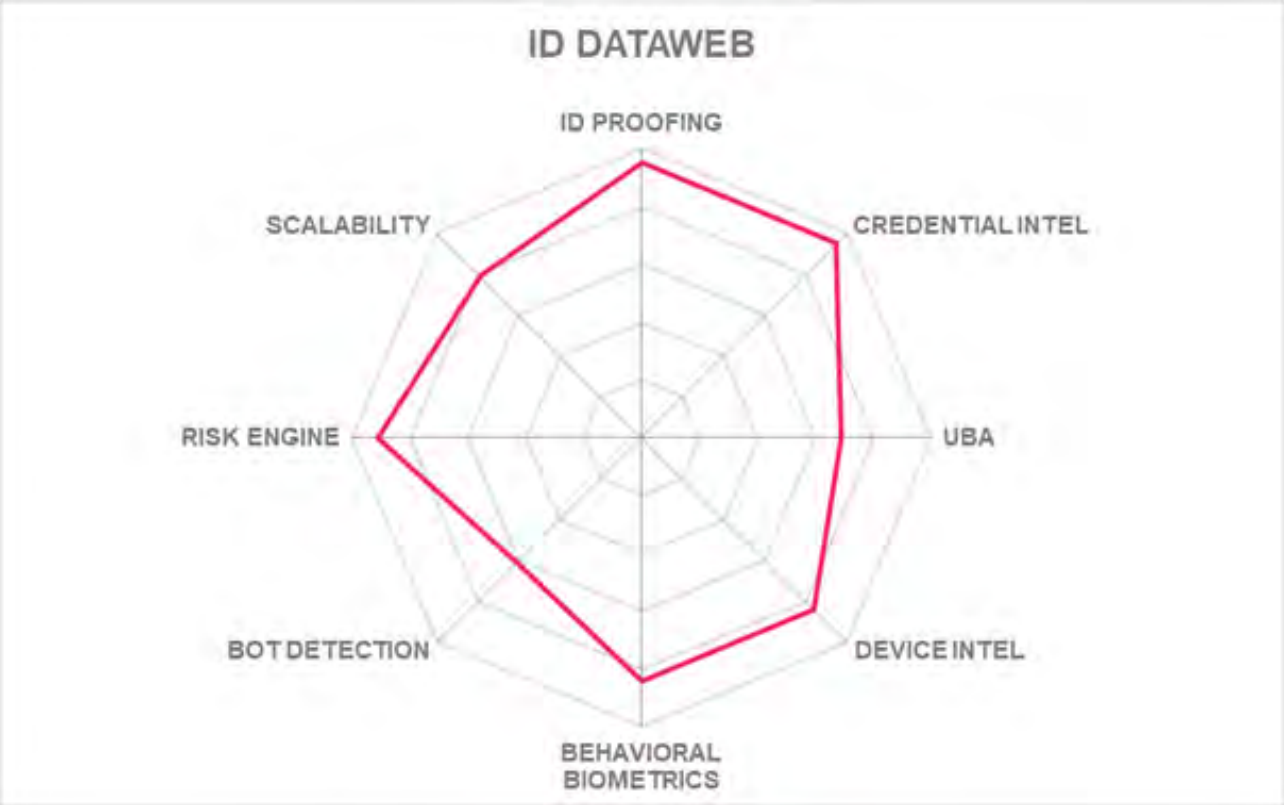
- Extensive ID proofing capabilities, including remote document verification
- Support for AML, KYC, LEI, OFAC, PEP, PSD2, and 3DS2.0
- Intuitive policy authoring interface allows selection of attributes from many ID proofing templates
- Advanced bot management
- Secure mobile SDK uses TEE
- Call center integration
- High uptime SLA

Challenges

- Small but growing service provider, mostly centered on NA market currently
- Default data storage periods should be longer
- UBA could be further enhanced by ML detection models

Leader in




ID DATAWEB
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.10 Kaspersky

Kaspersky has been a global cybersecurity innovator for more than two decades, with products in the endpoint and network security areas. Kaspersky is headquartered in Russia and has transparency centers in Switzerland and Spain. Their Fraud Prevention service includes Advanced Authentication and Automated Fraud Analytics, and contains elements for credential and device intel, UBA, and passive biometrics. Beyond session-based analysis for fraud, KFP aids with AML compliance and advanced bot management. The service is hosted in their own facilities and the public cloud across data centers in EU, NA, and Russia. Private cloud options are also possible. Licensing is per active or registered user per year.

KFP does not have identity proofing built in, but customers can design API callouts to 3rd-party services if desired. Both in-network and external compromised credential intelligence is used. UBA functions include all common attributes.

Device intelligence incorporates the full range of risk factors and is augmented by outside sources of IP and device reputation. Kaspersky has excellent malware detection for fraud use cases, which helps with PSD2 compliance. JavaScript and an SDK enable not only device intel but also passive biometrics, including keyboard/mouse/swipe/touchscreen/gyroscopic analysis as well as network information. Passive biometrics, in conjunction with bot signatures, facilitate bot detection. Granular bot detection capabilities allow customers to customize responses to bot events.

KFP utilizes an assemblage of ML detection algorithms to evaluate user, device, and transaction information. Customers can design their own risk-based policies using the rule constructor in the adjunct product Kaspersky Advanced Authentication to prioritize certain factors. The risk engine is accessible by APIs, but APIs are not rate-limitable or protected by WAFs. The risk engine outputs are coarse-grained, but more detailed rationales can be provided to customers. The three verdicts are permit, deny, and authenticate; detailed reasons, forensic information, and recommended actions can be returned. Basic reports for anomalies and fraud types are available. Analysts can drill into session specifics when needed. Data export to SIEM is supported, but typical API authentication and authorization standards are not supported.

