Fraud Reduction Intelligence Platforms (FRIP)

John Tolbert

April 25, 2023

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.

Contents

Figures

Introduction / Executive Summary

Fraud is a major cost to businesses worldwide and this has been exacerbated by the worldwide Covid pandemic. Banking, finance, payment services, and retail are some of the most frequent targets of fraudsters. 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. After years of being the focus of cybercriminals, banking and financial institutions are more likely to be better secured than other industries, meaning that fraudsters are increasingly likely to attack any potentially lucrative target if given the opportunity. Fraud perpetrators are continually diversifying and innovating their Tactics, Techniques, and Procedures (TTPs).

The most prevalent types of fraud businesses, non-profit organizations, and government agencies experience today are:

- **Account Takeover (ATO) Fraud** - 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.
- **Account Opening (AO) Fraud** – also called New Account Fraud or Synthetic Fraud, often happens as a result of using stolen identities or assemblages of personal information to create synthetic digital IDs. Such fraudulently created accounts can be more difficult to detect, which is an advantage for the attackers. This type involves gathering complete sets of or bits of PII (Personally Identifiable Information) on legitimate persons to construct illegitimate accounts. Educational, financial, government, employment, and medical records and social media 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. Various financial regulations require validation of users at registration time for Anti-Money Laundering (AML), Know Your Customer (KYC), US Office of Foreign Asset Control (OFAC), Politically Exposed Persons (PEP) validation, and other sanctions screening.

Many other types of online fraud exist and they continue to proliferate and evolve. Examples are listed below based on categories:

Phishing/Smishing/Vishing threats, many of which can be perpetrated by bots:

- Shopping scams
- Caller ID spoofing detection (app-based)
- Fake investment opportunities (crypto, gold, real estate, etc.)
- Fake push notifications
- Fake delivery notices
- Fake utility, telco, broadband cutoff notices

- Fake invoices
- Malicious invoice payment redirection
- CEO/CFO email impersonation for sending fraudulent payments
- Financial institution impersonation misdirecting customers to transfer funds for safety
- Fake Drivers' License offers
- Fake government welfare signup and collection notices
- Fake tax refund notices
- Fake student loan offers
- Fake notices from utilities, medical providers, pharmacies
- Fake tech support scams
- Fake "questionable charge" scams impersonating credit card companies or merchants
- Travel deal scams
- Travel refund scams
- Vacation rental scams
- Event ticket scams
- Fake vaccine cards (and scams)
- Lottery/inheritance/customs advance fee scams
- Realtor/mortgage email impersonation for escrow payment redirection
- SMS OTP harvesting
- Romance site scams
- Dox bots

Issuer issues:

- Card-Not-Present (CNP)
- Counterfeit (Skimmed or cloned)
- Stolen cards

Website operator issues, most of which are caused by bots:

- Malicious credential/payment skimmer code
- Inventory hoarding / Grinch bots
- Jingle bots (add to cart and abandon)
- API inventory checking bots
- Competitive price checking bots
- Headless browsers
- DDoS
- Fake reviews and comments
- Malicious link and ad insertion bots (comments, reviews, forums, etc.)
- Social media bots
- Ad Fraud/Click bots
- Account creation bots
- Credential stuffing bots
- File downloading bots

- Event ticket purchase and scalping bots
- Gift card cracking
- Malicious "overlay" apps
- SEO poisoning
- SIM swap (SMS OTP redirect)
- Email address harvest for spam bots
- Fake job postings
- Fake goods on auction sites
- Fake car, truck, and RV listings

Cryptocurrency

- Fake ICOs
- Fake coins
- Fake wallet aggregators
- Fake exchanges
- Cryptocurrency address / clipboard hijacking malware

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 are 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
- Credential intelligence
- Device intelligence
- User behavioral analysis
- Behavioral/passive biometrics
- Bot detection & management

Figure 1: The Six Major Fraud Reduction Techniques

Highlights

- Fraudsters continue to innovate, deriving additional techniques from existing ones and developing new methods delivered across all channels.
- Vendor solutions exhibit an increased emphasis on providing identity proofing services, either within their platforms or through OEM or technical partnerships.
- Call center integration, while not common across all FRIP vendors yet, is a growth area given the multi-pronged nature of fraud attacks. Vendors offering call center integration report that it is highly sought after by customers compared to just a few years ago.
- More FRIP vendors are using internal and third-party sources of compromised credential intelligence to prevent ATOs.
- Device intelligence is a mature capability utilized by most solutions; in some cases, FRIP service providers are members of the intelligence supply chain of other vendors.
- Bot detection and management have become more central to deterring many types of fraud attempts, since many forms of fraud are automated by bots. Vendors are improving their abilities to detect, classify, and provide options for handling bots.
- The Overall Leaders in Fraud Reduction Intelligence Platforms are Akamai, BioCatch, Experian, F5, Forter, GBG, Group-IB, HID Global, IBM, LexisNexis Risk Solutions, Outseer, and Transmit Security.
- The Product Leaders in Fraud Reduction Intelligence Platforms are Arkose Labs, BioCatch, Experian, F5, Forter, Group-IB, HID Global, IBM, ID Dataweb, LexisNexis Risk Solutions, Outseer, and Transmit Security.

- The Innovation Leaders in Fraud Reduction Intelligence Platforms are BioCatch, Experian, F5, Group-IB, HID Global, Human Security, IBM, ID Dataweb, LexisNexis Risk Solutions, and Transmit Security.
- The Market Leaders in Fraud Reduction Intelligence Platforms are Akamai, Broadcom, Experian, F5, Forter, GBG, HID Global, Human Security, IBM, LexisNexis Risk Solutions, Outseer, and Sift.

Market Segment

The Fraud Reduction Intelligence Platform market is mature and still growing in response to increased fraud risk levels globally. 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 robust bot detection & management. Others excel at user behavioral analysis and passive biometrics, but do not offer identity proofing. In general, identity proofing is quite specialized and is not built-in to all FRIP services. Many FRIP vendors allow customers to outfit their instances with identity proofing capabilities by enabling API callouts to 3rd-party ID proofing 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. Some have specializations for detecting and deterring ecommerce fraud. Others are more general purpose, offering their services for insurance, health care, gaming, hospitality, retail, travel, etc.

Delivery Models

In the Fraud Reduction Intelligence Platform market, solutions are mainly offered as SaaS. Vendors run their platforms in the cloud or in their own data centers and manage these services for their customers. FRIP services are consumed via APIs. For these SaaS offerings, the licensing model is often priced according to transaction volumes. There are a few vendor solutions that can run (or in one case, only run) on customer premises.

Required Capabilities

For this Leadership Compass, we evaluate solutions that address most of the six major functionality areas outlined below. 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 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. Innovative solutions may include support for Anti-Money Laundering (AML), Know Your Customer (KYC), US Office of Foreign Asset Control (OFAC), Politically Exposed Persons (PEP), Sanctions, Special Interest Entity (SIE), Special Interest Person (SIP), and Relatives & Close Associates (RCA) list validation. Providing mobile apps and SDKs that facilitate remote identity verification is another innovative solution gaining traction in this market.

- 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?". Some FRIP vendors aggregate credential intelligence from across their customer bases. Others receive and process such information from 3rd-party services, although this is uncommon.

- User Behavioral Analysis (UBA) – examination of past user activities to determine if the current login attempt or 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. Storage of personal information may be subject to data privacy regulations depending on jurisdictions. UBA is necessary for basic ATO protection. Innovative solutions in this space also perform transaction analysis.

- Device Intelligence - includes device hygiene (OS patch versions, anti-malware client presence, and RAT and other malware behavioral detection), device history and reputation, location history, IP reputation, MNO carrier information (IMSI, IMEI, etc.). MNO identifiers, in conjunction with UBA and Behavioral Biometrics (see next bullet point), can enable FRIP services to detect SIM swap attacks. Some services may include consumption of other 3rd-party sources of information. Innovation here is demonstrated by including the widest sources of relevant information for runtime analysis as well as consideration of the methods of acquisition.

- Behavioral/Passive Biometrics – the ability to analyze metrics of users' physical interaction with devices for comparison against registered samples. For desktop/laptop computers, this usually involves 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. Innovative vendors go beyond the basic attributes described above and can make predictions about fraudulent intent based on extrapolations and aggregations of this data type.

- Bot Detection and Management – 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. Some FRIP solutions allow for granular bot management, as not all bots are bad. Bot management capabilities include challenging, redirection, and throttling. Innovation in

this area involves extensive use of ML detection methods, unobtrusive techniques for challenging suspected bots, and highly configurable response options.

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 across all the data types listed above. This enables more accurate determination of risk scores and helps 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.

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 have created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right.

Overall Leadership
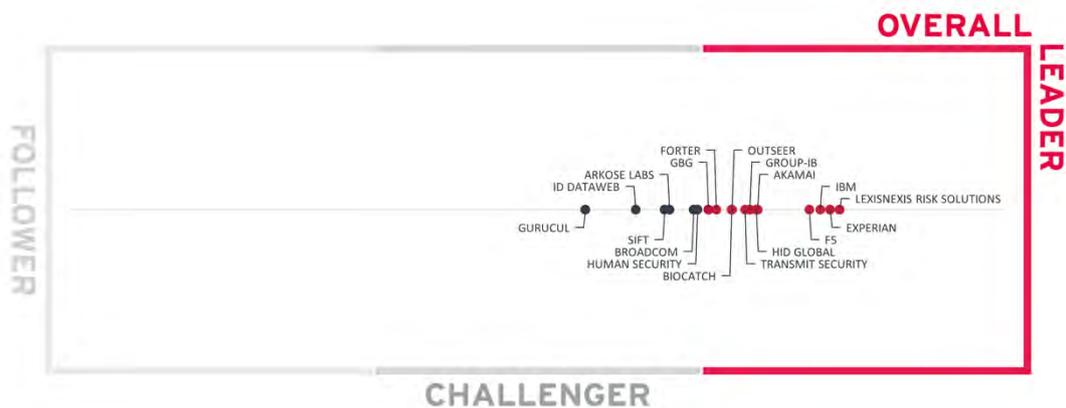
Figure 2: Overall Leaders in Fraud Reduction Intelligence Platforms

The Fraud Reduction Intelligence Platforms market is mature, with a well-defined but diverse feature set. The market itself is quite large and continues to grow as the prevalence and types of fraud expand.

