KuppingerCole Report

LEADERSHIP COMPASS

By John Tolbert | March 19, 2020

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 $2 trillion globally in 2019 and will rise to $6 trillion by 2021. 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, 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 diversify their Tactics, Techniques, and Procedures (TTPs).

Online fraud comes in several major forms:

- Account Takeover (ATO) - most often occur when fraudsters use breached passwords and credential stuffing attacks to execute unauthorized transactions
- New Account Fraud (NAF) - sometimes called Synthetic Fraud, can be more difficult to detect and have advantages for attackers. This type involves gathering 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 launch attacks and/or are used as mule accounts to move money around
- 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

One of the chief mitigations against these types of fraud is risk-based multi-factor authentication (MFA). Strong authentication or MFA can eliminate a substantial portion of ATOs by increasing authentication assurance levels. Risk-based MFA often includes mechanisms to increase identity assurance, such as identity proofing, user behavioral analytics, and behavioral/passive biometrics. Insider Fraud is handled differently due to the fact that in many cases, the access policy conditions are met because the individual(s) are authorized. Thus, monitoring and user behavioral analysis are key deterrents; and implementing the principles of least privilege and separation of duties are important to limit possible damage by insiders.

Risk-based MFA is characterized by transaction-time evaluation of multiple factors, including information about users, their devices, and the environments from which requests emanate. Risk-based MFA 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

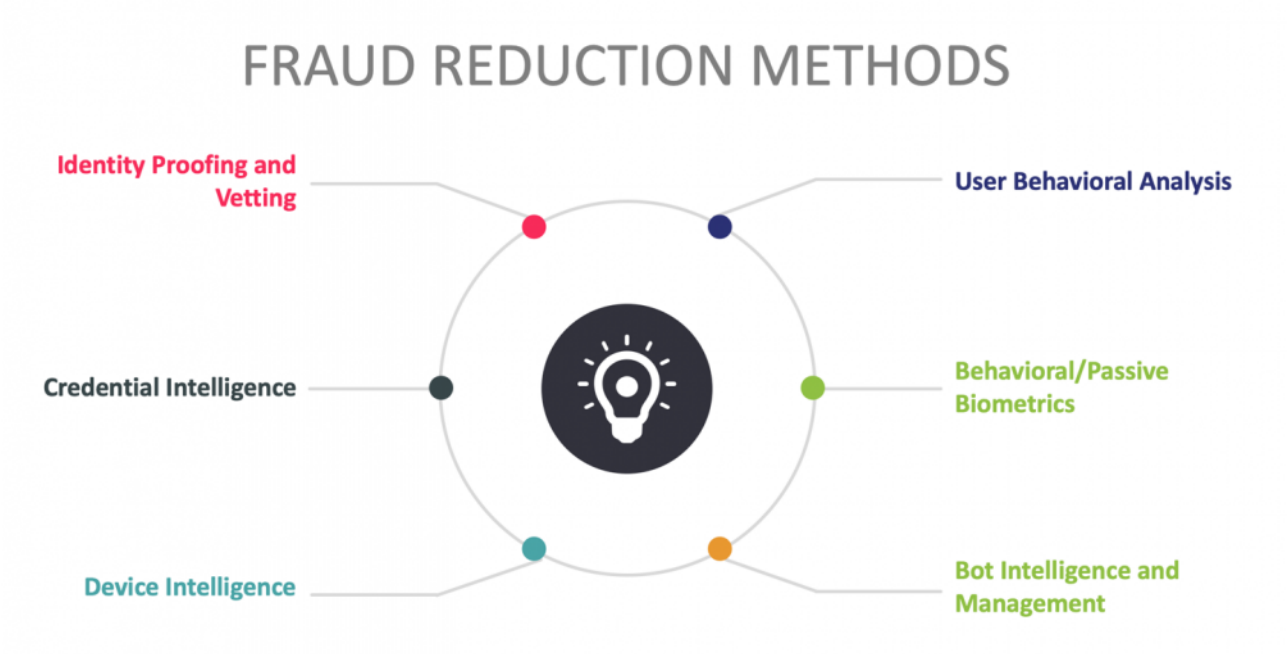


Figure 1: Major Fraud Reduction Methods

FRIP solutions also can interoperate with transaction processing systems, evaluating the context of each transaction request against pre-determined policies (similarly to authentication decisions in risk-based authentication systems) and then outputting risk scores. In these use cases, customers of FRIP solutions usually must write a bit of code to have their transaction processing systems query the FRIP service providers' APIs. For example, a FRIP customer will collect transaction context information and transmit that as part of the API call to the FRIP service. The FRIP solution analyzes the transaction request context, gathers additional intelligence relevant to the user and request in real-time, scores it in accordance with customer-determined policies, then returns the risk score to the calling customer. The customer's transaction processing logic than executes, taking into consideration the risk score from the FRIP service.

1.1 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 Mobile Network Operators (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 found in all FRIP services.

Furthermore, KuppingerCole research indicates that the particular market segments that vendors choose to target often has 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.

1.2 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.

1.3 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, usually validated against government-issued ID credentials
- Credential Intelligence - 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 effectiveness.
- Device Intelligence, which includes device hygiene (OS patch versions, anti-malware client presence, and RAT detection), device history and reputation, location history, IP reputation, MNO carrier information (SIM, IMEI, etc.). 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 Intelligence and Management – evaluation of pertinent cyber threat intelligence on botnet activities, request context behavior, and behavioral biometrics. 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, and ratings in this document reflect that.

Most vendor solutions that utilize these methods employ various Machine Learning (ML) algorithms to process the vast amounts of data required to make accurate risk scores and 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 user activity per user and compare it in real-time to incoming transaction requests; or those which interoperate with 3rd-party sources of user information
- Solutions which can harvest device intelligence in-network and/or consume 3rd-party device intelligence sources
- Solutions which can granularly build policies to evaluate business-relevant environmental attributes
- Solutions which can adequately identify bot-generated activities and present customer administrators with appropriate options for proactively handling these kinds of activities
- Solutions that utilize the above-mentioned types of information and offer customer administrators flexible and automated response actions such as
    - Permit

    - Deny
    - 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
    - Blacklist/whitelist IPs
- Solutions which generate dashboards and reports for customers including the following standard types:
    - Total number of dismiss, detect, case open, case closed, 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 benefits but not absolute functional requirements in this analysis:
    - Geographic and industry-specific compliance regimes and certifications, such as but not limited to AML, GDPR, KYC, OFAC, PCI-DSS, PSD2, etc.
    - OLAs or service guarantees that provide relief to customers in cases where missed fraud detections or false positives decrease customer revenue.

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. We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market. Features that are considered innovative are listed below.

- Support for relevant standards such as OAuth and Global Platform Secure Element (SE) and Trusted Execution Environment (TEE) standards
- A comprehensive and consistent set of REST-based APIs for integrating with customer transaction processing systems
- Browser and mobile app integration capabilities (SDKs).
- Integration with national e-IDs and passports.

Please note that we only listed a sample of features, and we consider other capabilities per solution as well when evaluating and rating the various consumer authentication solutions.

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

Figure 2: The Overall Leadership rating for the FRIP market segment

IBM, Transmit Security, and Gurucul top the chart for Fraud Reduction, with excellent and rich feature sets as well as market positions. Broadcom and RSA are also Leaders, with large customer bases, scalability, and good coverage of functionality.

Arkose Labs, Buguroo, ID Dataweb, Kaspersky, Neustar, NuData Security, and TransUnion are in the Challenger section.

Overall Leaders are (in alphabetical order):

- Broadcom
- Gurucul

- IBM
- RSA
- Transmit Security

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.

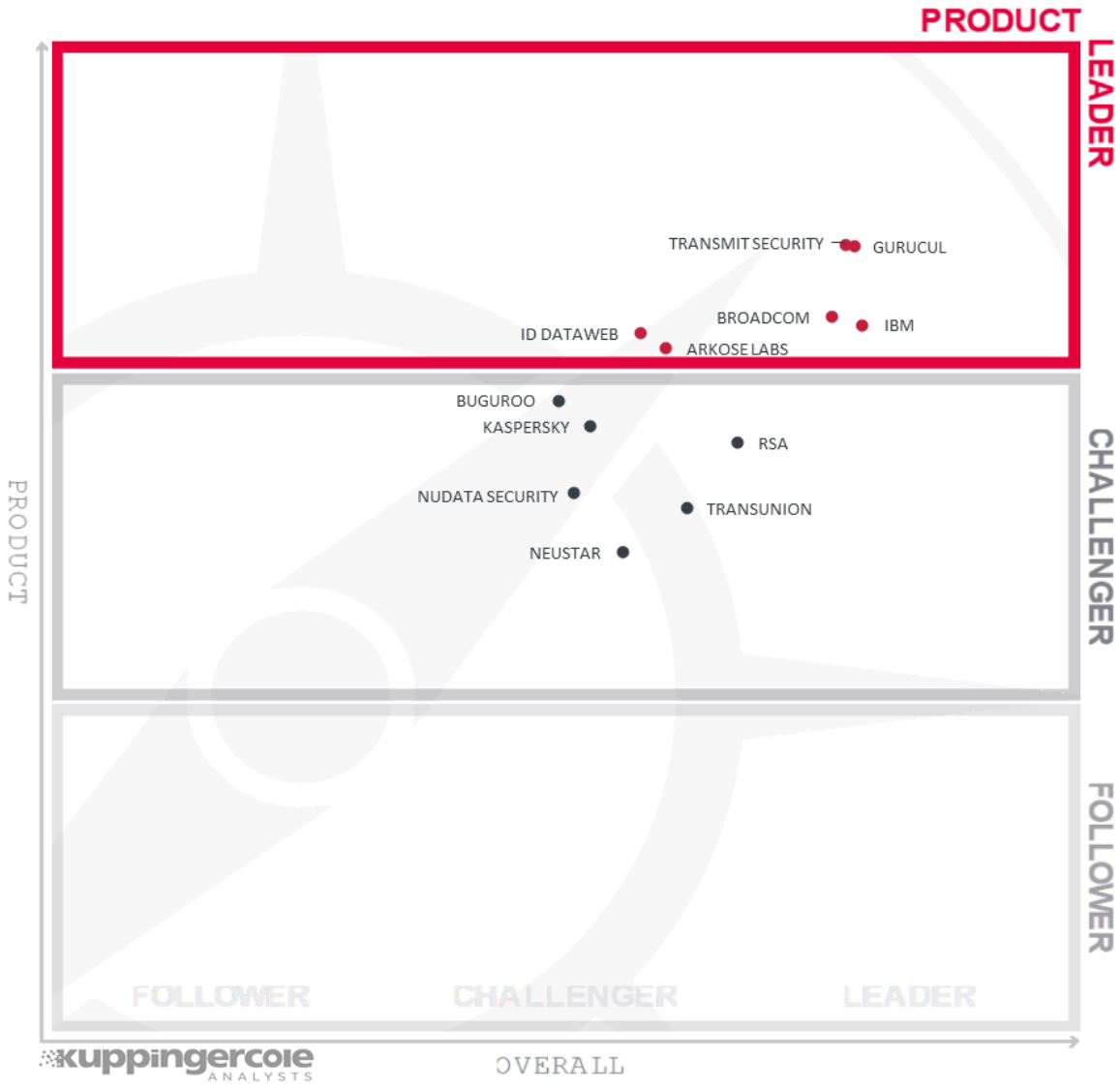


Figure 2: Product Leaders in the FRIP market segment

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

Arkose Labs, Broadcom, Gurucul, ID DataWeb, IBM, and Transmit Security, are the Product Leaders. Each of their products or services represents the strongest alignment to the functional requirements of Fraud Reduction Intelligence Platforms. FRIP is an amalgamation of service categories, and while all vendors surveyed may not provide every feature, these vendor solutions have the best overall combination of functions.

At the top of the Challenger section, we see Buguroo, Kaspersky, and RSA. Each of these solutions is close to the Leader area, meaning that their feature sets are also quite robust, but not quite as complete. Near the center of the Challenger block, Neustar, NuData Security, and TransUnion can be found. These solutions are generally missing several key functions but tend to excel at the functions which they do have in their products.

There are no Followers, indicating that this market segment has, in general, a good mix of mature solutions. It is important to remember that not all organizations need the same kinds of features, so Challengers could in some cases be a better fit than Leaders.

Product Leaders (in alphabetical order):

- Arkose Labs
- Broadcom
- Gurucul
- IBM
- ID DataWeb
- Transmit Security

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.