Kaspersky adheres to ISO 27017/27018. Additional certifications such as SOC 2 Type 2 would be advantageous. The solution can scale to meet existing regional customer demands. Kaspersky appears to have made significant progress with its bot detection capabilities, which extends its reach into new industries. Kaspersky develops all their own code: this platform has evolved organically, not by acquisitions or by licensing technology from other companies. Existing Kaspersky customers that are looking for fraud reduction services should give KFP a look.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

kaspersky

Strengths

- Global transparency centers allow customers to review code
- All code developed in-house
- Superior malware detection capabilities for PSD2
- Good implementation of UBA, device intelligence, and behavioral biometrics
- Advanced bot detection for retail, gaming, travel, and other industries

Challenges

- Built-in identity proofing connectors would be helpful for some customers
- Limited ITSM integration
- Additional standard API authentication mechanisms needed
- Large company with global support but few customers for fraud prevention service outside Russia
- Additional cloud security certifications would be useful

Leader in


KASPERSKY
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.11 Neustar

Neustar is a privately held data analytics company based in Reston, VA, offering both risk and marketing analytics services. They were founded in 1998 as a spin-off of Lockheed Martin. They have acquired a number of related companies over the last two decades to become one of the largest risk management service providers in telecommunications and internet services. Neustar Digital Authentication offers ID proofing, UBA, including phone UBA, device intel, and bot detection, and identity anomaly detection. The SaaS is primarily hosted in Neustar owned data centers, though they do also utilize AWS and GCP. Licensing fees are based on numbers of transactions and registered users.

Neustar occupies a unique space in the fraud reduction intelligence supply chain, aggregating user and device information from authoritative sources such as governments, credit bureaus, telecoms, MNOs, and utilities. Neustar performs ongoing identity, IP, location, and device verification services. Neustar leverages in-network and 3rd-party sources of credential intelligence in its risk assessments and is an upstream provider of identity verification services to other vendors in FRIP and IAM. Neustar's UBA capabilities are focused on analysis of login events, correlation of users to devices and email addresses, anonymizer detection, and web visitation patterns. Neustar processes PII but complies with CCPA and GDPR.

Neustar device intelligence features are based on basic fingerprinting, reputations, identity anomaly detection, "identity signs of life", MNO partnerships, and granular geo-spatial information. Evaluation of device intel plus MNO subscriber data allows for SIM swap detection. It does not perform advanced fingerprinting or assess device health. Neustar does not provide a mobile SDK with behavioral biometrics. The solution can detect bots based on IP reputation rather than signature or passive biometry.

Customers can create risk rules in the add-on Decision Navigator, which allows for inclusion of other data sources and risk feeds and custom integration with business applications. Standard decisions are permit, deny, and other. Neustar has separate services that provide call center integration, DNS security, and DDoS protection. Neustar supports OAuth2, OIDC, JWT for REST API authentication.

Neustar's service is SOC 2 Type 2 certified. As a key player in the fraud reduction intelligence supply chain, the service is quite scalable. Neustar offers the best uptime SLA among FRIP service providers. Neustar is centered on the US market but could expand into other areas. Neustar is strongest in the areas of user identity verification, device intelligence, and the triangulation of users/devices/email addresses.

Security	●●●●●
Functionality	●●●○○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●●○