The Overall Leaders in FRIP are Akamai, BioCatch, Experian, F5, Forter, GBG, Group-IB, HID Global, IBM, LexisNexis Risk Solutions, Outseer, and Transmit Security.

The Overall Challengers are Arkose Labs, Broadcom, Gurucul, Human Security, ID Dataweb, and Sift. There are no Followers in this edition.

Overall Leaders are (in alphabetical order):

- Akamai
- BioCatch
- Experian
- F5
- Forter
- GBG
- Group-IB
- HID Global
- IBM
- LexisNexis Risk Solutions
- Outseer
- Transmit Security

Product Leadership

Product Leadership is the first specific category examined below. This view is primarily based on the presence and completeness of required features as defined in section 1.4. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership Chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

Figure 3: 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. Product Leaders have the most complete mix of identity proofing, user behavioral analysis, credential and device intelligence, behavioral

biometrics, and bot detection & management capabilities. Not all solutions contain all components, as will be detailed in each vendor entry below.

Some FRIP solutions are more attuned to finance and payment security use cases, and others specialize in preventing fraud that impacts other industries' web presences, such as gaming, hospitality, insurance, retail, and travel. Some of the Product Leaders' solutions are more generalist, addressing the fraud protection needs of customers in multiple industries.

The Product Leaders in FRIP (in alphabetical order) are Arkose Labs, BioCatch, Experian, F5, Forter, Group-IB, HID Global, IBM, ID Dataweb, LexisNexis Risk Solutions, Outseer, and Transmit Security.

The Challengers in Product Leadership in FRIP are Akamai, Broadcom, GBG, Gurucul, Human Security, and Sift. The Followers section is empty.

Product Leaders (in alphabetical order):

- Arkose Labs
- BioCatch
- Experian
- F5
- Forter
- Group-IB
- HID Global
- IBM
- ID Dataweb
- LexisNexis Risk Solutions
- Outseer
- Transmit Security

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.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in section 1.4. The vertical axis shows the amount of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

Figure 4: Innovation Leaders in Fraud Reduction Intelligence Platforms

As a mature discipline, FRIP has many features that are expected and several features that are innovative enough to set some vendors' solutions apart from the rest. Among the noteworthy innovative developments in FRIP are increasing use of identity proofing (including the leveraging of external services), customization of ML detection models, sophisticated behavioral biometrics, thorough bot detection and management, and coverage of specific financial and ecommerce use cases.

The Innovation Leaders are BioCatch, Experian, F5, Group-IB, HID Global, Human Security, IBM, ID Dataweb, LexisNexis Risk Solutions, and Transmit Security.

The Challengers in Innovation are Akamai, Arkose Labs, Broadcom, Forter, GBG, Gurucul, Outseer, and Sift. No vendors appear in the Follower section.

Innovation Leaders (in alphabetical order):

- BioCatch
- Experian
- F5
- Group-IB
- HID Global
- Human Security
- IBM
- ID Dataweb
- LexisNexis Risk Solutions
- Transmit Security

Market Leadership

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.

The vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.
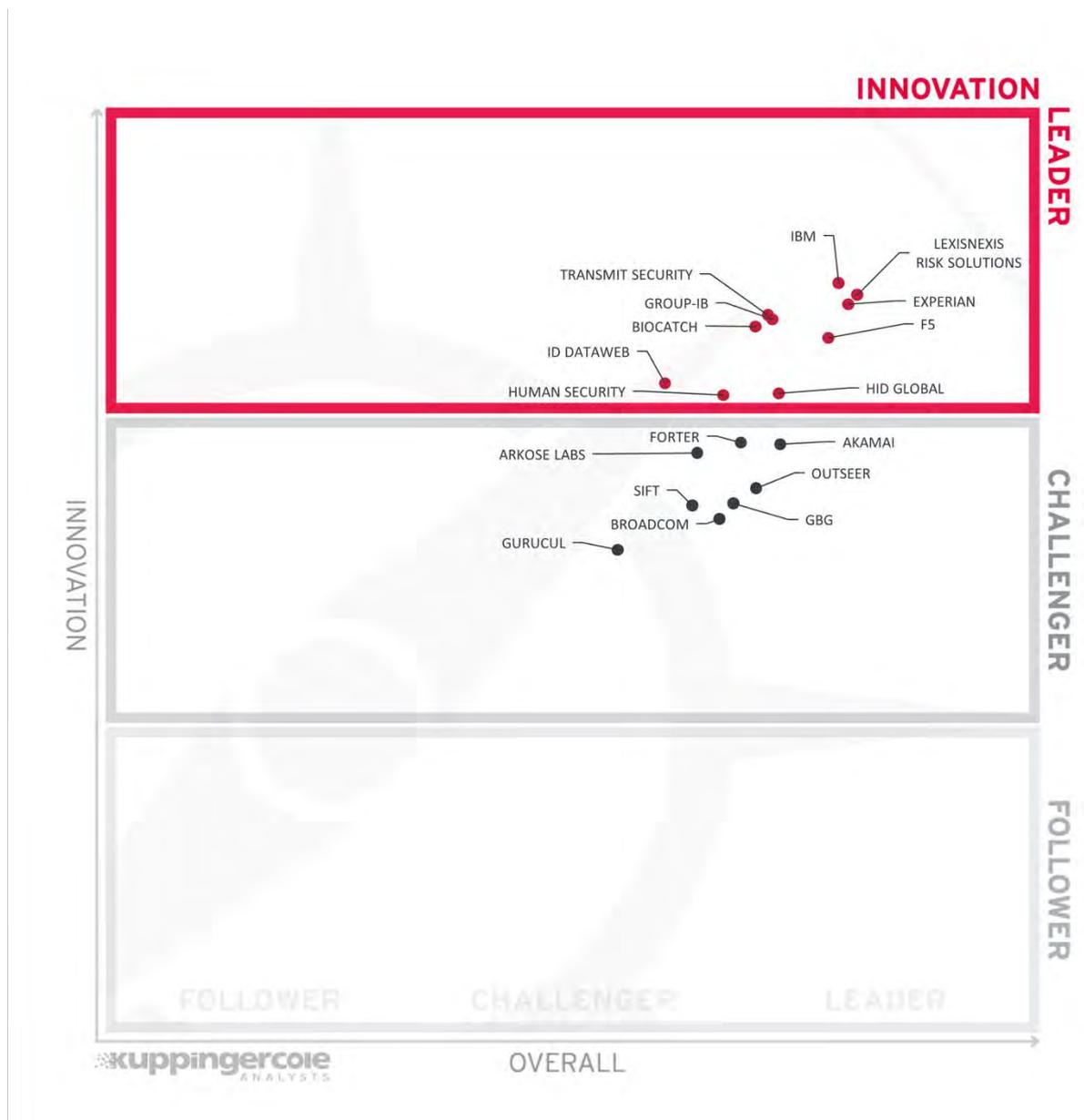

Figure 5: Market Leaders in Fraud Reduction Intelligence Platforms

Market Leadership in FRIP is determined by many factors, including overall vendor financial position, company sizes, numbers and geographic distribution of customers, number and geographic distribution of ecosystem partners such as system integrators, and levels of regional and language support.

The Market Leaders in FRIP are Akamai, Broadcom, Experian, F5, Forter, GBG, HID Global, Human Security, IBM, LexisNexis Risk Solutions, Outseer, and Sift.

The Challengers in Market Leadership for FRIP are Arkose Labs, BioCatch, Group-IB, Gurucul, ID Dataweb, and Transmit Security. There are no vendors listed in the Follower area.

Market Leaders (in alphabetical order):

- Akamai
- Broadcom
- Experian
- F5
- Forter
- GBG
- HID Global
- Human Security
- IBM
- LexisNexis Risk Solutions
- Outseer
- Sift

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 following charts are rectangular and divided into nine equal sections. A dashed line intersects the rectangle at the point where x- and y-axis values are equal.