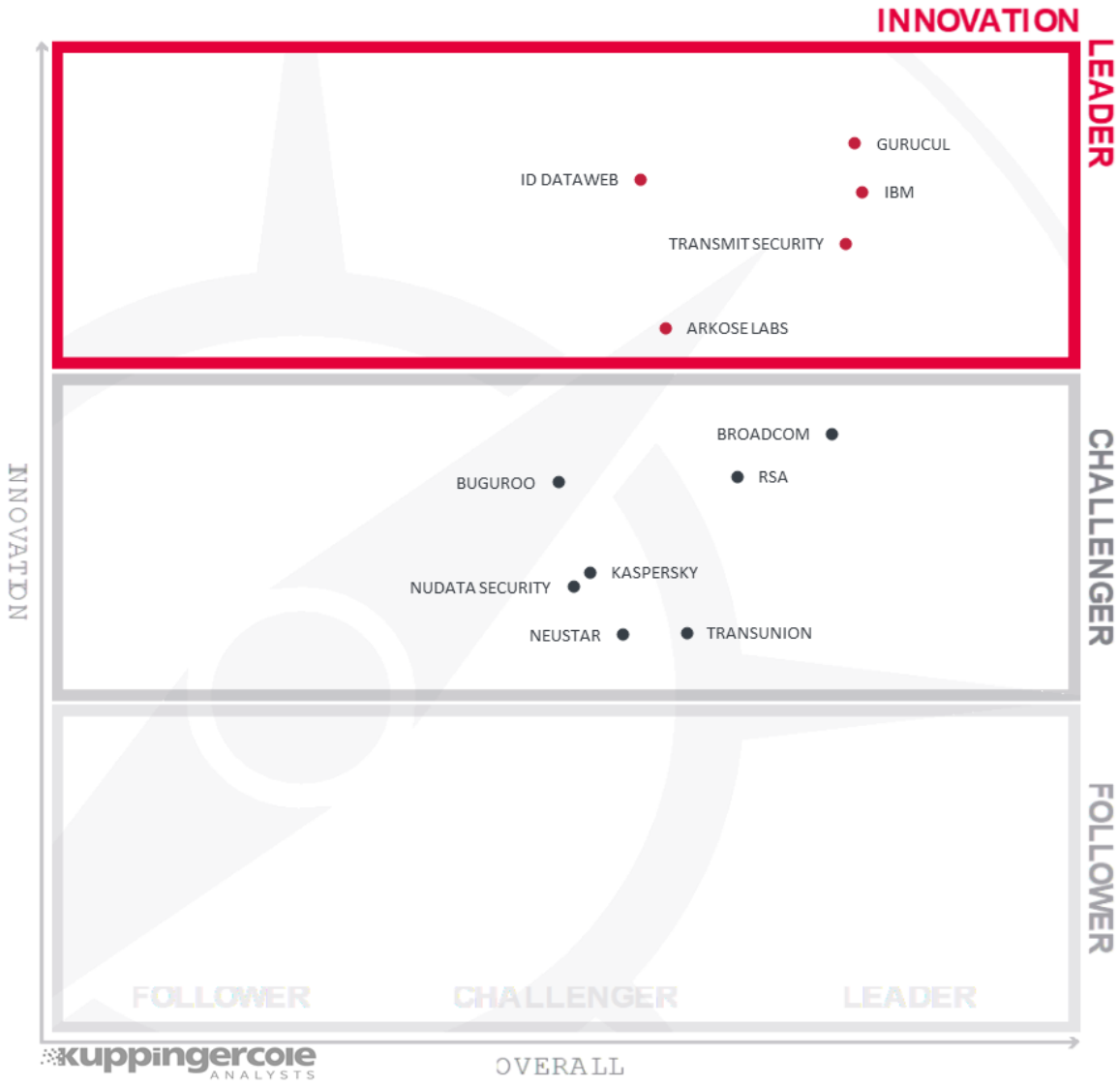


Figure 2: Innovation Leaders in the FRIP market segment

Innovation in FRIP can be interpreted 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. For example, ID proofing, credential intelligence, UBA all contribute to the User Intel rating; however, the ability to provide these different functions is quite challenging. Thus, we see that ID proofing is not provided by all vendors. Moreover, bot management is even further removed technically than the components of User Intel. This is likely why bot management is not incorporated in all FRIP solutions today.

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

device intel; sophisticated and granular risk analytics engines; regulatory compliance features; the ability to consume and process data types that require extra effort; and the effective use of multiple ML algorithms and trained models.

With that in mind, we find Arkose Labs, Gurucul, IBM, ID Dataweb, and Transmit Security as Innovation Leaders. Broadcom, Buguroo, Kaspersky, Neustar, NuData Security, RSA, and TransUnion are spread across the Challenger section. As in Product Leadership, we find no Followers due to the nature of this field, in which at least moderate innovation is required to remain viable.

Innovation Leaders (in alphabetical order):

- Arkose Labs
- IBM
- ID Dataweb
- Gurucul
- Transmit Security

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions 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. Market Leadership, from our point of view, requires global reach.

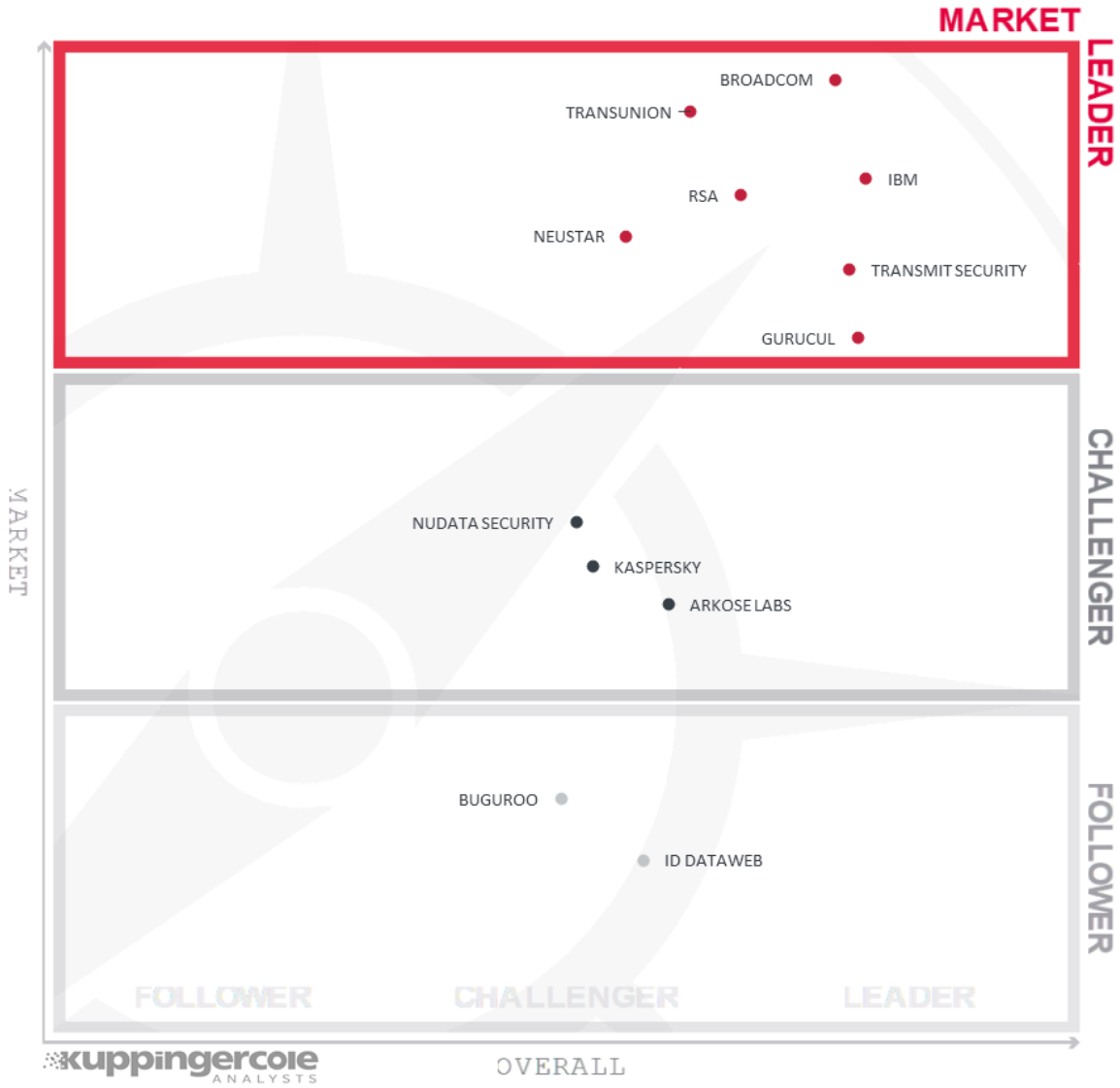


Figure 2: Market Leaders in the FRIP market segment

Broadcom, Gurucul, IBM, Neustar, RSA, Transmit Security, and TransUnion are the Market Leaders for FRIP. It's noteworthy that five of the six Leaders are long-established companies that have been providing elements of fraud reduction solutions for many years, with Transmit Security being the relative newcomer. In the earlier days, most fraud reduction efforts were centered on banking, finance, and payments. But with the proliferation of fraud techniques and targets, solution providers are adding functionality to accommodate other industries and use cases.

Arkose Labs, Kaspersky, and NuData Security are Market Challengers. Arkose Labs is a newer entrant in the market but doing quite well. Kaspersky is pivoting from UBA and cybersecurity respectively to offer FRIP services. NuData Security has specialized in fraud reduction from their

founding.

Likewise, the Market Followers, Buguroo and ID DataWeb are specialists in FRIP.

With the year-over-year increase in fraud attempts, incidents, and complexity, there is plenty of room for growth in this market for all vendors.

Market Leaders (in alphabetical order):

- Broadcom
- Gurucul
- IBM
- Neustar
- RSA
- Transmit Security
- TransUnion

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.

3.1 The Market/Product Matrix

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

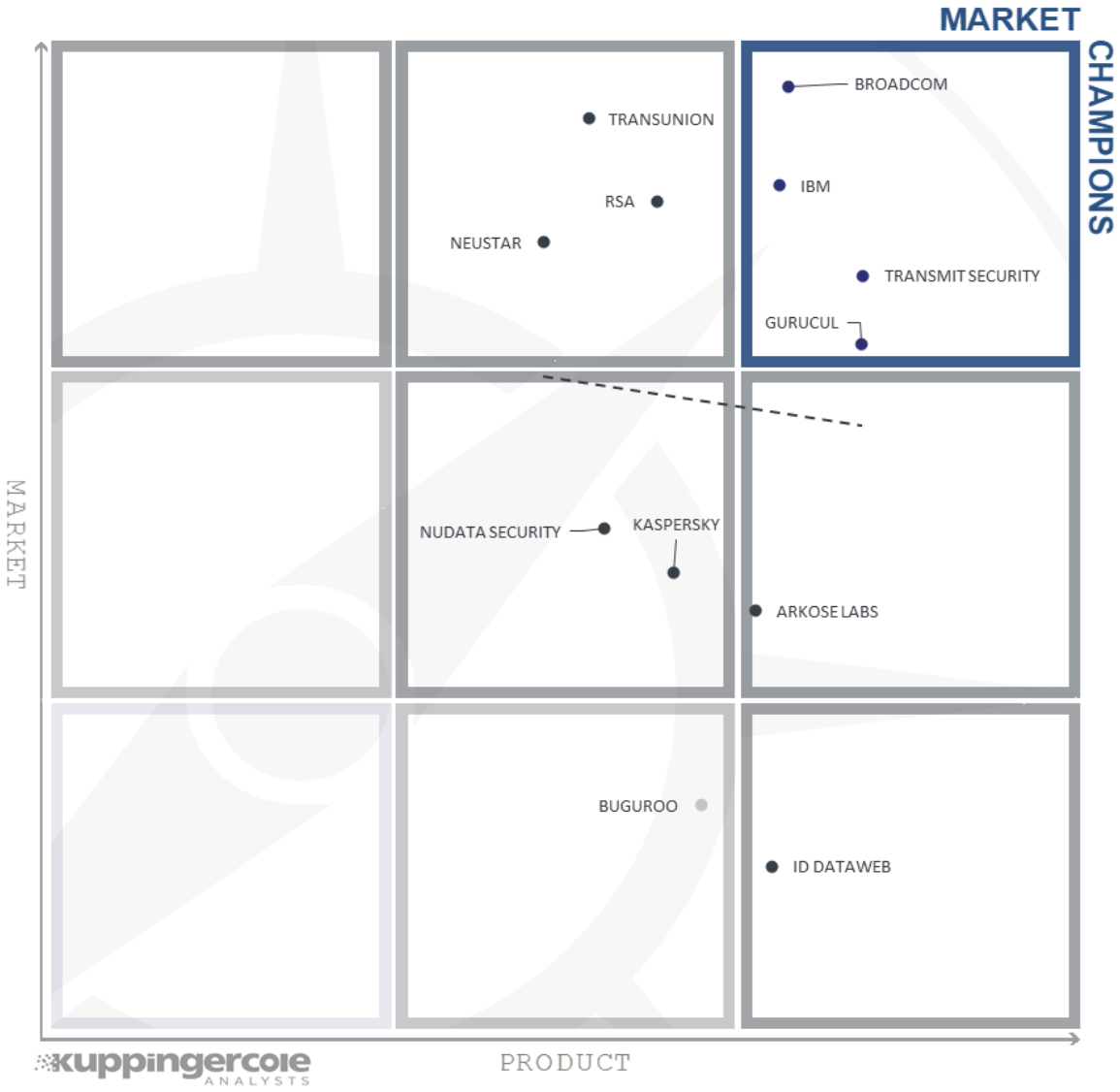


Figure 6: The Market/Product Matrix.