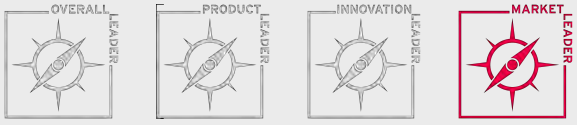
Strengths

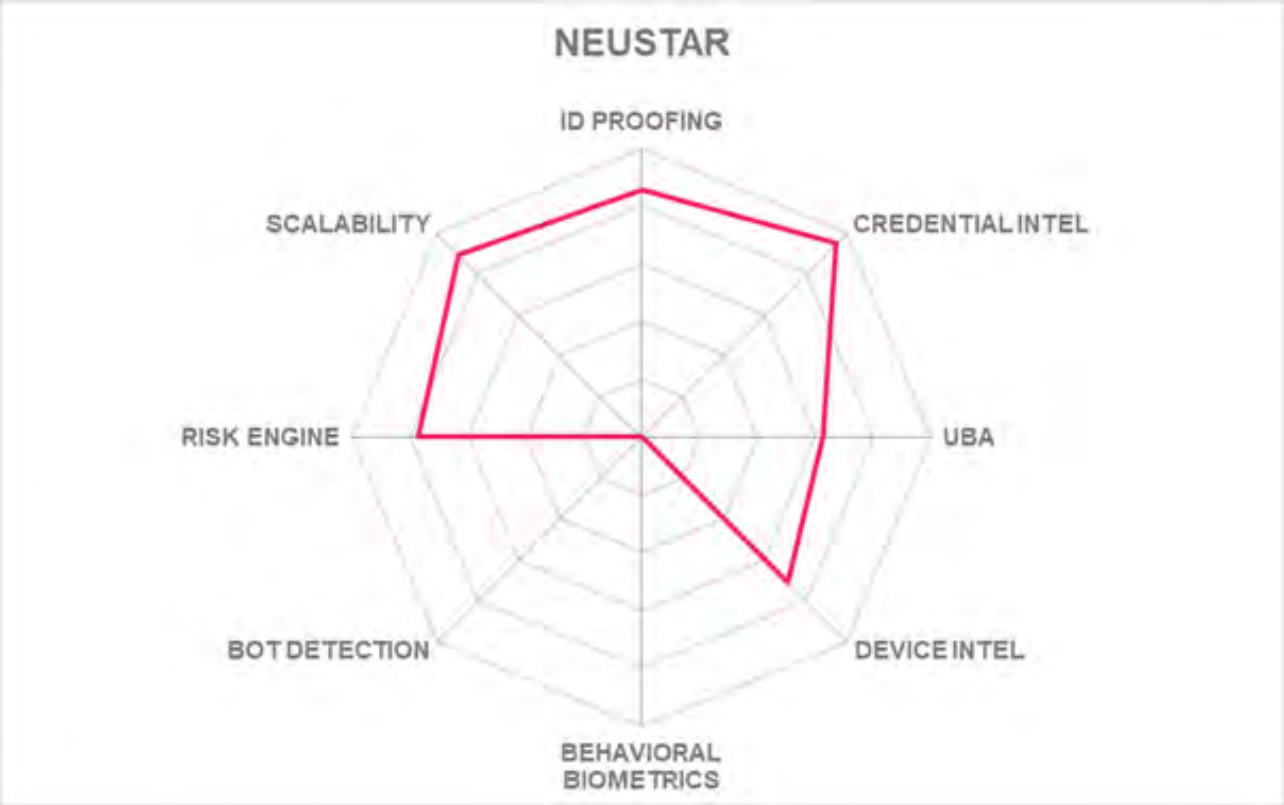
- Robust, ongoing identity verification services
- Partnerships with telecoms and MNOs allow granular device location analysis
- User to device and email address association for real-time risk assessments
- Strong ability to detect synthetic fraud
- Long default data retention period
- Highest uptime SLA
- Fast integration with customer apps

Challenges

- NA market only
- No behavioral biometrics
- Specialized UBA omits some common attributes
- No device health assessment or detailed device fingerprinting
- No OOB integration with security intelligence or ITSM apps

Leader in




NEUSTAR
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.12 OneSpan

OneSpan, formerly VASCO, is headquartered in Chicago, IL, US, and has offices in Brussels, Montreal, and Zurich. VASCO was founded in 1991 and has a history of providing highly effective security solutions, including token-based authenticators, e-signature, and fraud prevention to financial services and enterprise customers. VASCO was well-known for its Digipass® products and has acquired a number of security companies over the years. The services listed above comprise their entry in the FRIP market, which covers all aspects except for credential intelligence. The services are hosted in their own facilities and AWS in data centers in the EU and NA. Licensing is per-session/transaction or also by numbers of active or registered users per year.

OneSpan has a mobile app and SDK that allows customers to configure API-level connections to external identity proofing services and has partners for document and biometrics verification of many national ID credentials. Though OneSpan performs credential verification at registration, OneSpan does not utilize internal or external credential intelligence sources for risk decisions. The Trusted Identity Platform performs thorough UBA, examining >200 data points related to user behavior, profile changes, device, and transaction history. OneSpan employs an innovative matrix of data clustering and unsupervised and supervised ML algorithms for behavioral baselining and anomaly detection/classification.

OneSpan has collects device intel via JavaScript and a secure mobile SDK, which leverages Secure Element and Trusted Execution Environment on Android and Secure Enclave on iOS. Their implementation of device intel analyzes the full range of attributes, including device fingerprinting, health, and IMEI numbers, which help with SIM swap ATO detection. Additional IP reputation information comes from leading 3rd-party intelligence sources. The mobile SDK employs App Shield for protection against overlay malware, debuggers, screen mirroring, code injection, and other threats. Rather than relying on device manufacturer software, their SDK contains its own facial and fingerprint recognition code. Moreover, the SDK instantiates the common types of behavioral biometrics for continuous authentication as well as bot detection.

The admin interface is list-driven, and customers can modify and re-order the pre-built rules as needed. Fraud analysts launch investigations from the case management platform and from there can get a holistic view per user across all their devices and events. OneSpan can integrate with call center software and can be configured to link customer calls with their active web sessions. OneSpan can work with customers to tailor risk factor prioritization. The risk engine is API accessible, and decisions can include granular action recommendations, rejection codes, and forensic data. APIs are well-documented with Swagger and easy to modify by developers. The service is protected by WAF but per-customer rate-limiting is not in place. A Splunk connector is available for customers who want to output logs to their security intelligence systems.