The Market/Product Matrix

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

The vertical axis represents the market position plotted against product strength rating on the horizontal axis.
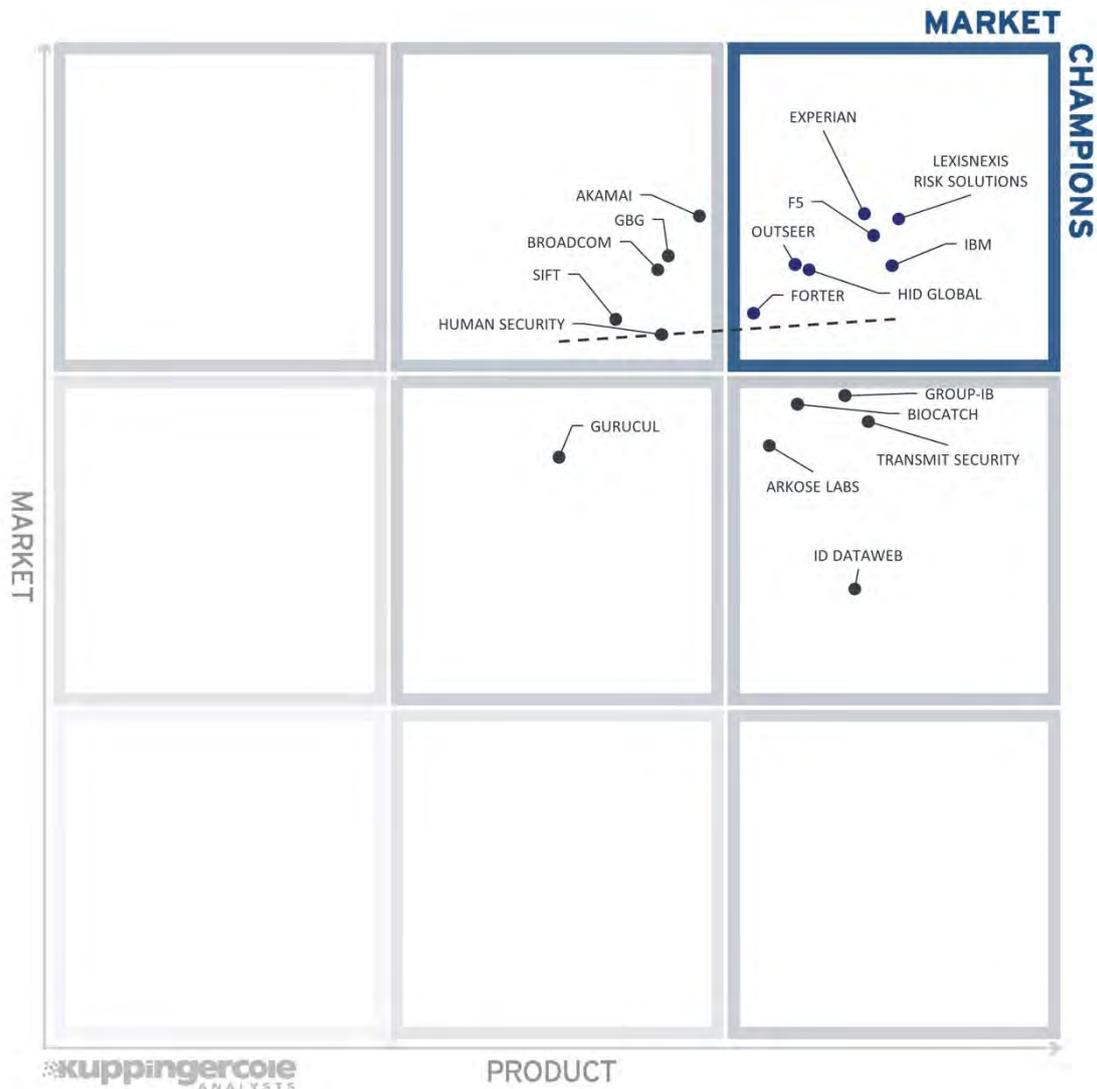
Figure 6: Market Champions in Fraud Reduction Intelligence Platforms

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 Champions in FRIP are (in alphabetical order) Experian, F5, Forter, HID Global, IBM, LexisNexis Risk Solutions, and Outseer.

In the top center box (and above the line), we see Akamai, Broadcom, GBG, Sift, and Human Security.

Gurucul appears below the line in the center of the chart.

In the right center box (and below the line), we find Group-IB, BioCatch, Transmit Security, Arkose Labs, and ID Dataweb. Given the strength of their products, we expect greater market growth opportunities for solutions in this section of the chart.

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.

The vertical axis represents the product strength rating plotted against innovation on the horizontal axis.
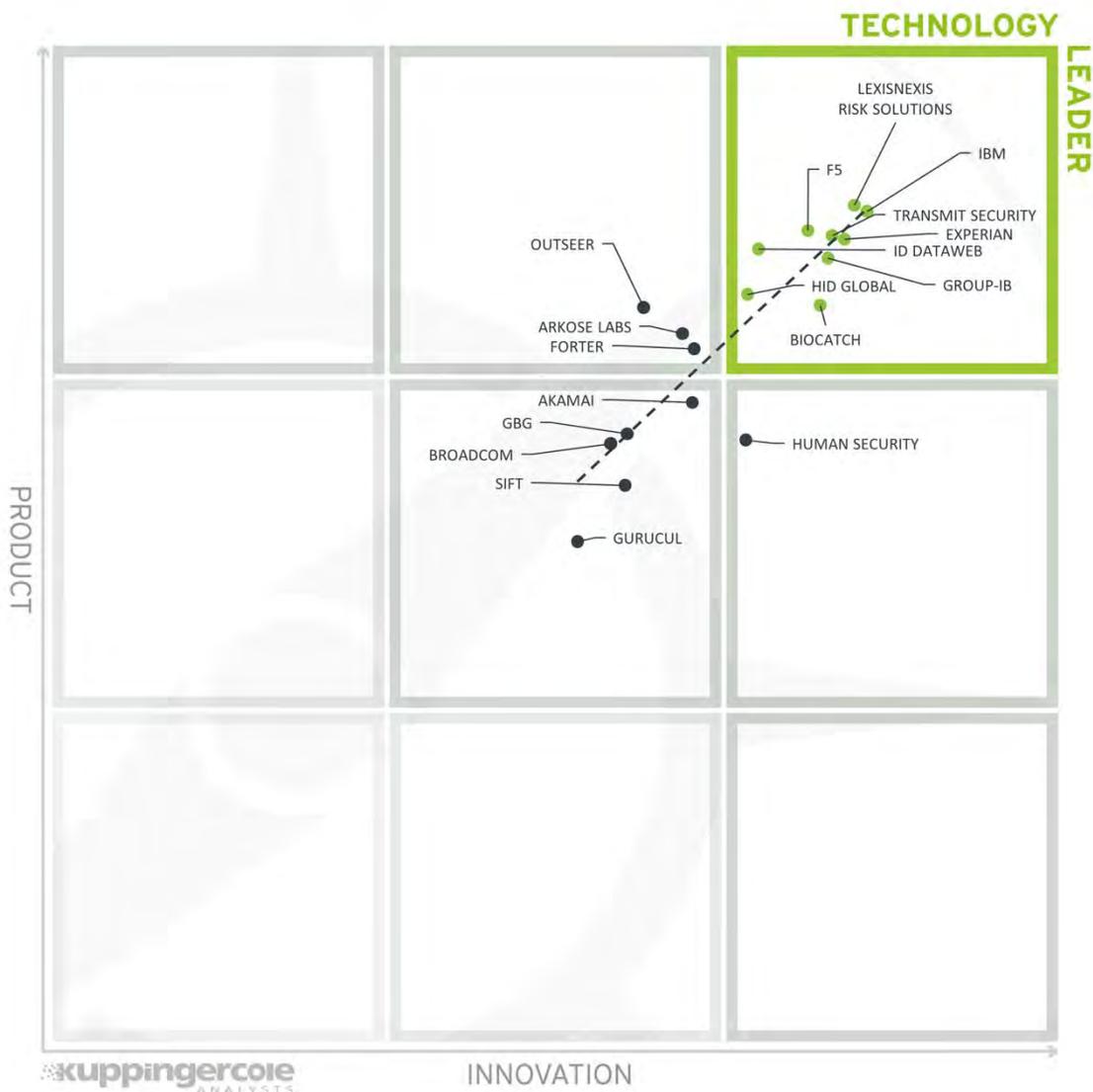
Figure 7: Technology Leaders in Fraud Reduction Intelligence Platforms

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 (in alphabetical order) BioCatch, Experian, F5, Group-IB, HID Global, ID Dataweb, IBM, LexisNexis Risk Solutions, and Transmit Security.

Arkose Labs, Forter, and Outseer are found in the top center box.

In the main sequence in the center box, we see Broadcom and GBG just slightly above and on the line with Akamai, Sift, and Gurucul below the line.

Human Security is in the center right.

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.