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.

The Market Champions are Broadcom, Gurucul, IBM, and Transmit Security, which are Product Leaders and Market Leaders. Their market shares correlate well to the strength of their products.

Just to the left in the top center, we see TransUnion, RSA, and Neustar. These four companies are doing well in terms of sales and consumer bases, with products that are somewhat less complete than others. Again, this is due to the lack of coverage in some functional areas of FRIP, and in order to be in this section, the products are still fairly strong.

Arkose Labs is in the right center, indicating less market share than expected given the quality of the product. ID Dataweb is in the bottom right, which shows that it hasn't achieved the market placement one would expect for the comparative value of the product.

Kaspersky and NuData Security occupy the center block below the line. Buguroo is in the bottom center.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

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.

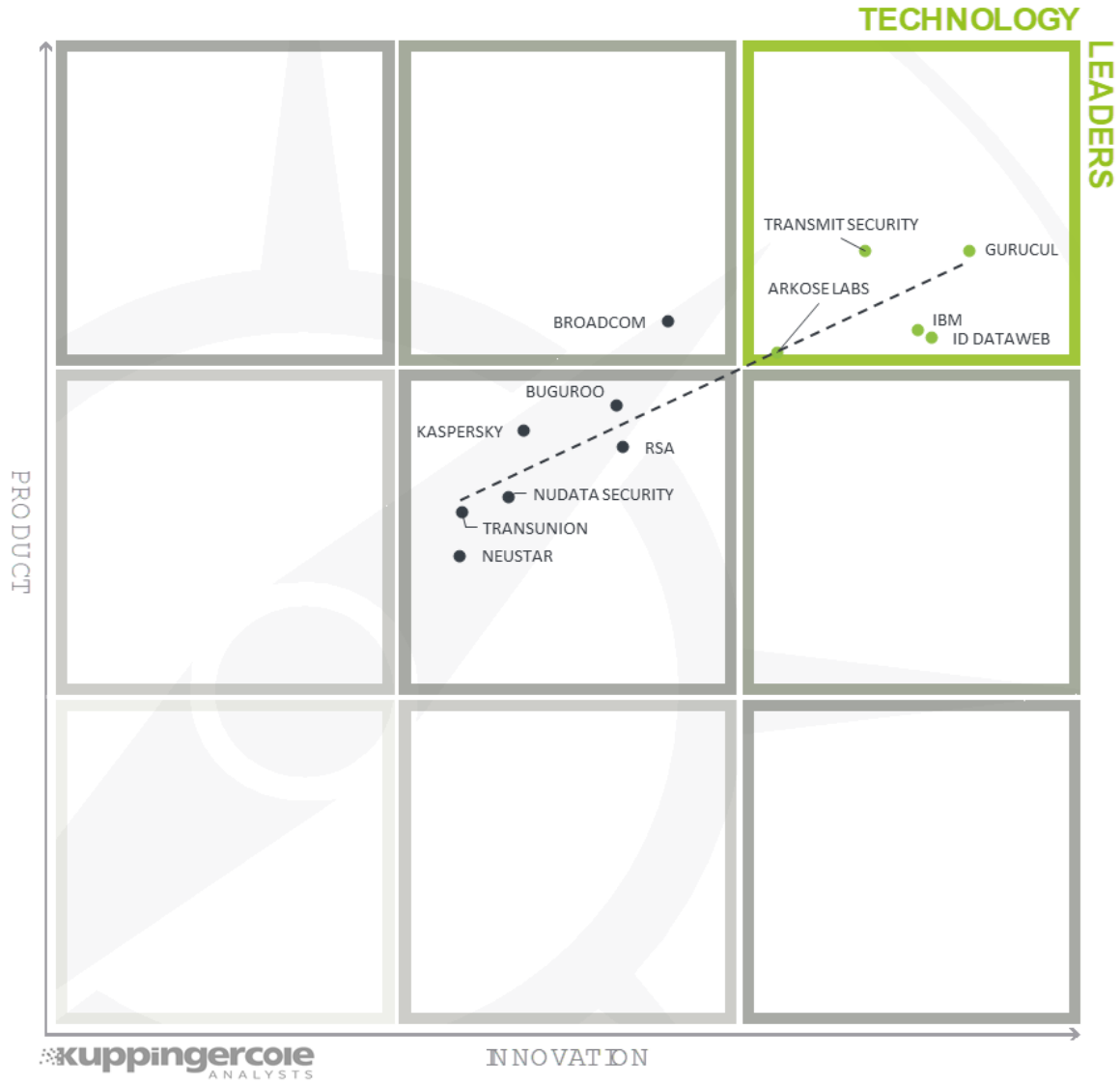


Figure 7: The Product/Innovation Matrix

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

Arkose Labs, Gurucul, IBM, ID DataWeb, and Transmit Security are the Technology Leaders. This placement is logical given that all five companies are both Product Leaders as well as Innovation Leaders.

Broadcom is in the top center; then Buguroo and Kaspersky are in the center box, and all are found above the line. Below the line in the center we have Neustar, NuData Security, RSA, and TransUnion.

The orientation of the line and proximity of almost all vendors to the line presents us several bits of information. The low acute angle of the line demonstrates that there is more variation in quantities of innovation than comparative quality in products. The line originates in the center box, which means the starting point for product completeness is average to above average in this market sector. Lastly, that nearly all vendor solutions are clustered near the line means that product quality and the quantity of innovative functionality are closely connected.

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 are Gurucul, IBM, and Transmit Security, having a strong conjunction between Innovation and Market Leadership. Broadcom, Neustar, RSA, and TransUnion are in the top center. All the vendors at the top of this chart are also Market Leaders; with left to right spacing determined by level of innovation (lower to higher).

Arkose Labs is in the right center and ID DataWeb is in the lower right. Though both are below the line, given their high innovation scores, they will likely capture more market share.

Kaspersky and NuData Security are in the center below the line. Buguroo is in the bottom center. All four vendors are more geographically regionalized, and their market positions may grow depending on their strategy.

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.

4.1 Ratings at a glance

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	Ease of Delivery
Arkose Labs Detect and Enforce	positive	positive	weak	positive	positive
Broadcom Arcot for Digital Banking	strongly positive	positive	strongly positive	positive	strongly positive
Buguroo BugFraud	positive	positive	neutral	positive	positive
Gurucul Fraud Analytics	strongly positive	strongly positive	strongly positive	strongly positive	positive
IBM Security Trusteer	strongly positive	strongly positive	positive	positive	strongly positive
ID Data Web Attribute eXchange Network	positive	strongly positive	strongly positive	strongly positive	neutral
Kaspersky Fraud Prevention	positive	positive	strongly positive	positive	positive
Neustar Digital Identity Risk and Digital Defense & Performance	strongly positive	neutral	positive	positive	positive
NuData Security NuDetect	positive	positive	neutral	positive	positive
RSA Fraud and Risk Intelligence Suite	positive	positive	neutral	positive	neutral
Transmit Security Platform	strongly positive	strongly positive	strongly positive	strongly positive	positive
TransUnion IDVision with iovation	positive	neutral	neutral	positive	positive
Legend		critical	weak	neutral	positive	strongly 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	positive	neutral	weak	weak
Broadcom Inc.	positive	strongly positive	strongly positive	positive
Buguroo	positive	weak	neutral	weak
Gurucul	strongly positive	positive	positive	neutral
IBM	strongly positive	strongly positive	strongly positive	strongly positive
ID Data Web	strongly positive	weak	weak	weak
Kaspersky	positive	neutral	strongly positive	neutral
Neustar	neutral	strongly positive	positive	neutral
NuData Security	positive	positive	strongly positive	weak
RSA Security	positive	strongly positive	strongly positive	strongly positive
Transmit Security	strongly positive	strongly positive	neutral	strongly positive
TransUnion	neutral	strongly positive	strongly positive	strongly positive
Legend	critical	weak	neutral	positive	strongly positive

Table 2 requires some additional explanation regarding the "critical" rating.

In Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, like support for multi-tenancy, shopping cart approaches for requesting access, and others.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets like France or Germany or even within these markets. Usually the number of existing customers is also limited in these cases.

In Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base but is also based on some other criteria. This doesn't imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it's also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no or a very limited ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

5 Product/service 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 six categories:

- User Intel
  This category represents the combination of identity proofing, credential intelligence, and user behavioral analysis as defined in Chapter 1.
- Device Intel
  This category is the combination of both device intelligence and behavioral/passive biometrics as described in Chapter 1.
- Bot Intel
  This category is bot intelligence and management as described in chapter 1.
- 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. This category is titled "Scalability" in the spider charts.
- App integration
  APIs and/or connectors which customers can use to facilitate integration with transaction processing and authentication systems. It also includes SDKs for adding FRIP functionality to websites (often as JavaScript) and SDKs for building mobile apps with secure functionality and the ability to gather device intelligence and environmental attributes for evaluation.
- Analytics 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 in assessing intelligence sources and input.

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 relatively young startup (2017) out of the San Francisco area. Their solution is focused solely on fraud reduction, covering the majority of finance, retail, gaming, etc. use cases. The solution utilizes challenge-response mechanisms to prevent ATO, new account fraud, inventory skimming, auction abuse, fake reviews, and many other kinds of attacks. Arkose Labs has functionality in the areas of bot/cred/device intel, passive biometrics, and UBA. Licensing is per-transaction, and there are fixed cost options available. They do not charge in cases of missed detections. The solution is SaaS-based and is SOC2 Type 2 certified.

Arkose Labs utilizes in-network and 3rd-party credential and device intelligence. Device intel attributes are centered on IP information plus proprietary fingerprinting techniques. The solution uses behavioral analysis to detect malware rather than anti-malware clients. It does not import MNO data such as IMEI numbers and does not perform jailbreak/root detection. Arkose Labs' UBA features cover all the basics with the exception of transaction amount history. The solution has a well-constructed ML implementation for fraud detection.

For passive biometrics, Arkose Labs uses JavaScript for full browser implementations and has a mobile SDK. Attributes evaluated are limited to event timing, keystroke/mouse analysis for computers, and gyroscopic analysis for mobiles. Other biometric modalities and FIDO authentication are not supported. Arkose Labs has excellent bot detection and highly customizable bot management policies. Their challenge-response mechanisms identify and handle single request attacks.

Limited MFA options are available for customer admins. Role/delegated access models are not supported. App integration and security infrastructure interoperability is possible via APIs. JSON format is supported but other relevant standards are not. Customers could potentially extract context information from authentication events and pass via APIs to Arkose Labs for transaction evaluation.