OneSpan's services are container-based and scale with client demand. OneSpan attests at CSA Star Level 1, and Level 2 work is in progress. The platform is also SSAE 18 SOC 2 Type 2 certified. The solution runs on ISO 27001 certified infrastructure but the solution itself is not yet certified. Inclusion of identity proofing facilities and compromised credential intelligence would be useful. With specific strengths in UBA and device intelligence, OneSpan's feature set is well-suited for transaction risk analysis for banks and financial

institutions, as well as for integration with other risk-adaptive authentication services and IAM systems.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●○

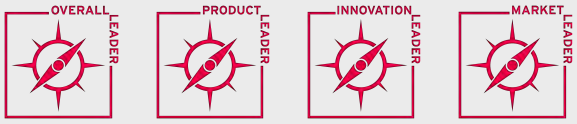
Strengths

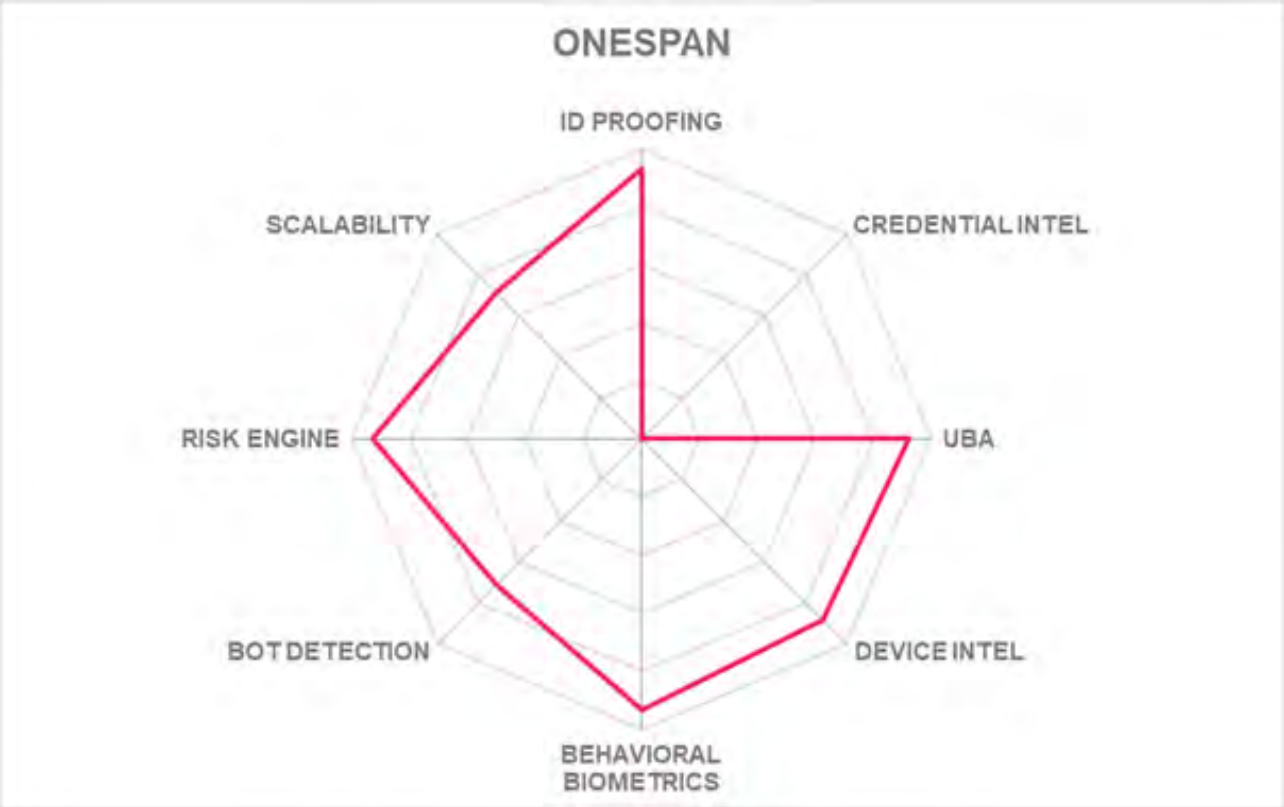
- Detailed UBA with customer configurable data retention periods
- App shielding for maximum device tamper resistance
- Remote identity proofing and document verification app/SDK
- FIDO U2F & 2.0 certified
- Innovative use of ML detection models
- Call center integration includes linking calls to web sessions

Challenges

- Service composed of multiple products
- External compromised credential intelligence not evaluated
- Needs support for additional API authentication methods
- No ITSM integration

Leader in




ONESPAN
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.13 Outseer (RSA)

RSA is a leading global cybersecurity vendor with products for encryption, IAM, IGA, NDR, and compliance monitoring. RSA was acquired by Symphony Technology Group in 2020, and Outseer is the new brand for what used to be their Fraud and Risk Intelligence business unit. Outseer is widely used in the financial sector, protecting over two billion consumers. It covers the functional areas of credential and device intelligence, and customers can create lists to use it for KYC, OFAC, PEP rules. It can be run on-premises on Linux or Windows with various supporting applications; it is also available as SaaS, hosted from their own facilities and Azure in the EU and NA. There are three separate solutions within Outseer (RSA) portfolio: Outseer Fraud Manager; Outseer 3-D Secure, which is Outseer's 3DS ACS solution for credit/debit card issuers; and Outseer FraudAction, their threat intelligence, management, and takedown solution. Licensing options for SaaS versions are per-transaction for on premise by the number of active users.

For identity proofing, Outseer (RSA) does not have built-in features but integrates with LexisNexis. Additional identity proofing integrations can be achieved via Outseer's Multi-Credential Framework APIs. Outseer FraudAction is a primary source of credential intelligence which can be augmented with external feeds. UBA functions include meticulous examination of not only user behavior, but login and transaction history across all channels and with location information.