The vertical axis represents the market position rating plotted against innovation on the horizontal axis.
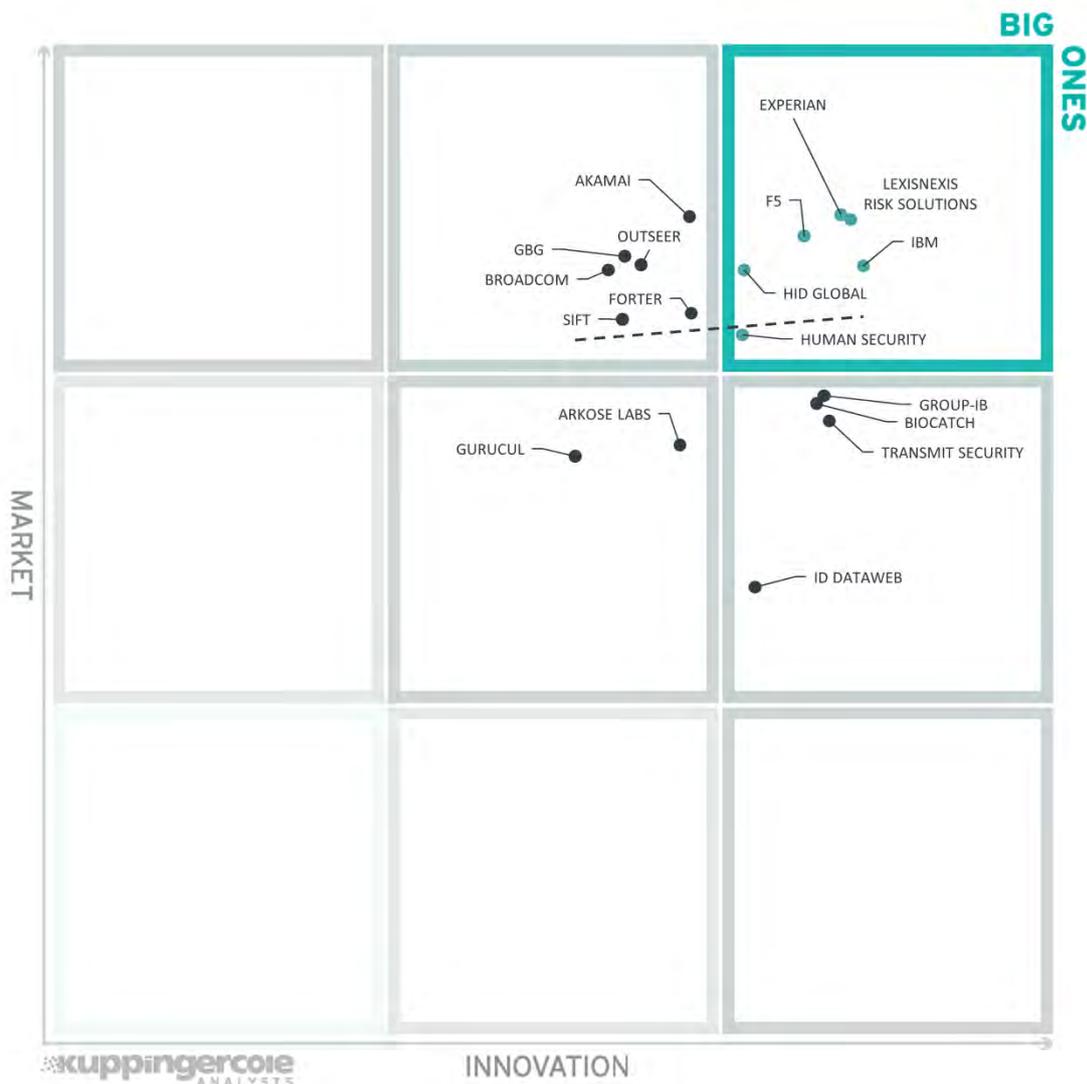
Figure 8: Big Ones in Fraud Reduction Intelligence Platforms

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 (in alphabetical order) Experian, F5, HID Global, Human Security, IBM, and LexisNexis Risk Solutions.

In the top center square, we see Akamai, GBG, Outseer, Broadcom, Forter, and Sift.

In the center of the chart, we find Arkose Labs and Gurucul below the line.

In the right center, we see Group-IB, BioCatch, Transmit Security, and ID Data Web.

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	Deployment	Interoperability	Usability
Akamai	Strong Positive	Positive	Strong Positive	Neutral	Positive
Arkose Labs	Positive	Positive	Neutral	Positive	Strong Positive
BioCatch	Positive	Positive	Strong Positive	Neutral	Strong Positive
Broadcom	Strong Positive	Positive	Neutral	Strong Positive	Strong Positive
Experian	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
F5	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Forter	Positive	Positive	Neutral	Neutral	Positive
GBG	Neutral	Positive	Positive	Positive	Strong Positive
Group-IB	Positive	Strong Positive	Positive	Positive	Strong Positive
Gurucul	Positive	Weak	Positive	Positive	Positive
HID Global	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Human	Positive	Positive	Strong Positive	Positive	Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
ID Dataweb	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive

LexisNexis Risk Solutions	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Outseer	Strong Positive	Positive	Strong Positive	Positive	Neutral
Sift	Positive	Positive	Neutral	Neutral	Neutral
Transmit Security	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for each 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
Akamai	Positive	Strong Positive	Strong Positive	Strong Positive
Arkose Labs	Positive	Positive	Positive	Positive
BioCatch	Strong Positive	Positive	Positive	Positive
Broadcom	Positive	Strong Positive	Strong Positive	Strong Positive
Experian	Strong Positive	Strong Positive	Strong Positive	Strong Positive
F5	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Forter	Positive	Strong Positive	Positive	Positive
GBG	Neutral	Strong Positive	Positive	Positive
Group-IB	Strong Positive	Positive	Neutral	Positive
Gurucul	Neutral	Positive	Positive	Neutral
HID Global	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Human	Positive	Strong Positive	Strong Positive	Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive
ID Dataweb	Strong Positive	Neutral	Neutral	Neutral
LexisNexis Risk Solutions	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Outseer	Positive	Strong Positive	Strong Positive	Strong Positive
Sift	Positive	Strong Positive	Positive	Positive
Transmit Security	Strong Positive	Positive	Positive	Strong Positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For some of the products there are additional KuppingerCole 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 Fraud Reduction Intelligence Platforms, we look at the following six categories:

- **ID Proofing & AO Protection** - 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. **ID Proofing is a primary means of reducing Account Opening Fraud and is a regulatory requirement in financial use cases in many jurisdictions.**

- **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, payees, exceptions for known travel, and user profile changes. **UBA is a key method for preventing ATO fraud.**

- **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, both internal and external. Some of the vendors examined below provide these functions to other FRIP vendors. **Device Intelligence is a key method for preventing ATO fraud and a contributing element to preventing AO fraud.**

- **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. **Behavioral Biometrics is a key method for preventing ATO fraud and a secondary means for preventing AO fraud in some use cases. Behavioral biometrics is generally instrumental for detecting bots.**

- **Bot Detection/Management** - This category considers the ability of vendor solutions to analyze traffic in real-time to accurately identify whether it is initiated by legitimate users or bots. In many cases, bots are detected through behavioral biometrics, but some services utilize overt methods that require end user interaction, activity signatures, cyber threat intelligence, and manual analysis. Bot Management addresses how the vendor services aid customers in handling bots. Common options are challenging, redirection, and throttling. Many of the fraud types experienced by website operators (as described in chapter 1) are perpetrated by bots. **Bot Detection and Management can help prevent automated ATO and AO fraud attempts.**

- **ATO Protection** - This category combines all the available information to represent the combined abilities of each solution to prevent ATO fraud, including credential and device intelligence, UBA, behavioral biometrics, and bot detection.

- **Ecommerce Support** - This rubric measures each vendor service with regard to how it protects against the many types of fraud and attacks experienced by ecommerce platforms, online businesses, and website operators in general, which is distinguished from the fraud protection functions offered for financial institutions described below. Examples of the types of fraud addressed here include API abuse, policy abuse, inventory checking and hoarding, fake goods/postings/reviews/comments, headless browsers, malvertising, social media bots, account creation and credential stuffing bots, ticket scalping, malicious overlay apps, SEO poisoning, gift card cracking, etc. Most of these fraud types are instigated by bots.

- **Finance & Payments Support** - This metric considers each vendor solution's capabilities in AML, KYC, OFAC, PEP, other sanctions list validation, EU PSD2, and 3DS2.x compliance, as well as detecting mule accounts, payments fraud, and fraud against banks and card issuers (including Card Not Present and detection of stolen or counterfeit cards).

Akamai – Account Protector, Bot Manager, and Page Integrity Manager

Akamai Technologies is a cloud and security provider headquartered in Cambridge, Massachusetts, USA. Founded in 1998, the company is one of the veteran players in the market, providing a broad range of security, compute, and delivery solutions through its Akamai Connected Cloud, one of the world's largest distributed edge and cloud platforms. For FRIP, the Akamai offering is composed of the above listed services, which address the device intelligence, user behavioral analysis, behavioral biometrics, and bot detection and management components. The services are run from their own facilities and public IaaS providers across global data centers. Costs are based on traffic volumes for web application security products with zero overage fixed fees. Customer applications call Akamai services via the REST API, and JSON formats are supported.

Akamai's suite of services is focused on ATO prevention and does not have specific features for financial regulatory compliance such as AML, KYC, OFAC, PEP, 3DS2, or PSD2. There are neither built-in identity proofing functions nor connectors to 3rd-party identity proofing services. Akamai does not gather or evaluate compromised credential intelligence. User behavioral analysis is limited to basic ATO detection without transaction-level awareness.

For device intelligence, Akamai collects a wide range of attributes but omits device health checks. Akamai deploys JavaScript and SDKs for behavioral biometrics, but only evaluates a limited set of such attributes. ML-enhanced detection models are used to discover anomalies, fraudulent user and device behavior, and bots. Akamai Bot Manager has extensive bot detection and management capabilities addressing the majority of fraud types affecting website operators. Bot Manager allows customer configurable granular responses ranging from allow/deny-listing, throttling, redirection, and challenging.

Call center integration is not currently possible. Case management and ITSM integration are not present within the Akamai solutions. Akamai's Data Science Operations team can assist customers with changing the weighting of risk factors. The customer admin interface enables simulating the effects of changes to policies. Risk evaluation results cannot be packaged in SAML, OAuth2, or JWT. Customer dashboards are intuitive and provide detailed information and can be configured as needed.