Arkose Labs is a growing startup that has captured some large customers. The solution excels at bot management and has adequate UBA and device intel features. Connections for ID proofing and support for more standards and biometrics would strengthen the offering. Organizations 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	●●●●○
Ease of Delivery	●●●●○

Arkose Labs

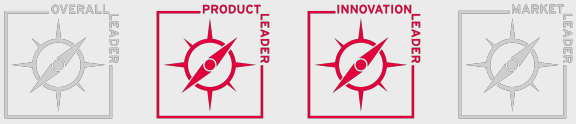
Strengths

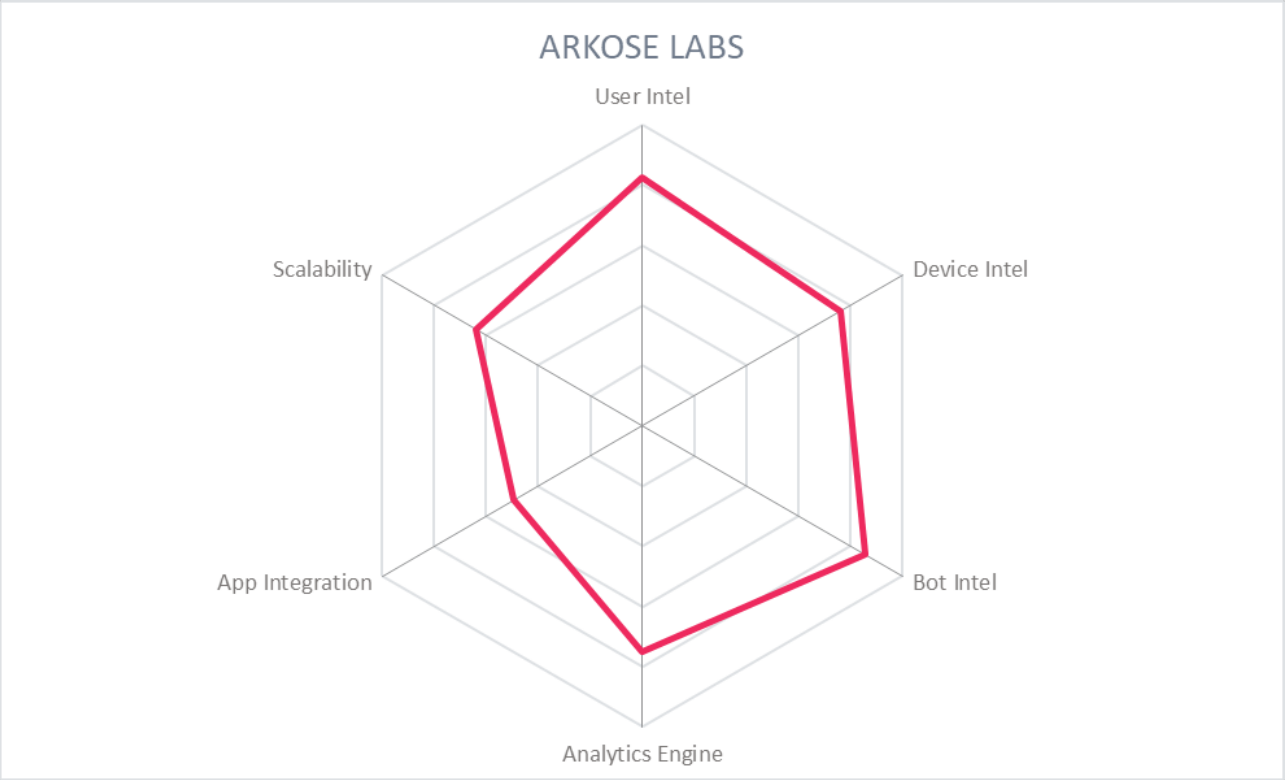
- Innovative use of variety of ML algorithms
- Strong bot intelligence and granular bot management response features
- Can detect single request attacks as well as bots and credential stuffing type attacks
- Sophisticated use of ML technology for fraud detection

Challenges

- No direct or indirect ID proofing
- No device health assessment
- Minimal support for standards

Leader in




ARKOSE LABS
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.2 Broadcom Inc.

Broadcom's entry in this market originated with Arcot Systems, a 3DS pioneer acquired by CA Technologies in 2010. Their solution offerings, Arcot for Issuers, Arcot for Merchants and Arcot for Digital Banking are heavily used by credit card issuers, processors, merchants and banks. Broadcom has functionality in the areas of credential and device intel, passive biometrics, and UBA. The solution is SaaS-based. The platform undergoes independently certified PCI and SASE audits. Broadcom offers licensing packages with unlimited numbers of transactions for large enterprises.

Broadcom utilizes in-network credential intelligence and both in-network and 3rd-party device intelligence. Device intel attributes are centered on IP information plus detailed fingerprinting techniques. The recent acquisition of Symantec brings improvements in their device intelligence features, including device health assessments, root detection, and MNO intelligence. Broadcom's UBA features expertly address the needs of the payment services industry, focusing on user, device, and transaction history.

For passive biometrics, Arcot uses JavaScript for full browser implementations and has a mobile SDK. Attributes evaluated are limited to location and network. Other biometric modalities and FIDO authentication are not supported. Broadcom does not directly perform bot detection. Arcot can sense abnormal, potentially bot-generated activity, and alert on it but does not provide bot management.

Excellent MFA options are available for customer admins. Role/delegated access models are supported. App integration and security infrastructure interoperability is possible via APIs and SOAP. JSON format is supported but other relevant standards are not.

Broadcom is a pioneer in payment services fraud reduction. The Arcot for Digital Banking platform offers customers scalability and support for complex use cases in this area as well as for other industries. The solution has excellent internal platform security. Extending passive biometrics and including support for credential intelligence and bot management would benefit the overall solution. Companies looking for proven FRIP solutions particularly in the payment services sector should review Broadcom Arcot for Digital Banking capabilities.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Ease of Delivery	●●●●●

BROADCOM®

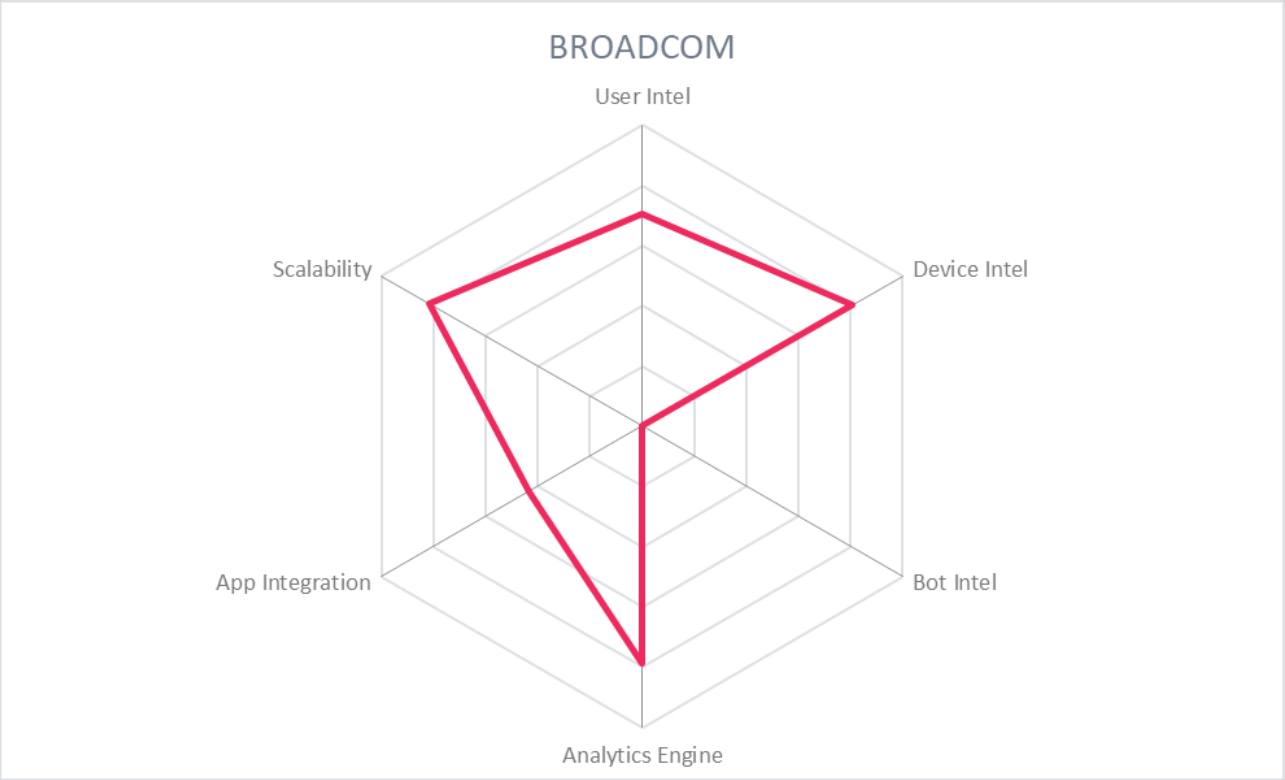
Strengths

- Widely used solution in payments sector
- Support for 3DS 2.0, AML, KYC, OFAC, PSD2, and many industry-specific profiles
- Unlimited transactions licensing plans for enterprise customers
- Good MFA options and access control models for customer admins
- Detailed device fingerprinting techniques

Challenges

- No ID proofing or bot management
- Passive biometrics could be improved with additional analysis methods

Leader in


BROADCOM
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.3 Buguroo

Buguroo was founded in 2010 in Madrid. The company is backed by venture capital and is focused on behavioral biometrics and fraud reduction. They are targeting the LatAm and Southern Europe markets primarily. The solution is SaaS-based, and they are currently pursuing ISO 27001 certification. They offer per-user and flat fee licensing rather than a per-transaction model.

Buguroo uses predominantly in-network credential and device intelligence. Device intel capabilities are comprehensive, including device health assessments, malware detection, root detection, deep fingerprinting, and IMEI/SIM data from MNOs. Buguroo's implementation of UBA covers all expected attributes including transaction habits, with the exception being transaction amounts.

For passive biometrics, BugFraud uses JavaScript for desktops/laptops/mobiles. More than 1,000 individual attributes are measured, including the basics of keystroke/mouse analysis, gyroscopic analysis, swipe and screen pressure analysis, networks, etc. Buguroo can integrate with native mobile biometrics but FIDO is not supported. Buguroo leverages their behavioral biometrics capabilities to perform bot detection, but it does not offer advanced bot management.

2FA options such as OTP are available for customer admins. Role-based access control is supported. App integration and security infrastructure interoperability is possible via APIs. JSON format is supported but other relevant standards are not.

Buguroo is comparatively small but actively growing, especially in the under-served LatAm market. Their solution offers advanced functionality in device intel and passive biometrics. UBA features are adequate, but bot intel and management could be improved. Tie-ins to authoritative attribute providers for ID proofing may be useful for some customers. Companies that want a FRIP solution that is strong in device intel and behavioral biometrics will want to closely evaluate Buguroo's platform.

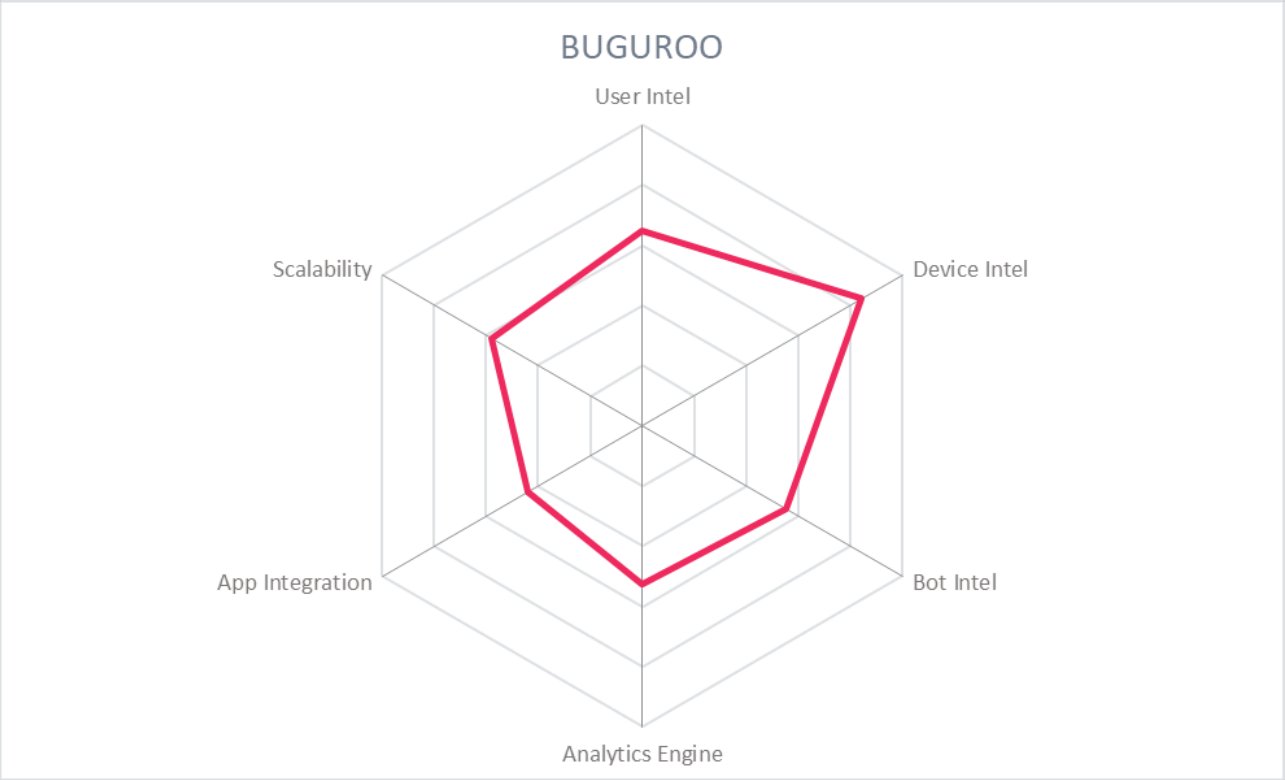
Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Ease of Delivery	●●●●○

Strengths

- Excellent use of device intel
- Full-featured behavioral biometrics implementation
- Built-in support for PSD2: behavioral biometrics and mobile client malware detection
- Fraudster Hunter module facilitates forensic investigations

Challenges

- Small but growing customer base
- No ID proofing
- Bot detection but no bot management


BUGUROO
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.4 Gurucul

Gurucul was founded in 2010 and is a privately-owned company headquartered in Los Angeles. Gurucul Fraud Analytics has functionality in all areas of FRIP. The solution can be run on-premises, in IaaS, or is available as SaaS. The SaaS solution is undergoing SOC2 type 2 examination. The solution is FIDO compliant. The cryptographic components of the solution are US FIPS 140-2 certified. The on-prem and IaaS versions are bundled with all components necessary to run the software or can use components already deployed by customers. Licensing is by monitored user or entity.