Outseer collects most expected device intel parameters through its secure mobile SDK, including IP and device history, root detection, device fingerprinting, and IMEI/SIM data where possible, but only limited device health assessments. Outseer eGlobal Data Network, a global repository of data that shares intel across geographic regions, industries, and customers supplements device intel for risk decisions. Limited behavioral biometrics are harvested via JavaScript on browsers but covers only keyboard/mouse analysis and network information. Customers can choose 3rd-party behavioral biometrics and telemetry can be considered by the Outseer risk engine. Bot detection is limited to analysis of cyber threat intelligence.

The policy authoring interface is drop-down style with granular selections available. Rules can be ordered according to customer priority. The primary dashboard shows attack trends, current activities, takedowns, trojan families detected, threat activities by industry, and high-level forensic findings (mule accounts, ATOs, phishing kits, etc.). The analytics dashboard shows fraud rates vs. intervention/prevention rates, case management, transaction volumes and values, and per-customer savings and losses. Outseer (RSA) can obtain risk information from customer call centers but offers no integration with call center solutions. Customers can create and modify their risk analysis policies and choose to include other data sources for evaluation. The risk engine is accessible by API, and verdict classifications are allow, deny, review, and step-up. Reason codes can be defined by customers. API authentication options are limited to SAML and SOAP. The service is protected at the application layer by WAF and against DDoS. Outseer (RSA) can output to external security intelligence solutions via APIs and syslog or by sFTP-ing raw data in CSV format.

Outseer Fraud Manager (Cloud) is SOC 2 Type 2 compliant, and the eCommerce solution is SOC 2 Type 2, PCI-DSS, and PCI-3DS compliant. UBA features are well-suited for safeguarding financial transactions. The

omissions in the areas of behavioral biometrics and device health evaluation should be addressed, either by building capabilities or partnering with specialists. As a large provider trusted by many in the financial industry, Outseer (RSA) solutions are proven to scale well. Enterprises that are looking for configurable and extensible fraud risk engines, but that have other sources for behavioral biometrics and device health, will want to look at Outseer's (RSA) portfolio.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●○○

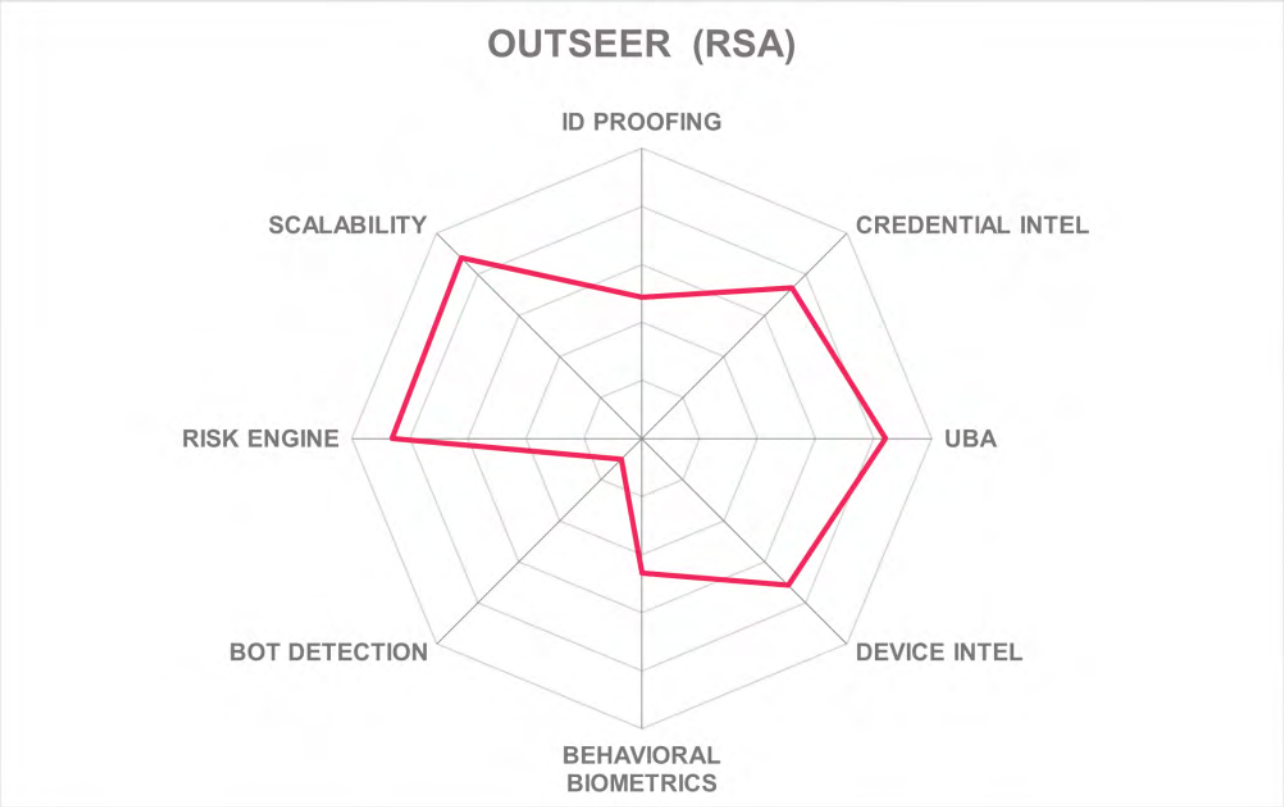
Strengths

- Informed by Outseer Fraud Action intelligence with threat management and fraudster takedown capabilities
- Cross-channel UBA considers broad range of attributes
- Secure mobile SDK uses SE/TEE on Android
- Support for 3DS and PSD2

Challenges

- Limited device health assessments
- Behavioral biometrics lack the ability to examine several key parameters
- Limited bot detection
- Additional identity proofing services require Outseer Multi-Credential Framework
- Potentially long deployment times

Leader in


OUTSEER (RSA)
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.14 ThreatMark

ThreatMark was founded in 2015 and is headquartered in Brno, Czechia. The company is in growing startup mode and focused on reducing banking and payments fraud. The solution addresses PSD2 compliance, ATO and AO prevention, transaction analysis, and malware and bot detection. ThreatMark has a dedicated SOC and fraud intelligence team to help customers manage incidents. Their SaaS is hosted in their own facilities and in AWS in the EU region. The solution can also be run on-premises or in customers' preferred IaaS providers. Licensing is by numbers of active users over the variable contract terms.