Akamai services are highly scalable and globally distributed. Their CDN components are SOC 2 Type 2 and US FedRAMP Moderate certified. Their solution is geared toward ATO and bot perpetrated fraud types rather than Account Opening and advanced financial and payment industry use cases. Organizations looking for robust bot and ATO protection, especially existing customers of Akamai's other services, should consider Akamai's suite of fraud reduction solutions.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Neutral
Usability	Positive

Table 3: Akamai's rating

Strengths

- Fixed fee based on traffic volumes with zero overage protection cost model.
- Advanced bot management capabilities are present.
- Good support for preventing many common fraud types experienced by website operators.
- Excellent customer administrator/analyst interface

Challenges

- No identity proofing capabilities or connectors.
- Does not perform Device Posture Checks.
- Modifying risk factor weighting requires Akamai support.
- No call center or ITSM integration

Leader in

AKAMAI
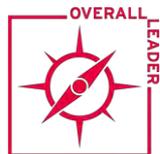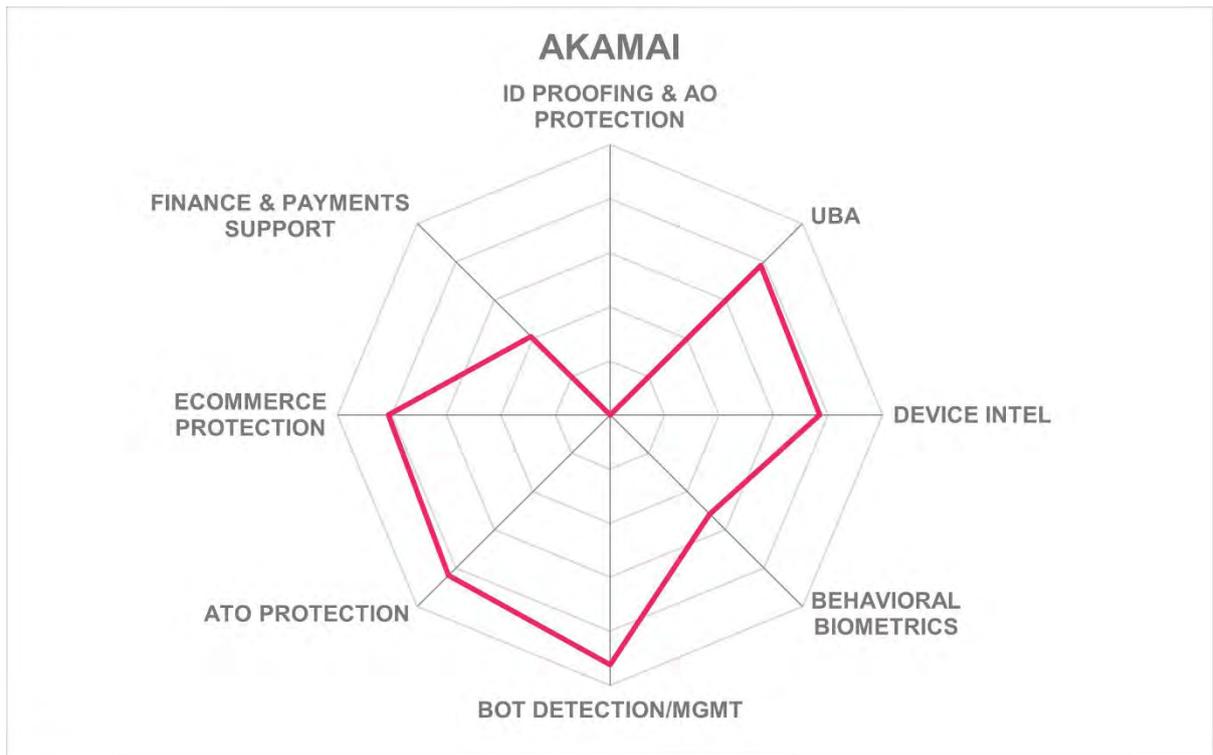
Arkose Labs – Arkose Bot Manager

Arkose Labs is a mid-stage startup established in 2017 in San Francisco. Their solution is focused on reduction of ATO fraud, covering many finance, retail, gaming, etc. use cases, as well as inventory hoarding, screen scraping, loyalty card abuse, and fake reviews. Of the six core functional areas of FRIP, Arkose Labs has credential and device intelligence, user behavioral analysis, behavioral biometrics, and bot detection. The service is hosted in public IaaS in data centers around the globe. Customer applications connect to Arkose Bot Manager via the REST API. Key exchange and SAML are supported for API authentication. The pricing model is based on per-transaction rates.

Arkose does not support AML, KYC, OFAC, or PEP compliance. Arkose can work with merchants for 3DS2 and PSD2, but this is not a primary focus. Their solution does not provide identity proofing or integrate with other identity proofing services. It does evaluate in-network credential intelligence. Arkose Email Intelligence helps deter AO and ATO attempts by leveraging partner information about the trustworthiness and risk levels of consumer email addresses. The UBA functions are constrained to login/transaction times and frequencies but not transaction types/amounts.

Device intelligence functions in Arkose Bot Manager include device type, custom fingerprinting techniques, various external IP reputation sources, and computation of geo-velocity. Device health is not assessed and malware behavior on end user device is not detected. Arkose Labs' behavioral biometrics implementation considers gyroscopic analysis from mobiles, and it uses JavaScript to pull keyboard/mouse/touchscreen interaction characteristics. Mobile environmental attributes are not currently evaluated. Arkose uses its behavioral biometrics and 3rd-party intelligence sources for bot detection, and it has advanced bot handling functions including redirection, throttling, and highly innovative and user-friendly CAPTCHA and proof-of-action challenges. Arkose can detect and handle a large subset of ecommerce fraud types, including inventory checking and hoarding, price checking bots, headless browsers, fake reviews/comments, social media bots, account creation and credential stuffing bots, ticket scalping, and gift card cracking. Customers can work with Arkose Labs Technical Account Managers to create detailed policies for advanced bot management.

Arkose Bot Manager does not integrate with call center systems. The risk analysis engine outputs risk scores, risk bands, and/or 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. Customers would need to configure connectors to their ITSM and SIEM systems if desired.

Arkose Labs is ISO 27001, 27002, 27018, and SOC 2 Type 2 certified. Arkose is unique in offering an SLA for 100% remediation of automated attacks and $1M credential stuffing attack prevention warranties. The solution is specialized for ATO prevention and bot detection and management. Connections for ID proofing, and additional functions in the areas of UBA, device intel, and behavioral biometrics would strengthen the offering.

Organizations looking for ATO protection and strong bot management should consider Arkose Bot Manager.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Positive
Usability	Strong Positive

Table 4: Arkose Labs' rating

Strengths

- User-friendly CAPTCHAs and proof-of-action challenges
- Good bot detection and advanced bot management capabilities
- SLA guaranteeing 100% remediation of automated attacks.
- $1M warranty against credential stuffing attacks
- Many relevant security certifications

Challenges

- No identity proofing integrations
- Additional device intelligence attributes should be evaluated by the risk engine.
- UBA and behavioral biometrics functions could be expanded.
- Policy creation and maintenance currently requires vendor assistance.

Leader in

ARKOSE LABS
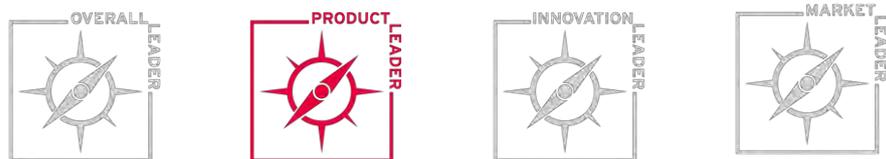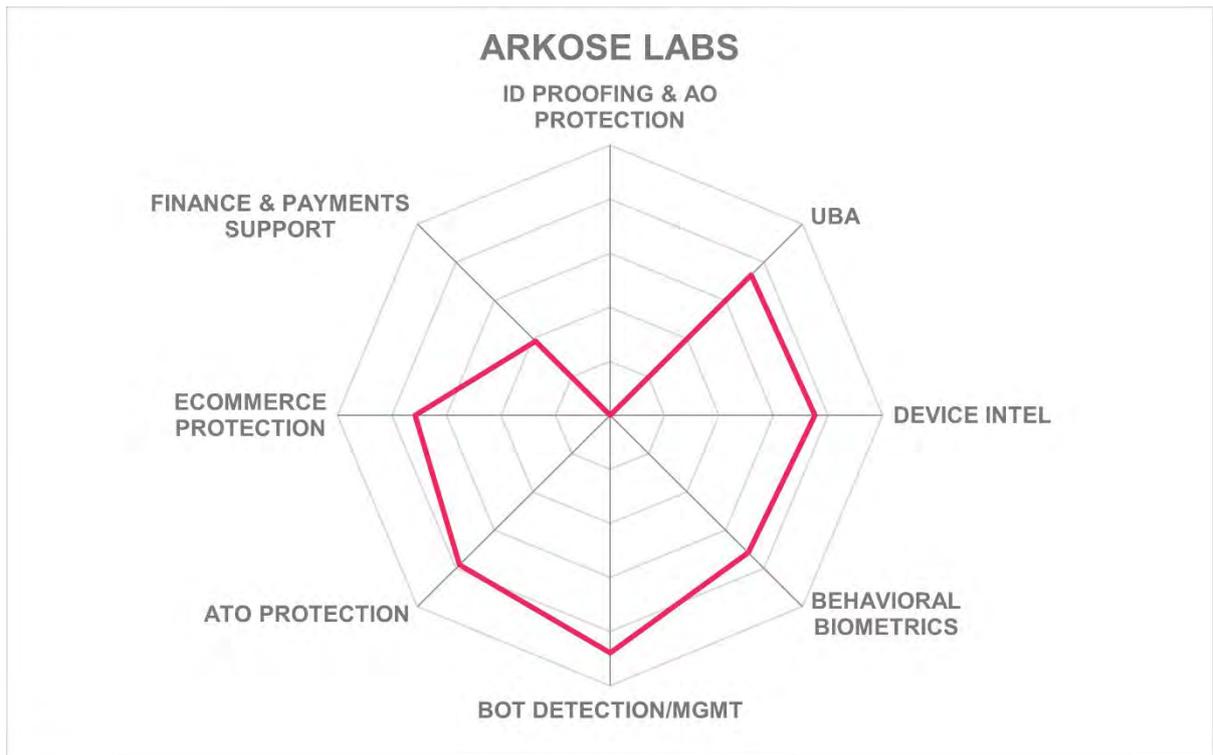
BioCatch – Platform

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. Their suite is composed of modules handling Account Opening Fraud Protection, Account Takeover Fraud Protection, Social Engineering Fraud Detection, Mule Account Detection, Phishing Site Detection, and PSD2/SCA compliance. Of the six pillars of FRIP, BioCatch has identity proofing, device intelligence, behavioral biometrics, and bot detection. Their service is hosted in multiple Microsoft Azure locations across the EU and APAC regions. Subscriptions are priced per-user for ATO, Social Engineering, Mule Account, and Phishing Site Detection; and per-transaction for AO Protection and PSD2/SCA services.