Gurucul can interoperate with various 3rd-party ID proofing services. Gurucul leverages in-house credential intelligence and can query 3rd-party services. Fraud Analytics' device intel capabilities are extensive, including device health assessments, malware detection via behavioral analysis, device fingerprinting, and IMEI/SIM data from MNOs. Gurucul's implementation of UBA is thorough: considering all pertinent attributes. Moreover, its implementation of multiple ML algorithms and hundreds of trained models gives it a distinct advantage.

For passive biometrics, Gurucul relies on other vendor's agents, such as Tanium EDR. If deployed in conjunction with other agents, Gurucul can harvest passive biometric elements such as keystroke/mouse analysis, gyroscopic analysis, swipe and screen pressure analysis, networks, etc. Gurucul can integrate with native mobile biometrics and 3rd-party FIDO compliant authenticators. Fraud Analytics' ML engines can detect bots and it offers various management and automated mitigation responses.

Gurucul accepts SAML for authentication and authorization, enabling it to interoperate with major MFA providers. Role-based and delegated access control are supported. App integration and security infrastructure interoperability are possible via APIs. JSON, JWT, OAuth2, OIDC, and all relevant threat data exchange standards are supported.

Gurucul is well-known for its UBA capabilities. Given that the solution meets and exceeds requirements for FRIP, it should be on the short list for any organization conducting an RFP for fraud reduction services.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Ease of Delivery	●●●●○

GURUCUL

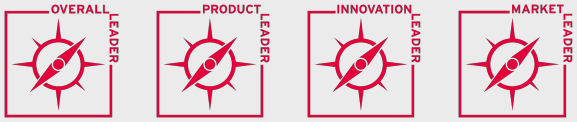
Strengths

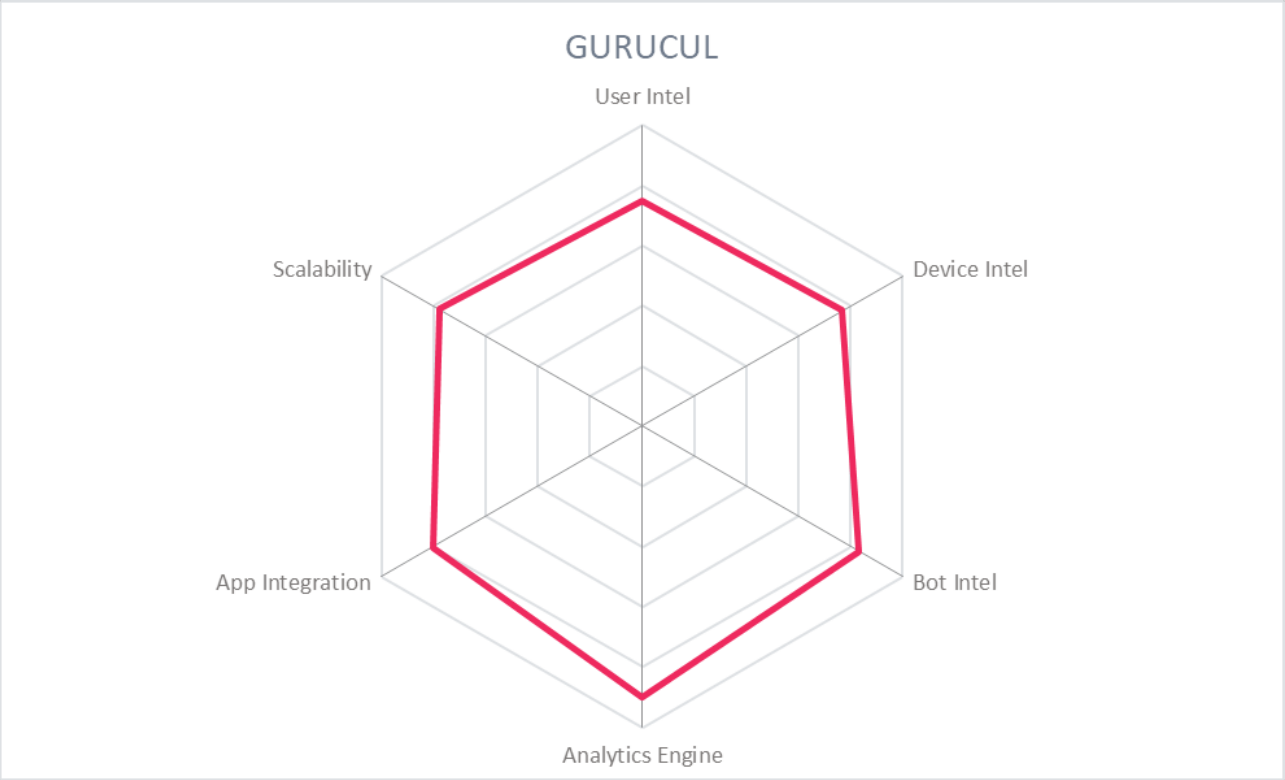
- Excellent support of all relevant standards
- Interoperability with ID proofing services
- Strong device intel and passive biometrics
- Industry-leading UBA functionality
- Extensive ML implementation
- Sophisticated bot detection and management
- Call center software integration

Challenges

- No built-in mobile SDK or JavaScript for passive biometrics collection
- Default data storage period should be increased

Leader in




GURUCUL
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.5 IBM

IBM's FRIP solution is composed of Trusteer modules and makes use of IAM, QRadar and Resilient for security intelligence and incident response. The integrated suite covers all aspects of FRIP except credential intelligence. IBM offers industry-specific profiles and support for a variety of sectors including finance, insurance, e-commerce, health care, gaming, travel, and more. The solution is SaaS delivered, and the service is ISO 27001 and SOC 2 certified. Licensing is per-session.

IBM can interoperate with a 3rd-party ID proofing / phone verification service. Trusteer's device intel capabilities are comprehensive, including device health assessments, malware detection, root detection, device fingerprinting, and IMEI/SIM data from MNOs. IBM has robust UBA, considering all germane data points including behavioral biometrics.

For passive biometrics, IBM uses JavaScript on computers and has a mobile SDK. Trusteer can analyze many elements such as keystroke/mouse analysis, gyroscopic analysis, swipe and screen pressure analysis, networks, etc. Moreover, IBM supports FIDO 2.0 authentication. IBM's solution uses activity analysis and passive biometrics to detect bots; recommendations can be made to the customer regarding how to treat bots, but actual bot management must be at the customer application(s).

The IBM platform offers MFA options for customer admins. Role-based and delegated access control are supported. App integration and security infrastructure interoperability are possible via APIs. JSON, OAuth2, and SAML standards are supported. Trusteer can be extended to interoperate with call center systems, IAM systems, and omnichannel tools though it requires customization.

IBM's security solutions are widely used across many enterprises. Solutions such as Trusteer Pinpoint and QRadar provide much functionality. Organizations with existing IBM security solution deployments may find it natural to utilize Trusteer Pinpoint for Fraud Reduction Intelligence purposes. For organizations looking for new FRIP solutions, particularly those with strong device intel and UBA features, IBM's suite should be on the consideration list. The IBM solution would benefit from credential intelligence and more bot management functionality.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Ease of Delivery	● ● ● ● ●

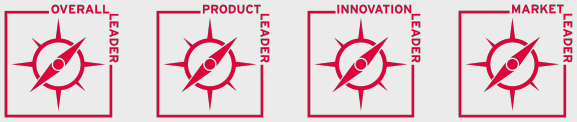
Strengths

- Interoperability with ID proofing services
- Excellent device intel features
- Strong UBA
- Bot detection capabilities
- Support for FIDO, OAuth2, and SAML

Challenges

- Bot response actions are limited
- No credential intelligence
- Multiple modules needed for full deployment
- Threat intel exchange standards not supported

Leader in




IBM
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.6 ID Data Web

Virginia-based ID DataWeb was founded in 2011. AXN was developed to address a need for collecting authoritative attributes (ID proofing) for government and commercial applications. The company was initially backed by venture capital but is now self-funded and revenue positive. Their solution now covers all aspects of fraud reduction. The solution is SaaS-based and is ISO 27001 certified. Licensing is a combination of per-user and per-transaction, depending on the type of attribute services requested.

AXN can draw from many authoritative attribute providers for ID proofing. An example of AXN's ID proofing is facial biometrics to government ID matching. The solution is used for employment verification, medical license verification, student verification, criminal watchlist checking, and OFAC compliance, and other use cases. ID DataWeb offers a secure mobile SDK for building additional mobile ID proofing apps. For credential intelligence, AXN uses in-network intel and feeds from ThreatMetrix and iovation. IDW's device intel capabilities run the gamut on all major data types including device health assessments, malware detection, root detection, device fingerprinting, and IMEI/SIM data from MNOs. IDW assesses a complete list of user behavioral attributes, albeit without using ML algorithms.

For passive biometrics, IDW uses JavaScript on computers and the aforementioned mobile SDK. IDW can analyze a wide range of data points such as keystroke/mouse analysis, gyroscopic analysis, swipe and screen pressure analysis, networks, etc. IDW supports FIDO authentication and can interoperate with other FIDO authenticators. IDW's solution uses embedded pixels, behavioral analysis, and passive biometrics to detect bots. IDW also gives customers a sophisticated array of bot management options, including challenging, throttling, redirection, and others.

ID Data Web has many MFA options for customer admins. Role-based and delegated access control are supported. App integration and security infrastructure interoperability are possible via APIs and these protocols/standards: JSON, JWT, OAuth2, OIDC, and SAML. AXN can interoperate with call center solutions; for example, using their Mobile Match service that can validate and pass on caller information.