ThreatMark does not perform direct identity proofing and does not support remote document verification. AFS uses credential intelligence from across its customers but doesn't ingest 3rd-party credential intelligence. Data retention periods are definable per customer, allowing AFS to examine large sets of user history and transaction details if requested.

ThreatMark uses JavaScript and an SDK for device intelligence and behavioral biometrics. It can pull a wide range of attributes to create high resolution device fingerprints, including examination of data points not commonly considered by other solutions. AFS performs device health assessments, allowing it to detect MITM and overlay attacks. AFS analyzes all the expected behavioral biometrics such as keyboard/mouse usage, gyroscopic data, Wi-Fi connections, mobile network info, etc. Behavioral biometrics permits AFS to decide if activities are human vs. bots, but advanced bot detection and management are not available. The combination of behavioral profiling, device intel, and IMEI evaluation enables SIM swap detection.

ThreatMark uses a combination of ML detection algorithms in its API-accessible risk engine. Customers can use the flowchart style policy building interface to define risk factors, priorities, and output actions. The dashboard is a common starting point for managers and analysts. The analyst interface features a timeline per transaction view that enables step-by-step lookups and makes investigations more intuitive. Reports cover fraud types and trends and others can be designed as needed. OIDC is supported for interoperability with authentication systems. API interaction can be throttled per agreement, and JWT and OpenID are supported for API authentication. Syslog can be used to send info SIEMs.

The infrastructure ThreatMark uses has various certifications but the service itself has not yet achieved them independently. As a public SaaS-hosted service, ThreatMark can likely scale as needed. AFS can perform continuous risk assessments encompassing device intelligence, behavioral biometrics, and UBA across sessions. ThreatMark has visually impressive and useful management and analyst interfaces. As a solution it is missing a few features as outlined above that would help it to expand to cover other use cases and geographies. ThreatMark emphasizes the JavaScript and SDK components of their solution as a way to minimize requirements for API integration and thus speed deployments and Time-to-Value. AFS is adaptable, and financial institutions with existing identity proofing integration, device intelligence sources and bot management capabilities may want to consider ThreatMark for its advanced device fingerprinting and behavioral biometrics capabilities.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Deployment	●●●○○

Strengths

- Excellent analyst UI
- Graphical policy builder in flowchart style
- Detailed device fingerprinting
- Strong session-level malware detection functions
- Good implementation of behavioral biometrics
- Multi-faceted approach to SIM swap detection

Challenges

- Small company that is currently most active in EU and Turkey, but expanding
- No connectors for identity proofing
- Compromised credential intelligence limited to in-network sources
- Bot detection could be enhanced


THREATMARK
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

5.15 Transmit Security

Transmit Security was founded in 2014 and is headquartered in Tel Aviv and Boston. The company is self-funded. Their FRIP platform covers all areas except bot management. Its software can run on-premises, but they host SaaS in AWS, Azure, and GCP across globally distributed data centers. Transmit addresses AO and ATO fraud and facilitates compliance with 3DS 2.0, KYC, and PSD2. Licensing is per-user over variable time periods and/or per-transaction.

Transmit Security's SDK and app support facial recognition with liveness detection, ID document scanning, and ID document verification against identity proofing services such as Equifax, LexisNexis, Payfone, and others. FlexID allows customers to integrate compromised credential intelligence sources via API calls and consider those results in risk decisions. Transmit's UBA functions monitor hundreds of user and transaction details such as amounts, payees, frequency, locations, etc. ML is used for anomaly detection. Data retention periods are set by customers.

Transmit can collect a good range of device intel parameters via their SDK. Device health assessment is limited to obtaining OS patch levels. Malware detection requires outside services. IP reputation information can be enhanced by 3rd-party sources at customer discretion. The SDK provides access to the standard behavioral biometric attributes. Basic bot detection is possible due to behavioral biometrics, plus FlexID allows customers to integrate with more advanced bot detection and management solutions. Interoperability with BioCatch is available OOB.

FlexID's risk engine is configured through the Journey Editor policy builder. It features an innovative, flowchart style interface. Data sources can be plumbed in easily and risk engine output can be sent over APIs that can be secured using JWT, OAuth2, OIDC, and SAML authentication. Transmit enables customers to set multiple actions based on risk scores and to define evaluation result codes and equivalences among MFA methods. FlexID supports call center integration with Genesys, Nuance, and Pindrop, allowing call-to-web session mapping. APIs are protected against attacks and can be rate-limited. Connections to SIEMs are possible over syslog.