BioCatch has some features for AML, KYC, and Mule Account Detection, and these can be extended with the BioCatch Rule Manager for OFAC and PEP checks. These functions comprise their identity proofing capabilities. No integrations for 3rd-party ID proofing services are available. The solution does not collect or evaluate compromised credential intelligence. SCA for PSD2 and 3DS2 are supported via the behavioral biometric functions. BioCatch can also detect CNP and counterfeit cards. This solution provides support for a subset of the website operator fraud protection use cases described in the introduction.

BioCatch uses JavaScript and mobile SDKs for collecting device intelligence and behavioral biometrics. Device intelligence parameters that are analyzed include geo-location (and geo-velocity); IP and reputation; device ID, type, fingerprint, and reputation; and device health checks; and SIM card properties. Behavioral biometrics are the foundation of BioCatch's integrated suite of services, and as such it can look at all available parameters. The platform performs cognitive analysis to discover behavioral anomalies and criminal intent indicators including low familiarity with subject PII, high application fluency, excessive deleting, copy/paste activity, etc. The platform performs full UBA including transaction level analysis and it can take known travel into account. Behavioral analysis also enables malware detection. BioCatch has advanced bot detection through its behavioral biometrics. BioCatch deploys Invisible Challenges that fool bots but are unobtrusive to real users. Of the list of ecommerce fraud types, BioCatch can detect headless browsers, account creation and credential stuffing bots, Buy Now Pay Later fraud, and Authorized Push Payment fraud. Customers decide how to handle detected bot activities independently.

BioCatch outputs detailed transaction risk analyses enabling customers to build granular rules. Customers access this information and conduct investigations in the BioCatch Analyst Station. REST APIs allow integration with customer applications. JWT, HTTP basic authentication, and mutual TLS are the available API authentication methods. SAML, OAuth2, and OIDC are not supported. Call center integration is not currently offered but is on the roadmap. Customers manage fraud cases in the provided BioCatch Case Management component, integration with customer ITSM systems is not available. Dashboards are visible within the Case Management application. BioCatch has dedicated threat analysts assigned to each customer to extend and customize reports as needed.

BioCatch is ISO 27001 and SSAE SOC 2 Type 2 certified. The solution is currently built on a single IaaS provider, but multi-cloud support is planned. The company specializes in financial

use cases. BioCatch has excellent behavioral biometrics which form the basis of their FRIP. The advanced cognitive analytics are highly innovative. Plans are in work to add functionality to address the gaps mentioned above. Organizations across the finance sector looking to reduce fraud should consider BioCatch's range of services.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Neutral
Usability	Strong Positive

Table 5: BioCatch's rating

Strengths

- Thorough implementation of behavioral biometrics
- Advanced cognitive analysis for reducing AO fraud.
- Built-in case management and fraud analyst workstation
- Transaction details analysis
- Mule Account Detection
- Social Engineering Detection
- PSD2 and 3DS2 compliance support

Challenges

- SDK does not allow remote ID proofing or document verification.
- 3rd-party ID proofing integrations not available
- Compromised credential intelligence not collected or considered.
- Ability to detect additional ecommerce fraud types would be beneficial.
- Call center integration is on the roadmap.
- No support for 3rd-party ITSM systems.

Leader in

![kuppingercole ANALYSTS logo]

BIOCATCH radar chart with axes: ID PROOFING & AO PROTECTION, UBA, DEVICE INTEL, BEHAVIORAL BIOMETRICS, BOT DETECTION/MGMT, ATO PROTECTION, ECOMMERCE PROTECTION, FINANCE & PAYMENTS SUPPORT
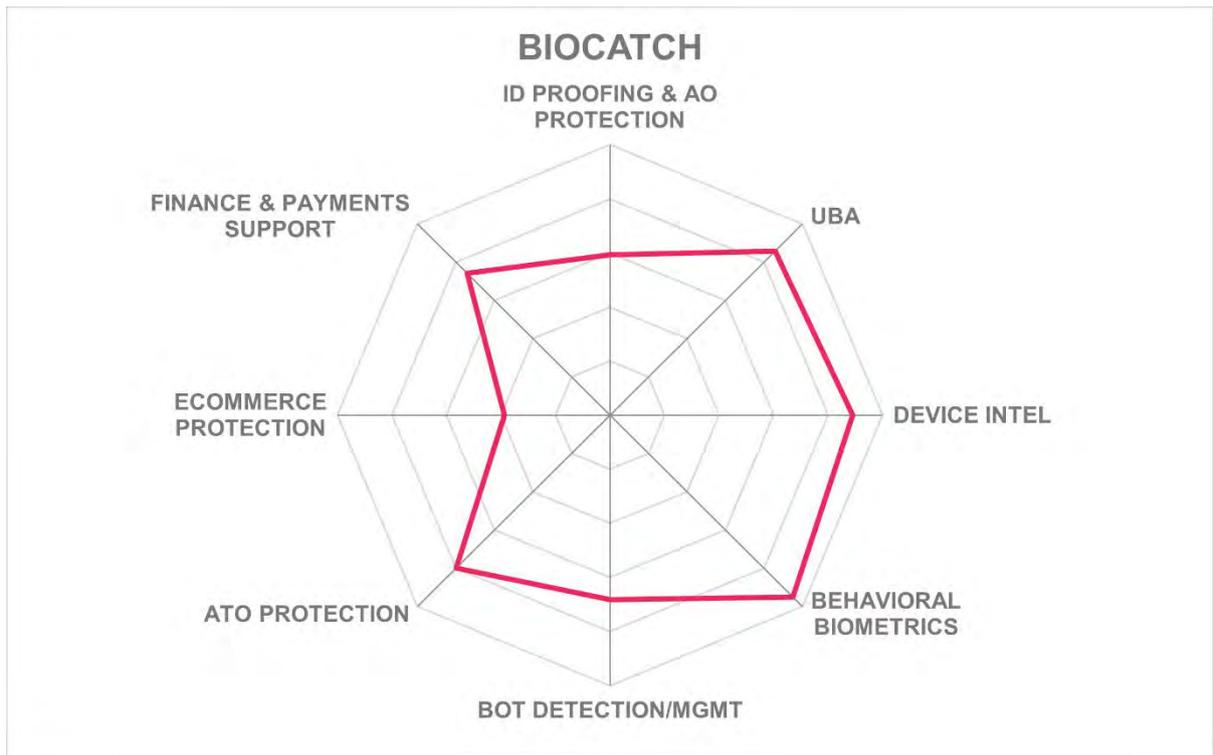
Broadcom – Arcot Network for Issuers

Broadcom's entry in this market originated with Arcot Systems, a 3DS pioneer acquired by CA Technologies in 2010. Arcot was founded in 1997 in the Bay Area of California. The Arcot Network for Issuers solution offering is heavily used by credit card issuers, processors, merchants, and banks. Broadcom has a wide range of IT hardware and software products and services, with many in the cybersecurity and identity management areas. Broadcom Arcot Network for Issuers has functionality in UBA, device intel, credential intelligence, and limited behavioral biometrics and bot detection. Arcot Network for Issuers is a SaaS that is hosted in Broadcom facilities and in one IaaS provider in the US. Service pricing is either on a per-transaction or fixed cost basis.

Arcot specializes in 3DS2.x and PSD2 compliance and CNP fraud detection, but does not have AML, KYC, OFAC, or PEP compliance support. Arcot does not perform identity proofing, nor does it offer integration with 3rd-party ID proofing services. It does leverage in-network compromised credential intelligence.

Arcot has comprehensive device intelligence capabilities, examining IP reputation, device ID/type/fingerprint/history and security posture. The solution performs detailed user behavioral and transaction analysis, such as user-merchant association, time and day patterns, location patterns, etc. Multiple ML detection models are employed. Behavioral biometrics from specialist 3rd-party providers can be integrated for customers, many of which do have these in place for other digital service channels. While the base solution doesn't include such capabilities, it does provide Behavioral Analytics capabilities, a form of inherence which is accepted by some regulators based on transaction profiling. Bot detection is not featured, but some bots can be detected by IP addresses and insights from their UBA.

Arcot has integration with customer communications solutions such as FICO. Customers connect the apps via GraphQL, REST, SOAP, or WebAuthn APIs. Arcot APIs support multiple secure authentication methods including JWT, key exchange, mutual TLS, OAuth2, OIDC, and SAML. The risk engine output is granular and configurable by customers. Action recommendations provided to customers are allow, deny, log, alert, and step-up, with reason codes. Customer organizations can integrate Arcot with their ITSM systems, but no specific connectors are provided. Arcot provides case management within their interface. Many reports are available through the customer console, including admin activities, organization level summaries, risk advice summaries, rule configurations, and case activities. Report customization is not supported; instead, most customers extract this data via APIs and use 3rd-party tools for analysis.

Broadcom is EMV 3DS 2.1/2.2, PCI-DSS, and SSAE 18 SOC 2 Type 2 certified. The solution is scalable. As a solution focused on e-commerce card payment authentication and fraud prevention, it lacks identity proofing, AML/KYC/OFAC/PEP compliance, advanced behavioral biometrics, bot detection, and most website operator fraud protection functions. Arcot has significant clout in the areas of device intelligence, user behavioral analysis, transaction analysis, and its ML-enhanced risk analysis engine. Arcot offers a compelling mix of fraud reduction features for the finance and payments industries.