ID DataWeb is small but growing rapidly thanks to their innovative and useful feature set. Organizations, both public- and private-sector, that need the full set of FRIP functionalities should consider AXN in RFPs. Organizations that have complex requirements for ID proofing against authoritative repositories, or that need mobile ID proofing solutions will especially want to look at IDW's AXN.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Ease of Delivery	●●●○○

iddataweb

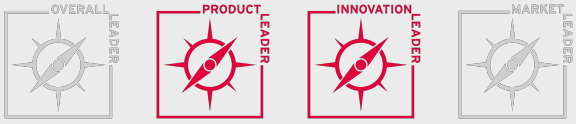
Strengths

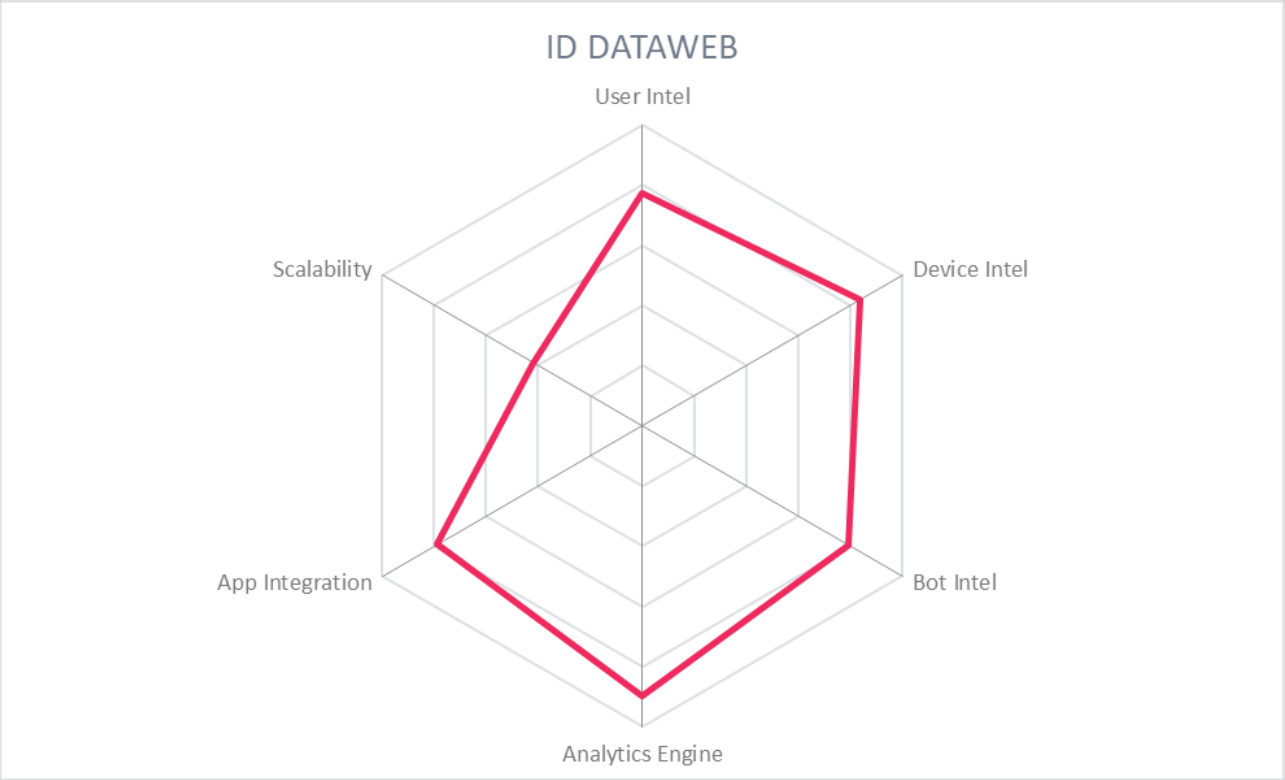
- Highly configurable, industry-leading ID proofing solution
- Full featured credential and device intel
- Good bot detection and management
- Secure mobile SDK that uses TEE

Challenges

- ML not used for UBA
- Small company and user base, but expecting to grow
- Mostly limited to North America at present

Leader in




ID DATAWEB
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.7 Kaspersky

Kaspersky has been providing cybersecurity solutions for more than two decades. Though headquartered in Russia, Kaspersky has a global presence with transparency centers in Switzerland and Spain. The solution can be run on-premises, in IaaS, or SaaS-delivered. For on-prem and IaaS, it runs on CentOS, Apache Cassandra, Kafka, and PostgreSQL. Kaspersky is pursuing ISO 27001 certification in 2020. Licensing is per-user. Kaspersky Fraud Protection (KFP) covers the functional areas of credential intel, UBA, device intel, passive biometrics, and bot management.

KFP does not currently integrate with 3rd-party ID proofing services but could be extended. For credential intelligence, KFP uses in-network intel and some external sources. KFP device intel capabilities are thorough, including device health assessments, malware detection, root detection, detailed device fingerprinting, and IMEI/SIM data from MNOs. KFP evaluates the full spectrum of user behavioral attributes and utilizes combinations of unsupervised and supervised ML algorithms for analysis.

For passive biometrics, KFP uses JavaScript on computers and a mobile SDK. KFP can analyze a wide range of data points such as keystroke/mouse analysis, gyroscopic analysis, swipe and screen pressure analysis, etc. FIDO support is on the 2020 roadmap. KFP uses behavioral analysis and passive biometrics to detect bots. KFP presents a risk score and analysis to customers that indicates likelihood of bot activity and allows customers to decide how to handle bots within their own applications.

For MFA for customer admins, Kaspersky supports OTP and their proprietary authentication app. Role-based control is supported. Kaspersky can interoperate with threat intelligence providers using OpenIOC and STIX. App integration and security infrastructure interoperability are possible via APIs; JSON and JWT are also supported.

KFP leverages Kaspersky's cybersecurity expertise in the area of FRIP. KFP's feature set is compelling overall, even though more MFA and bot management options would help the solution. Organizations with existing Kaspersky solutions may find it easy to include KFP, and others looking for FRIP functionality should review KFP's features in detail.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Ease of Delivery	●●●●○

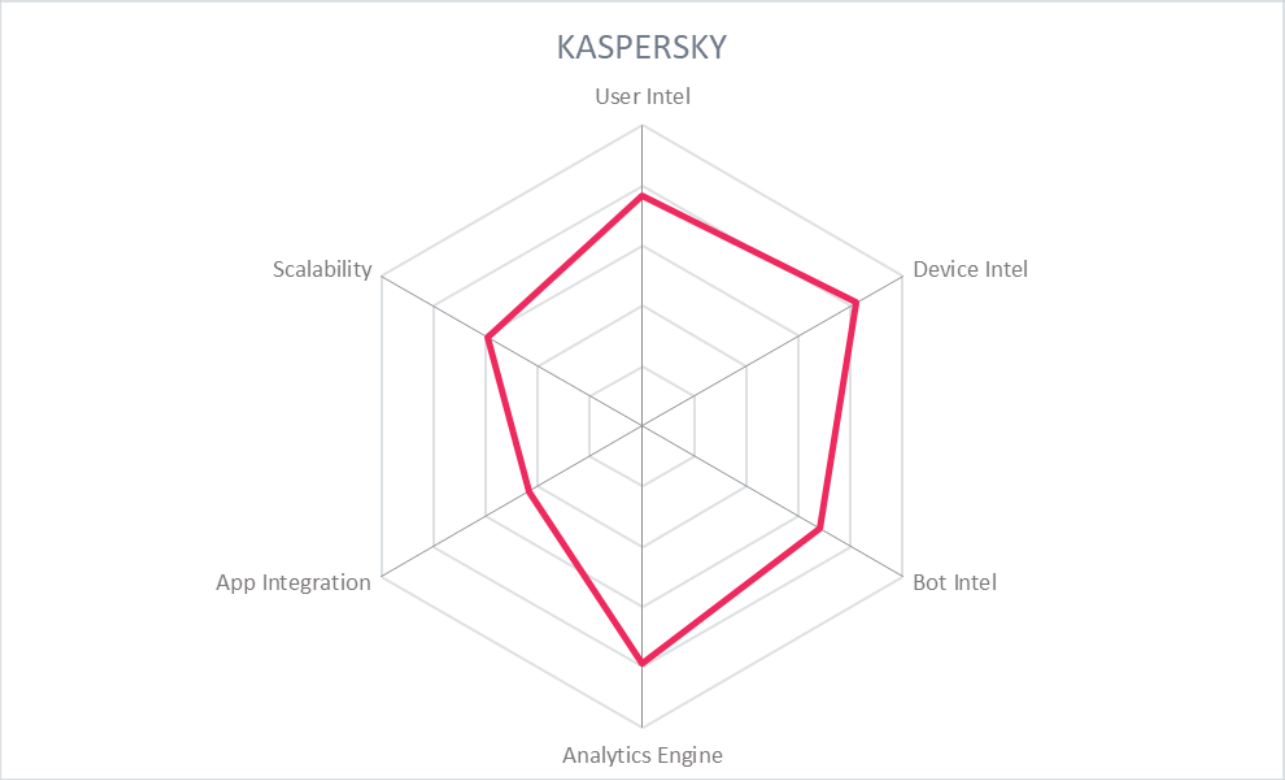
kaspersky

Strengths

- Excellent device intel and UBA capabilities
- Effective use of multiple ML techniques for anomaly detection and risk reduction
- Support for OpenIOC and STIX formats
- Global transparency centers where customers can review code

Challenges

- No ID proofing
- Limited bot management functionality
- Largest presence in RU but growing in EU
- Support for SAML and more MFA options would be helpful


KASPERSKY
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.8 Neustar

Neustar is a privately held risk analytics company based in Sterling, VA. 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 provides Domain Name Registry services and have been delegated authority for several top-level domains. Neustar Digital Identity Risk offers ID proofing, UBA, device intel, and bot management. It is a cloud-delivered service. Licensing is per-transaction. Neustar's service is both ISO 27001 compliant and SOC 2 Type certified.

For ID proofing, Neustar performs name/address/phone/email/IP verification and processes 13 billion records relating to North American residents. This information is also correlated with device intelligence. It can also consume 3rd-party authoritative attributes. No additional credential intel is gathered or evaluated. For device intel, IP reputation, IMEI/SIM, and location attributes are considered but it does not perform device health assessments, detailed fingerprinting, root detection, malware detection. They have a limited implementation of ML algorithms for enhanced analysis.

For UBA, login statistics, browser history, email address-to-device associations, identity-to-device associations and use of anonymizer attributes are evaluated. Other common UBA attributes are omitted from their UBA model. Even though Neustar processes PII, they are compliant with CCPA and GDPR.

Neustar does not utilize passive biometrics. They did not provide information on how the separately licensed Ultra-WAF service performs bot detection and management.

Neustar has separate services that provide call center integration, DNS security, and DDoS protection. Neustar supports OAuth2, JSON, JWT, and provides a REST API for application integration. The service supports highly secure management practices including MFA and role-based access control for admins.

Neustar's solution is highly scalable and performant. They provide basic ID proofing services, as well as IP reputation and domain registration for other service providers in this business. Neustar offers several related add-on products which make their solution appealing as a multi-faceted suite of fraud reducing services. Enhancing their device intelligence and UBA features would strengthen their overall offering. Businesses and agencies that need highly scalable FRIP services and access to a range of authoritative attributes should consider Neustar Digital Identity Risk and corresponding services.

Security	●●●●●
Functionality	●●●○○
Interoperability	●●●●○
Usability	●●●●○
Ease of Delivery	●●●●○

neustar®

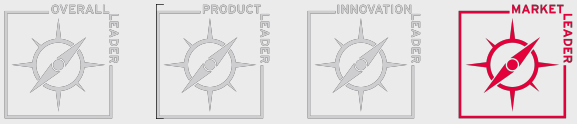
Strengths

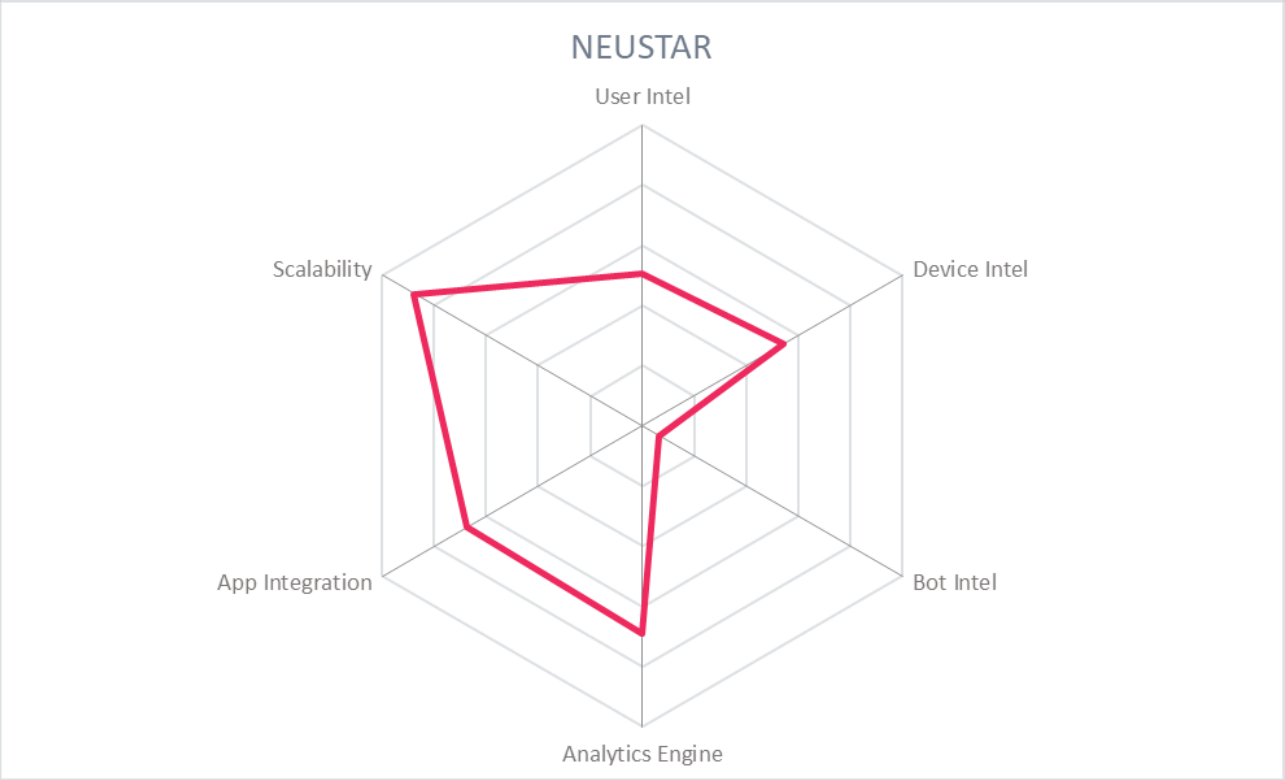
- Strong internal service security
- Large scale ID proofing service
- One of the largest IP reputation and intelligence repositories
- Call center integration, DNS protection, DDoS protection possible with add-ons