Transmit Security's platform processes over a billion transactions daily for their customers worldwide. The service is SOC 2 Type 2 certified. The solution could be enhanced by employing additional ML detection models. FlexID's implementation of UBA, its Journey Editor interface, and the flexibility of configuring multiple intelligence sources and output destinations makes it a leading FRIP solution that should be considered in RFPs across banking, insurance, retail, and other industries.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

transmit security

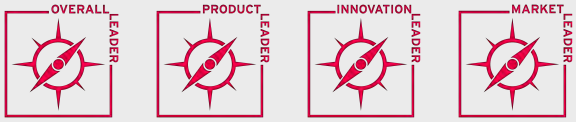
Strengths

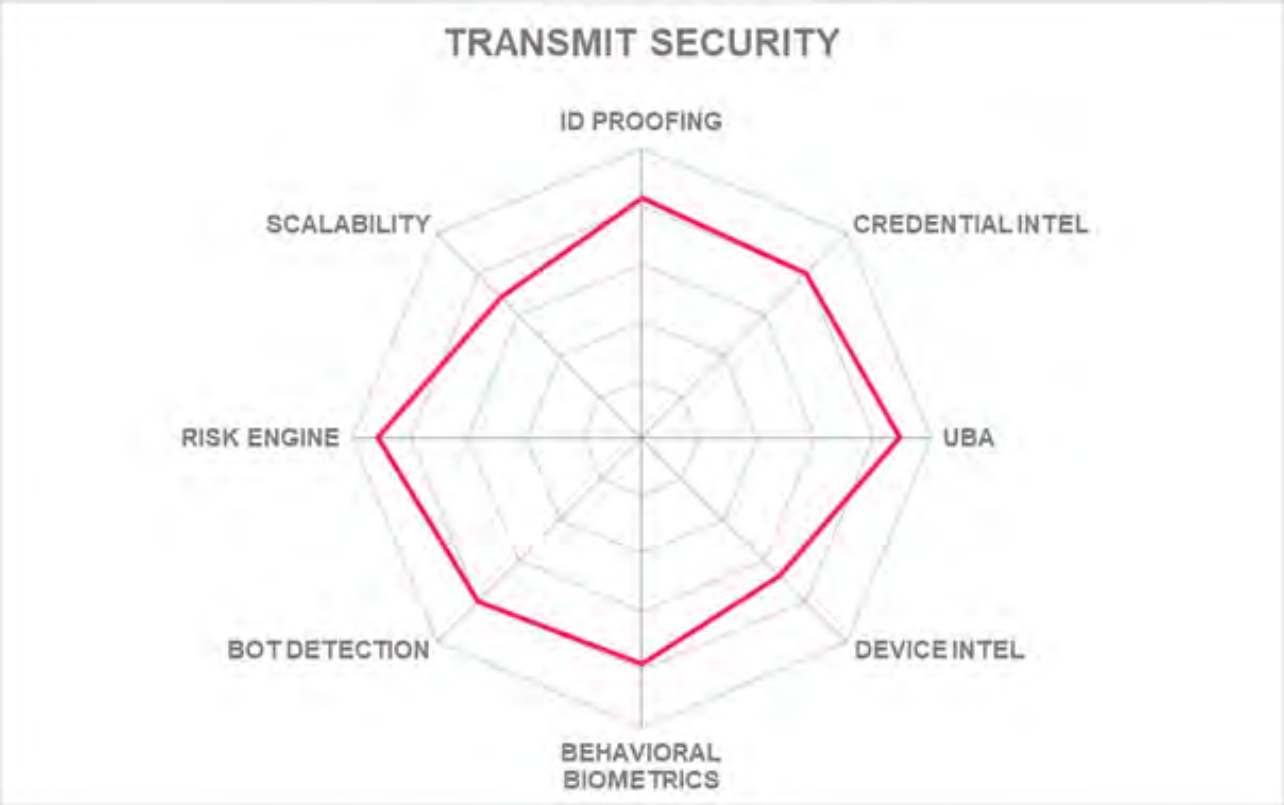
- Easy-to-use Journey Editor, the flowchart driven policy builder interface
- App/SDK for ID proofing integrations and device intel
- Credential intelligence feeds can be configured
- Exhaustive UBA and transactional risk analysis
- Call center integration enables call-to-web session mapping
- Rapid deployment and integration
- High uptime SLA

Challenges

- Device health checks are limited; malware detection requires 3rd-party services
- Additional ML detection models could be deployed
- Credential intelligence could be built-in by default
- Bot detection could be expanded

Leader in




TRANSMIT SECURITY
ID PROOFING
CREDENTIAL INTEL
UBA
DEVICE INTEL
BEHAVIORAL BIOMETRICS
BOT DETECTION
RISK ENGINE
SCALABILITY

6 Vendors to Watch

Beyond the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the market segment of FRIP or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

6.1 Acuant

Acuant was founded in 1999 and is headquartered in the Los Angeles area. Acuant offers identity proofing services, including biometric matching against authoritative identity providers. Acuant also facilitates AML, KYC, OFAC, and PEP compliance.

Why worth watching: Acuant has made acquisitions to expand their FRIP capabilities. Several FRIP vendors are customers of their identity validation services.

6.2 Buguroo

Buguroo was founded in 2010 in Madrid. The company is focused on behavioral biometrics for fraud reduction Their SaaS solution has strong features in device intelligence and user behavioral analysis as well. It can perform bot detection but does not offer bot management or ID proofing extensions. Buguroo was covered in the previous edition of the Leadership Compass on Fraud Reduction Intelligence Platforms, but the company was not able to respond in time for this report.