Security	Strong Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Strong Positive
Usability	Strong Positive

Table 6: Broadcom's rating

Strengths

- Thorough user behavioral analysis, including transaction details and history.
- Excellent device intelligence capabilities
- Advanced ML detection models employed.
- 3DS 2.1 and 2.2 certified
- Fixed cost plans available.
- Support for WebAuthn and GraphQL

Challenges

- Customer analyst interface needs to be updated.
- Report customization not available; data must be pulled via API and analyzed separately.
- Missing identity proofing and AML/KYC/OFAC/PEP compliance
- No built-in behavioral biometrics, but 3rd-party solutions can be utilized.
- Limited bot detection; no bot management
- Lacks support for most website operator fraud types outside of financial use cases.

Leader in

BROADCOM radar chart showing ID PROOFING & AO PROTECTION, UBA, DEVICE INTEL, BEHAVIORAL BIOMETRICS, BOT DETECTION/MGMT, ATO PROTECTION, ECOMMERCE PROTECTION, FINANCE & PAYMENTS SUPPORT
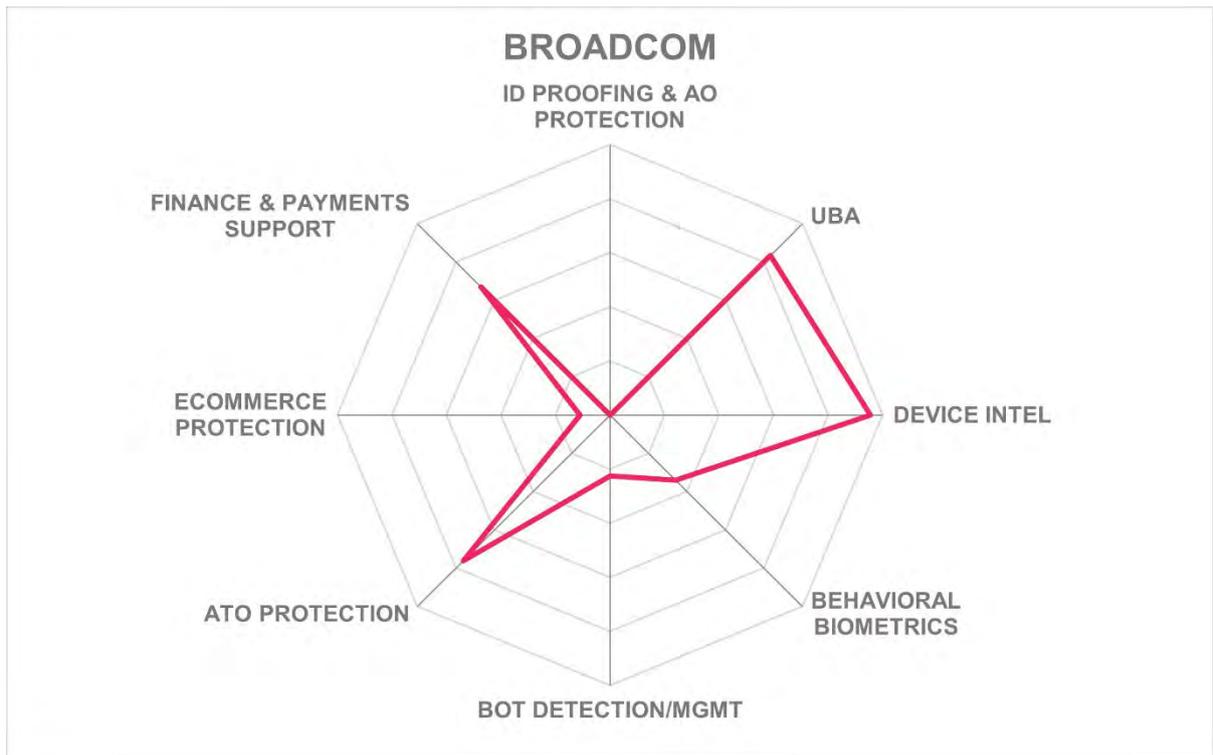
Experian – CrossCore

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. 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-user and/or transaction per time period and by the types of fraud covered.

Experian supports AML, KYC, OFAC, PEP, sanctions lists, SIE/SIP/RCA validation and compliance, and mule account detection. In the realm of payments security, Experian facilitates 3DS2.x and PSD2 compliance; moreover, CrossCore can detect CNP and stolen/counterfeit credit card usage. 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 BioCatch, Boku, Daon, Ekata, eMailage, FacePhi, GBG, GDC, ID.me, IDfy, LexisNexis, Mitek, OnFido, Prove, and RapidID. Customers sign addenda to their agreements with Experian to get access to these partner services. Compromised Credential Intelligence is not present but planned.

For device intelligence, CrossCore looks at geo-location, geo-velocity, device fingerprint/ID/type, and device and IP reputations. Device intelligence evaluations are based on rules and deny lists. Device health assessments and malware detection are indirect. CrossCore's UBA functions leverage multiple ML detection models to evaluate login patterns and profile changes but not device intel or transaction details. Behavioral biometrics are provided via partnership with a leader vendor and include all expected modalities plus advanced cognitive analysis and invisible challenges which obviate the need for CAPTCHAs. Behavioral biometrics also provide CrossCore's bot detection functions. Bot management is limited, but CrossCore can detect and alert customers to many major website operator fraud types.

Call center integration and SIM swap detection capabilities can be added via Experian partners. REST APIs enable customer application integration, and these APIs are secured by strong authentication mechanisms. ITSM integration is not supported. CrossCore has a modern admin interface that allows customers to select intel sources for evaluation and set weights per attribute for the risk evaluation processes. Analysts use FraudNet and the Hunter application for investigations. Experian provides many BI and fraud reports.

Experian's CrossCore is very 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 worldwide as an

authoritative attribute provider. CrossCore's technical capabilities for fraud reduction are well-suited for detecting AO and ATO fraud as well as some types of fraud against websites. Beyond their native identity proofing, device intelligence, and transactional risk analysis capabilities, through partnerships, they add strong features in document verification, behavioral biometrics, and bot detection. Once again, Experian is a Leader in Fraud Reduction Intelligence Platforms. Any organizations looking for a full-featured FRIP service with global support should consider Experian CrossCore.

|	
Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 7: Experian's rating

Strengths

- Comprehensive identity proofing capabilities, including remote document verification
- Authoritative attribute provider for many partners and government agencies
- Widest variety of sanctions list validation features
- Numerous partners for identity and device attributes
- Ideally positioned to detect AO fraud.
- Supports detection and alerting on many of the major types of fraud that impact website operators.
- Easily configurable policy and decisioning engine
- Massive scalability; data centers across six continents

Challenges

- Compromised Credential Intelligence is not present but is in work.
- Does not evaluate SIM for device intelligence.
- Device intel and some UBA functions do not leverage ML-enhanced detection models.
- Coarse-grained UBA does not consider transaction details.
- Webhooks and WebAuthn APIs not supported.

Leader in

EXPERIAN
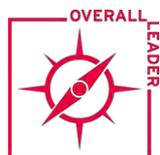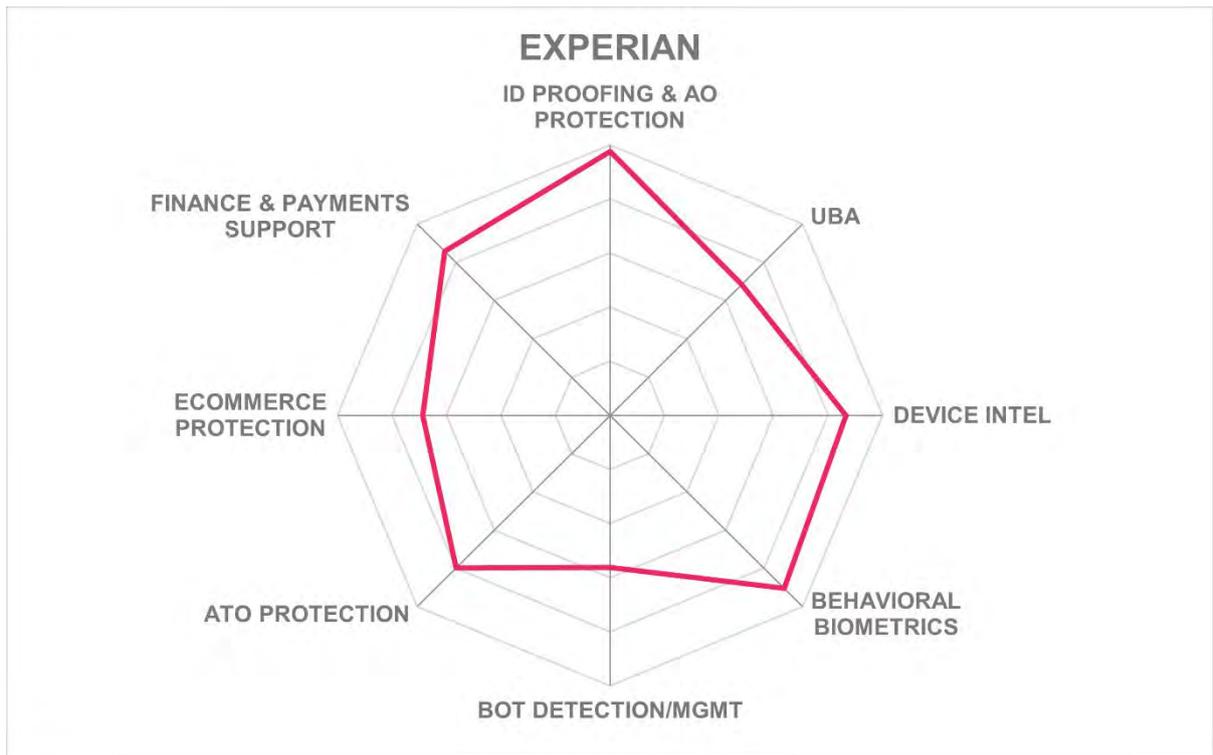
F5 – Distributed Cloud

F5 is a leading network application delivery and security provider headquartered in Seattle. F5's entry in FRIP is largely based on Shape Security's tools which they acquired in 2020. F5's portfolio includes BIG-IP, DDoS Hybrid Defender, and NGINX. For fraud prevention, their components described here include F5 Distributed Cloud Bot Defense, Account Protection, Authentication Intelligence, Data Intelligence, Aggregator Management, Client-Side Defense, and Malicious Activity Detection. Their products cover credential and device intelligence, UBA, and bot detection & management. These services are hosted in their own facilities and public IaaS providers across North America, APAC, and EU locations. Licensing models are per-transaction / per-application with volume discounts available.