Challenges

- Bot management via separate WAF
- No passive biometrics or credential intel
- Basic implementation of device intel
- Large North American presence but not elsewhere

Leader in




NEUSTAR
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.9 NuData Security

Mastercard acquired Vancouver-based NuData Security in 2017. NuDetect is their FRIP solution, which covers the areas of UBA, device intel, behavioral biometrics, and bot management. NuDetect is SaaS-delivered but can be deployed for private cloud integration, or backhauled over VPNs or private links. The SaaS version is SOC 2 certified and PCI-DSS compliant. NuDetect has profiles for all major industries and enables connections to 3DS 2.0 providers, and compliance with KYC, OFAC, and PSD2. Licensing options include per-user, per-transaction, and fixed costs.

NuDetect does not integrate with 3rd-party ID proofing services but does process internal credential intelligence. For device intel, NuDetect utilizes device health assessments, root detection, detailed device fingerprinting, IP reputation, but does not detect malware or get IMEI/SIM data from MNOs. Instead, NuDetect mitigates account hijacking through malware using session-level behavioral analysis. NuDetect evaluates a wide range of user behavioral attributes. NuDetect employs a limited set of ML algorithms for analysis.

For passive biometrics, NuDetect uses JavaScript on browsers and client-side libraries on application servers and a mobile SDK. NuDetect can analyze data points such as keystroke/mouse analysis, gyroscopic analysis, network locations, etc. FIDO support is on their roadmap. NuDetect uses behavioral analysis, passive biometrics, and other methods to detect bots. NuDetect provides several bot management options, including challenging, throttling, and white/black-listing.

NuData accepts Google authenticator for admin access. Role-based access control is supported. NuDetect does not integrate with external threat exchange sources. App integration and security infrastructure interoperability are possible via APIs and JSON is supported.

NuDetect is well-positioned inside Mastercard to provide fraud reduction services for the payments sector. In particular, the 3DS 2.0, OFAC, and PSD2 compliance features demonstrate their ability to serve the large payments services market. However, NuDetect has good functionality and support for various industries beyond finance and should be considered when general FRIP capabilities are needed. The solution would be strengthened by adding support for ID proofing, credential intelligence, and threat exchange standards.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Ease of Delivery	●●●●○

NuData Security

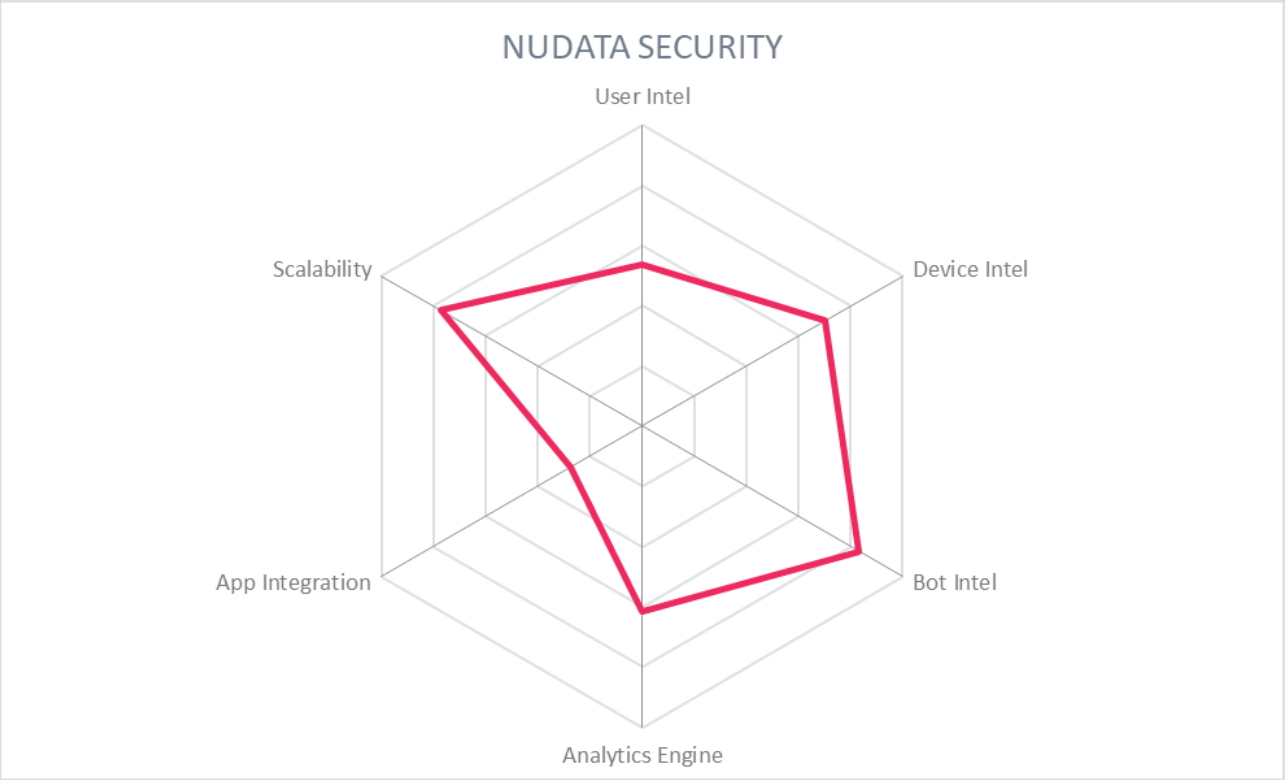
mastercard

Strengths

- Highly scalable
- Support for 3DS 2.0, KYC, OFAC, and PSD2; CCPA and GDPR for privacy
- Good bot management capabilities

Challenges

- Not extensible for ID proofing
- Does not utilize credential intelligence
- No malware detection


NUDATA SECURITY
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.10 RSA Security

RSA is a leading global cybersecurity vendor. Their Fraud and Risk Intelligence Suite is widely used in the finance sector, protecting over two billion consumers. It covers the functional areas of credential and device intelligence. It can be run on-premises on Linux or Windows with various supporting applications, and it is also available as SaaS. There are two separate solutions within RSA Fraud & Risk Intelligence Suite: RSA Adaptive Authentication Cloud, which is SOC 2 compliant; and RSA Adaptive Authentication for eCommerce, which is RSA's 3DS ACS solution for credit/debit card issuers. The eCommerce solution is SOC 2, PCI-DSS & PCI -3DS compliant. Licensing options for SaaS versions are per-transaction plus monthly hosting fees; licensing for the on-premise version is per-user/consumer.

RSA integrates with LexisNexis for KBA ID proofing. eFraudNetwork is RSA's credential intel service, which is a repository of known bad data elements, such as IP, device fingerprints, hashed IBAN Mule account identifiers, etc., which is shared globally between RSA customers. RSA processes a large subset of expected device intel parameters, including IP and device history, root detection, device fingerprinting, and IMEI/SIM data, but not device health assessments. RSA evaluates a wide range of user behavioral attributes, with many specific to payments use cases. However, patterns in failed login attempts are not discerned by the solution.

RSA does not have passive biometrics built into their solution, but telemetry from 3rd-party vendors can be processed by their analytics engine. FIDO support is currently available via the RSA Multi Credential Framework. RSA does provide a secure mobile SDK. Bot detection and management features are unavailable.

MFA over SAML or via APIs is supported for customer admins, as is role-based control. App integration and security infrastructure interoperability are possible via APIs; JSON, SAML, and SOAP are also supported. RSA FRIS has limited integration with call center solutions, however data from call center can be sent to the risk engine for risk analysis.

RSA Fraud and Risk Intelligence Suite possesses some competitive advantages: excellent credential intelligence (EFraudNetwork) and a UBA implementation that goes deeper into transaction details and histories than do other solutions. The platform needs bot detection/management and passive biometrics built-in, as well as a few enhancements in device intel and UBA.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●○○
Usability	●●●●○
Ease of Delivery	●●●○○

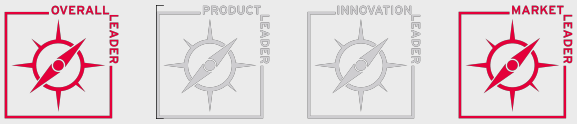
Strengths

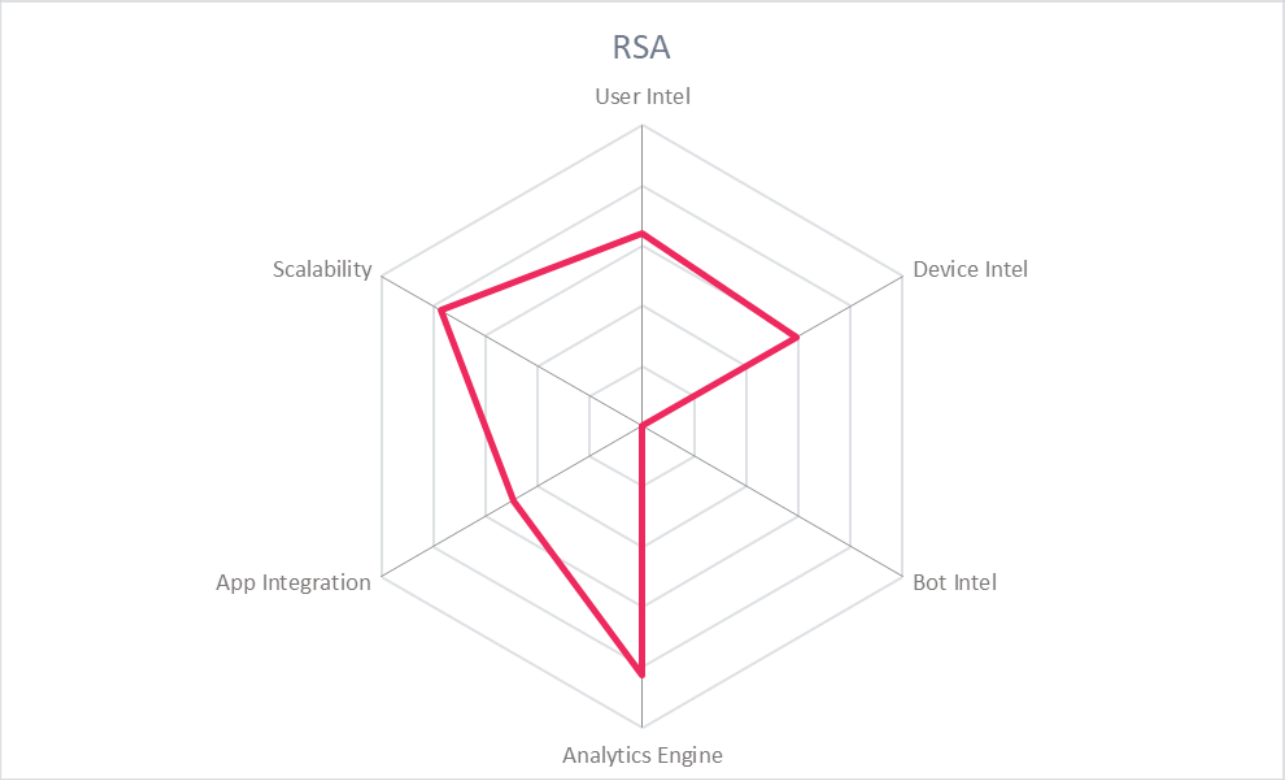
- Highly scalable
- Excellent credential intelligence features
- Good use of ML with daily updates to use-case-specific models.
- Sophisticated UBA covers transaction histories and cross-channel activities
- High Fraud detection rate with low intervention rates

Challenges

- No analysis of failed login attempts
- No malware detection
- Passive biometrics not built-in, although 3rd-party information can be consumed
- No bot detection or management
- Requires licensing multiple services for partial FRIP functionality

Leader in




RSA
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.11 Transmit Security

Transmit Security was founded in 2014 and is headquartered in Tel Aviv, Israel with its US headquarters in Boston, Massachusetts. The company is self-funded. Their FRIP platform covers all areas except bot management. Its software can run on-premise on Linux with MongoDB, SQL, Cassandra, and DynamoDB. It is also available as PaaS (SOC 2 certified). Their platform processes over a billion transactions daily for their customers worldwide. Transmit facilitates compliance with 3DS 2.0, KYC, and PSD2. Licensing is per-user over different time periods.