Why worth watching: Buguroo is comparatively small but actively growing, especially in the under-served LatAm market.

6.3 Deduce

Deduce is a relatively young startup in the FRIP space, founded in 2019 and headquartered in New York. They leverage experience from creating large scale bot and ATO detection solutions for the event ticketing

markets. Deduce utilizes large data sets and proprietary ML algorithms in their risk analysis engine, and outputs decisions for customers to process within their own applications. Deduce covers elements of device intelligence, credential intelligence, user behavioral analysis, behavioral biometrics and bot management. They do not integrate with identity proofing and vetting services at present. The service is API-driven, and customers can configure Webhooks to share signals with other IAM and security applications in their environments.

Why worth watching: Deduce is focused on transaction analysis speed and efficiency. Though they process high volumes of data, they do not retain PII within their systems so as to facilitate compliance with privacy regulations. Their alerting product can render decisions about impossible travel and quickly disseminate that status to downstream applications.

6.4 Forter

Forter was founded in 2013 in Tel Aviv. Forter declined to participate fully in this report, but KuppingerCole will monitor Forter and include them in future research.

Why worth watching: They specialize in various types of fraud prevention, including payments fraud, phone fraud, ATO protection, new account fraud prevention, inventory depletion protection, and others. They also have transaction decisioning services and PSD2 solutions. They offer chargeback guarantees, assuming liability for their decisioning service on behalf of their customers. Forter publishes a Fraud Attack Index annually, which summarizes their findings on attack trends.

6.5 Guardian Analytics

Guardian Analytics was founded in 2005 in the Bay Area. Fraud Cockpit & Business Intelligence and Fraud Detection Analytics & Intelligence are their relevant services.

Why worth watching: Guardian Analytics is mainly focused on providing fraud reduction intelligence services to banks, payment services, transaction clearing houses, and other types of financial firms.

6.6 Ravelin

Ravelin is a mid-stage startup that was founded in 2015 in the UK. They provide payments fraud detection and prevention for clients in delivery services and retail. In addition to payments fraud, they also offer ATO, authentication, and promotional abuse detection and prevention.

Why worth watching: Their solution uses customized ML detection models tailored for each client. Ravelin covers not only customer fraud, but also supply-side fraud detection and prevention. With the rapid expansion of delivery services and online ordering, this segment of the fraud reduction intelligence market is likely to grow.

6.7 ThreatMetrix, a LexisNexis Risk Solutions Company

ThreatMetrix is a global fraud, identity and authentication company, helping customers deliver a unified and secure experience across their digital customer journeys. ThreatMetrix draws upon multiple sources of user and contextual information to produce accurate confidence, risk, and trust scores. Thus, ThreatMetrix offers FRIP services covering identity proofing, credential and device intelligence, and bot detection and management. ThreatMetrix outputs both risk and trust score decisions.

Why worth watching: ThreatMetrix is a highly scalable solution, and an intelligence source / supply chain component to many other FRIP service vendors as well as IAM and authentication service providers. KuppingerCole has reported on ThreatMetrix in the past and will continue to include their service evaluations when information is available.

6.8 TransUnion

TransUnion IDVision is a Fraud Reduction service, which leverages iovation, their Portland, OR based subsidiary launched in 2004. IDVision has FRIP functionality in the areas of ID proofing, device intel, and bot detection. TransUnion reports they block more than one million fraud attempts daily. The SaaS solution is ISO 27001 and SOC 2 Type 2 compliant.

Why worth watching: TransUnion is one of the “Big Three” credit rating agencies with broad scope for authoritative attributes. TransUnion services are utilized by other FRIP service providers. TransUnion was covered in the previous edition of this report but was unable to participate in the update.

7 Related Research

Leadership Compass: Fraud Reduction Intelligence Platforms - 80127
Leadership Compass: CIAM Platforms – 79059
Leadership Compass: Cloud-based MFA Solutions – 70967
Leadership Compass: Adaptive Authentication - 79011
Executive View: BioCatch – 80415
Executive View: ThreatMetrix Digital Identity Network - 79049
Whitepaper: OneSpan Intelligent Adaptive Authentication - 80026

Methodology

About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders in that market segment. It is the compass which assists you in identifying the vendors and products/services in a market segment which you should consider for product decisions.

It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

Types of Leadership

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what we expect from products in that market segment. They are mature.
- **Market Leaders**: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders**: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders**: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.

For every leadership type, we distinguish between three levels of products:

- **Leaders**: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.
- **Challengers**: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers**: This group contains products which lag behind in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even the best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in a given market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, as well as other sources.

Product rating

KuppingerCole as an analyst company regularly conducts evaluations of products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- **Security**
- **Functionality**
- **Integration**
- **Interoperability**
- **Usability**

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are

understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration – integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability – interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs.

Usability – accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.

- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product security, functionality, integration, interoperability, and usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

Vendor rating

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are:

- **Innovativeness**
- **Market position**
- **Financial strength**
- **Ecosystem**

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position – measures the position the vendor has in the market or the relevant market segments. This is an average rating overall markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength – even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to become an acquisition target, with massive risks for the execution of the vendor's roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor

Rating scale for products and vendors

For vendors and product feature areas, we use – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

Strong positive
Outstanding support for the feature area, e.g. product functionality, or outstanding position of the company, e.g. for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. for market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral
Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Denial of participation:** Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.
- **Lack of information supply**: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview of vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.