Transmit integrates with multiple 3rd-party ID proofing services such as Equifax, LexisNexis, and Payfone; and has a mobile SDK to facilitate mobile document verification. Transmit uses its own credential intelligence and allows customers to plug in 3rd-party sources. Transmit collects a full set of device intel, including IP reputations from external sources, as well as device health assessments, IMEI/SIM data, root detection, detailed device fingerprinting, but does not detect malware. Transmit's ML-enhanced profile engine evaluates the broadest range of user behavioral attributes, including transaction details and information from social media, where allowed.

For passive biometrics, Transmit uses JavaScript on browsers and a mobile SDK. It can collect information from 3rd-party authenticators and analyze keystroke/mouse analysis, gyroscopic analysis, swipe analysis, network locations, etc. FIDO UAF and 2.0 are supported. Transmit does not directly detect or manage bots.

Transmit provides several MFA options for admins. Role-based and delegated access control is supported. App integration and security infrastructure interoperability are possible via APIs, and JSON, JWT, OAuth2, OIDC, OpenIOC, SAML, STIX, TAXII are supported. Transmit interoperates with call center solutions such as Nuance and Pindrop.

The Transmit Platform has advanced support for almost all FRIP functions with the exception of bot detection and management. Within the categories of device intel and UBA, their solution is able to analyze potentially pertinent information that other solutions cannot. Their support for standards maximizes interoperability with other security and identity systems. Transmit Security should be on the shortlist for any organization looking for fraud reduction solutions.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Ease of Delivery	●●●●○

transmit SECURITY

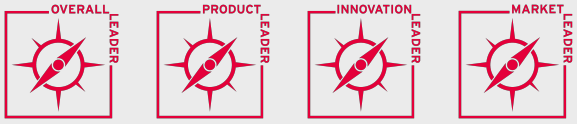
Strengths

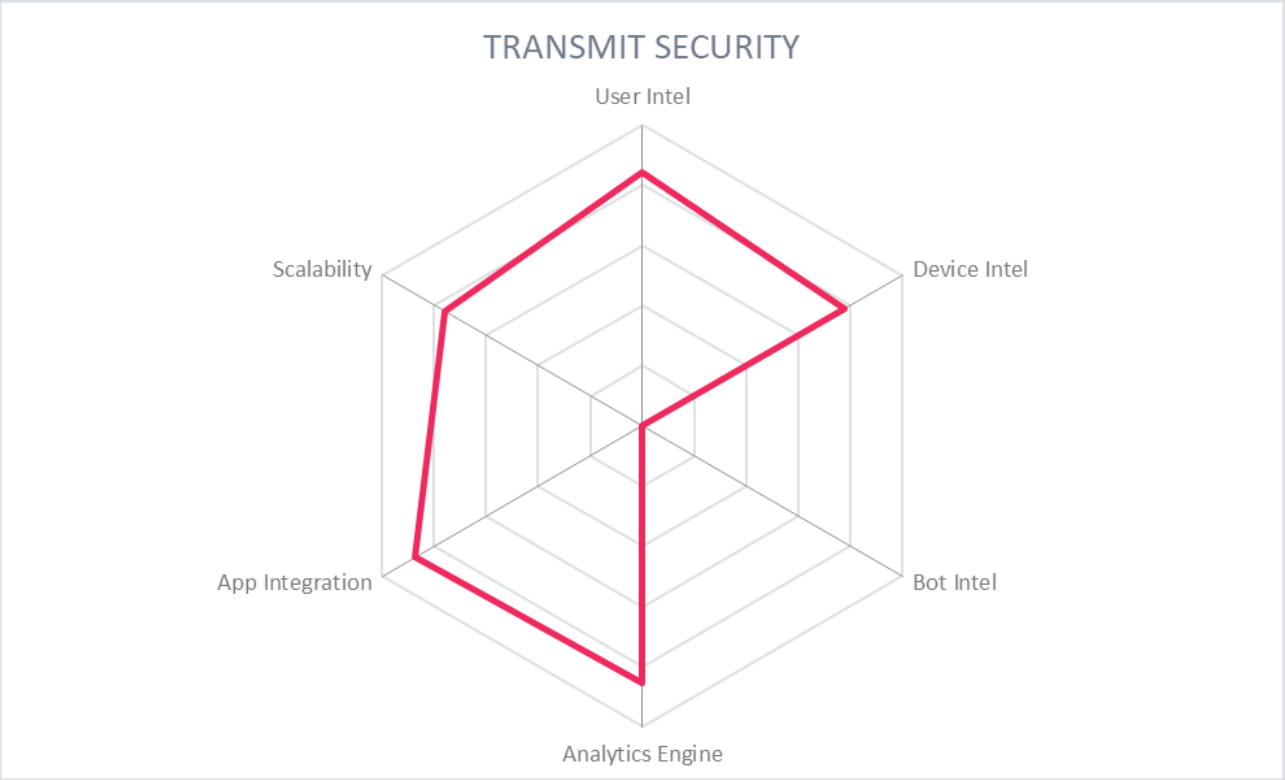
- Service connectors and mobile SDK for ID proofing
- Excellent cred and device intel features
- Largest selection of UBA attributes analyzed
- Broadest support for threat exchange and identity standards
- Call center integration

Challenges

- Does not detect malware on end-user devices
- No bot management
- Limited case management functionality

Leader in




TRANSMIT SECURITY
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

5.12 TransUnion

TransUnion IDVision is their FRIP service, which leverages iovation, a Portland, OR based company launched in 2004. iovation is now a subsidiary of TransUnion. 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. Multiple licensing options are available.

TransUnion is a native IP proofing solution and thus has access to attributes from multiple authoritative providers. TransUnion does not perform credential intelligence. TransUnion processes a complete set of device intel by means of JavaScript and SDKs, which include data types such as IMEI/SIM data, IP reputation, proxy and root detection, device fingerprinting. However, it does not detect malware or perform device health assessments. TransUnion does not engage directly in UBA, but some limited UBA-like functionality can be inferred from device intel and history. Customers can opt for TransUnion TLOxp, a social media analysis service that can be used for manual reviews at account-creation-time.

TransUnion does not provide passive biometric analysis. IDVision with iovation provides IP-based botnet detection as part of its device risk assessments. This includes a business rule specifically to watch for botnet history. IDVision with iovation does not provide bot management; rather, fraud analysts at customer sites decide how to handle botnet activity in accordance with their own policies.

Strong authentication for customer admins is not available. Role-based and delegated access control is supported. App integration is possible via APIs and JSON is supported. TransUnion states that they receive and process external feeds of threat intelligence, which includes email and phone intelligence, IP-based geolocation data, proxy usage, and botnet history but does not specify the sources or standards supported. TransUnion can respond to phone number authentication requests via its Transaction API to facilitate call center integration. Moreover, customers may opt to use TransUnion's FRIP services with their MFA services.

TransUnion is one of the three largest credit rating agencies in the US and is a provider of authoritative transaction, device details, and history in certain domains. Their ID proofing capabilities are strong, but they lack several key features needed for full implementations of FRIP. Their SDKs could be extended to provide additional device intelligence, passive biometrics, and bot detection features. Organizations that need excellent ID proofing functions in supported locations will want to consider TransUnion services.

Security	●●●●○
Functionality	●●●○○
Interoperability	●●●○○
Usability	●●●●○
Ease of Delivery	●●●●○

TransUnion

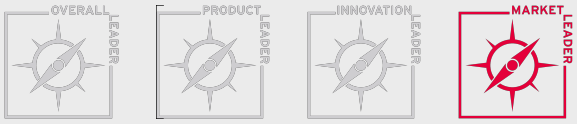
Strengths

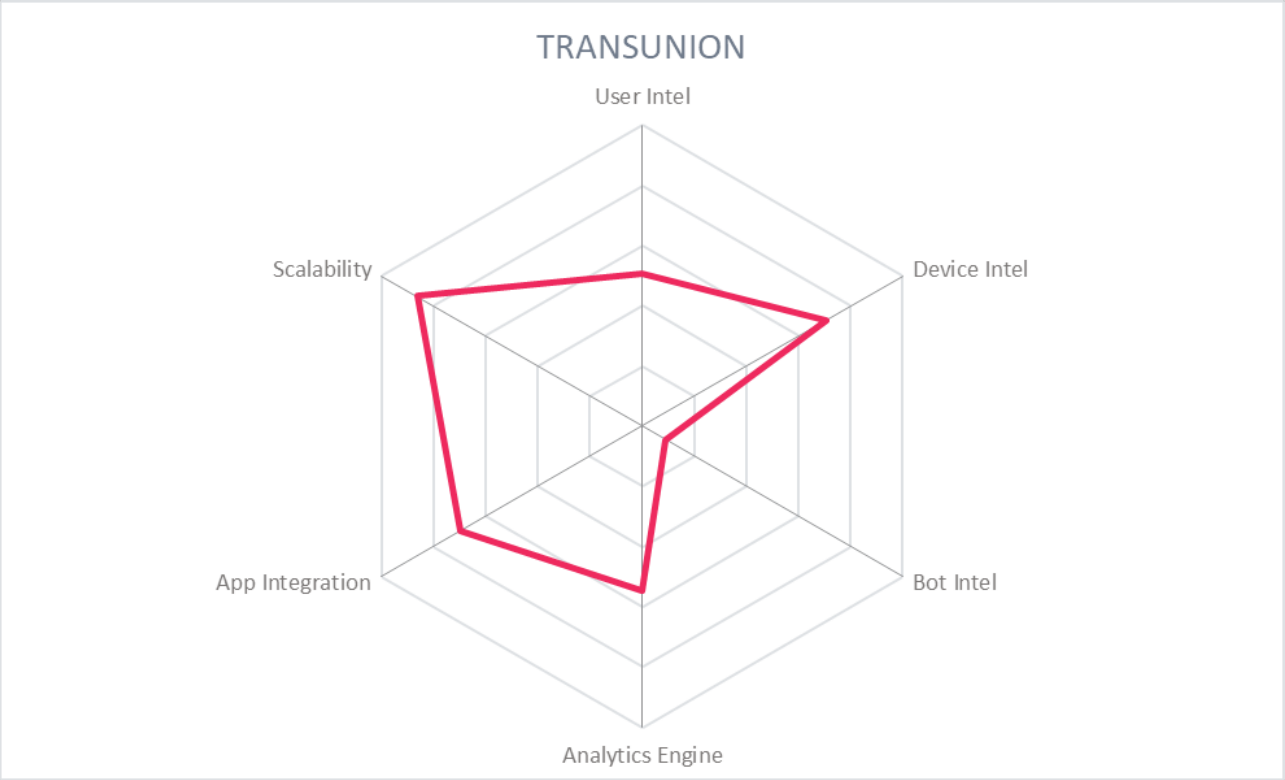
- Robust built-in ID proofing solution
- Access to authoritative attributes
- Highly scalable and performant services
- iovations' device intelligence services are used by other FRIP and risk-adaptive authentication service providers

Challenges

- No credential intel or passive biometrics
- No UBA functions
- Some bot detection but no bot management

Leader in




TRANSUNION
User Intel
Device Intel
Bot Intel
Analytics Engine
App Integration
Scalability

6 Vendors and Market Segments to watch

Aside from 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 Forter

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

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

7 Related Research

Leadership Compass: CIAM Platforms – 79059
Leadership Compass: Cloud-based MFA Solutions – 70967
Leadership Compass: Adaptive Authentication - 79011

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 ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole Analysts, founded in 2004, is a global analyst company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.
For further information, please contact clients@kuppingercole.com.