F5 Distributed Cloud supports PSD2 SCA, CNP and carding fraud detection. F5 does not offer identity proofing, but customers could configure connections to 3rd-party services via APIs. In-network credential intelligence is used.

Distributed Cloud makes use of a good range of device intelligence factors including geo-location and geo-velocity; IP address and reputation; device type, fingerprint, hygiene, and reputation. It can infer the presence of various types of malware on devices as well. For UBA, this solution examines all pertinent attributes including transaction types, amounts, and histories. JavaScript collects keystroke/mouse/swipe characteristics, gyroscopic, and network data. All these analysis techniques leverage advanced ML detection models. F5 Distributed Cloud has sophisticated bot detection and management, giving customers the ability to choose how to handle the various bot types encountered such as inventory checking/hoarding, price checking/scraping, carding, policy abuse, refund abuse, and ticket scalping. Distributed Cloud Client-Side Defense protects against MageCart, form-jacking, skimming, PII harvesting, and other critical security vulnerabilities.

While the risk engine is granular, F5 professional services can be engaged to provide around the clock monitoring and, if needed, to make attribute weighting and authentication policy changes on behalf of clients. Customers connect their applications via REST API; webhooks and WebAuthn are not supported. API authentication methods are JWT and SAML. Integration with customers' ITSM systems is not supported. Call center integration is not offered. F5 Distributed Cloud has customer dashboards and reports that provide all expected basic reports and are further customizable.

F5 Distributed Cloud is ISO 27001, PCI-DSS, and SSAE 18 SOC 2 Type 2 certified. Distributed Cloud does not have identity proofing capabilities, but F5 offers pre-built connectors for 3rd-party services such as Amazon CloudFront. The solution has advanced device intelligence and behavioral biometrics. F5 has compelling bot detection and management features that are especially relevant for payments, retail, and entertainment industries. Any organization looking for FRIP services, especially those that are already using other F5 products and services, will want to consider these F5 Distributed Cloud components.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 8: F5's rating

Strengths

- Highly scalable, low latency services
- Utilizes granular device intelligence.
- Sophisticated behavioral biometrics
- Advanced bot detection and management
- Client-Side Defense protects against many forms of fraud that confront web properties, especially ecommerce vendors.
- Supports CNP and carding fraud detection.
- Many relevant service certifications
- Intuitive dashboards and fraud analyst interface.

Challenges

- Identity proofing capabilities not present.
- No call center or ITSM integration
- 99.9% uptime guarantee is comparatively low.
- Policy changes require engaging F5 professional services.

Leader in

F5
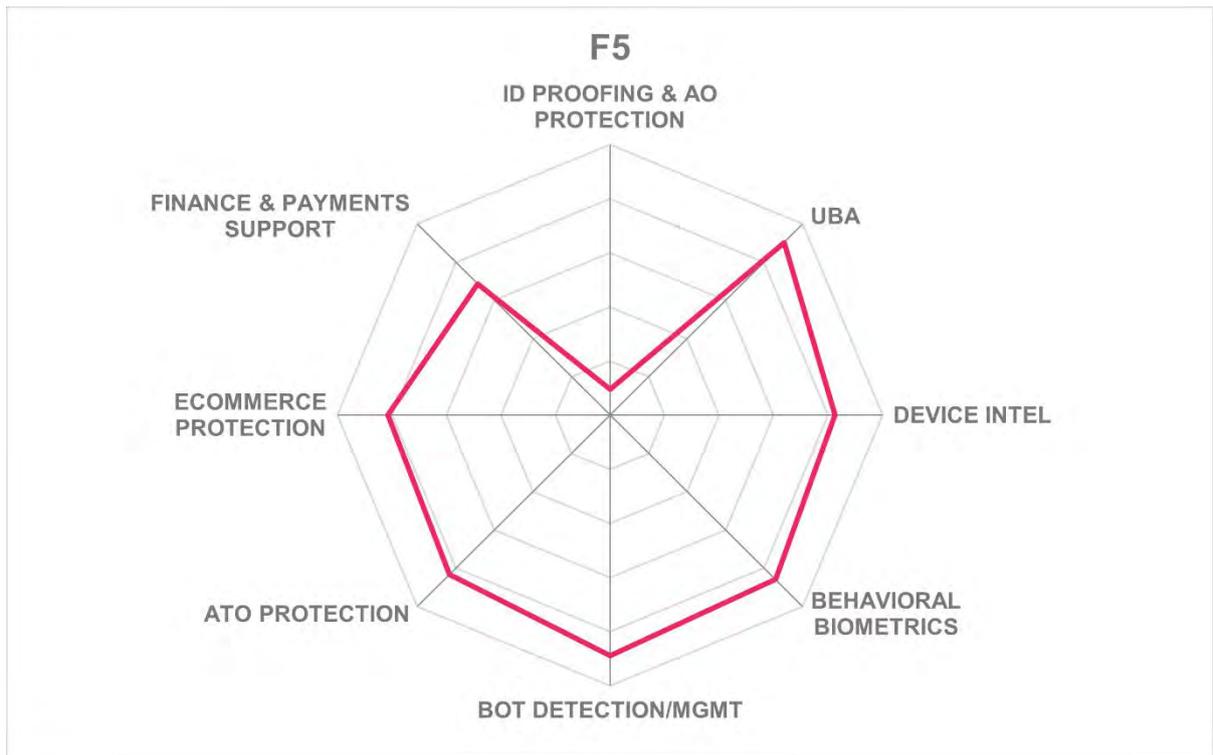
Forter – Trust Platform

Forter, founded in 2013 and headquartered in New York, is a late-stage venture-backed fraud prevention specialist. The Forter Trust Platform is a suite composed of modules for improving customer conversions, reducing false declines, detecting policy abuse and adjusting policies, payments security, and ATO prevention. FRIP components present in the platform include credential intelligence, device intelligence, UBA, and bot detection and management. Their services are hosted across US and EU data centers. Forter Trust Platform is integrated into some major ecommerce and payment service provider platforms in the US. Pricing for services is based on transaction volumes.

Forter Trust Platform assists with AML, mule account detection, KYC, and 3DS2.x and PSD2 compliance. The solution does not have built-in identity proofing functions, but customers can contract with identity proofing services and the Trust Platform can be configured to evaluate that input. Forter uses credential intelligence from in-house and external consortia sources.

Forter Trust Platform has access to a wide range of device intelligence attributes including geo-location and geo-velocity; device type, ID/fingerprint, and hygiene; and IP address and reputation. It does not detect malware behavior on devices, however. Forter Trust Platform analyzes a large number of user behavior data points as well as transaction level details. Forter Trust Platform's real-time UBA and device analysis is powered by ML detection models. Behavioral biometrics are not part of the solution today. It detects bots by UBA and activity signature matching. Customers often pair Forter Trust Platform with 3rd-party bot detection and management services. The solution helps prevent many forms of fraud against websites and policy abuses such as payment skimmer code, inventory hoarding, price checking, returns and item not received, headless browser operations, fake reviews and comments, malicious ad insertions, credential stuffing, fake product listings, Buy Now Pay Later, and authorized push payments. For policy abuse cases, the solution can modify policies for individual accounts, for example, revoking returns privileges.

Fraud teams, call center staff, and other support roles use their portal to drill down into details as to why transactions are rejected, but telecom/network operator information is not integrated. Forter Trust Platform applies policies for customers; it can import customer written rules and policies, but this is not standard and is not recommended. It is a decisioning engine, thus it does not output risk scores or reason codes. REST API and Webhooks are supported. Basic authentication and SAML used for customer API connectivity. Case management is provided within the portal. No connectors for ITSM systems are available. Customer analysts can drill down into transaction analysis from the dashboard, which is easily customized if needed.

Forter Trust Platform is ISO 27001, PCI-DSS, and SOC 2 Type 2 certified. It has one of the highest SLAs in the field. Forter is US based but serves EU customers with PSD2 requirements. Their Trust Platform addresses many fraud reduction use cases specific to the ecommerce and payments industries and provides sophisticated remediation capabilities for policy abuse. Organizations in these targeted sectors which need FRIP services should consider Forter Trust Platform.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Neutral
Usability	Positive

Table 9: Forter's rating

Strengths

- Integrated directly into major ecommerce and payment service provider platforms.
- Protects against many fraud types affecting website operators as well as policy abuse.
- Ability to programmatically modify policies at the individual consumer level for cases of returns and item not received abuse.
- Very high availability SLA of 99.995%
- Straightforward pricing model

Challenges

- No built-in identity proofing, but customers can connect service providers through their APIs.
- Does not detect malware on devices.
- No behavioral biometrics
- Additional API authentication mechanisms would be beneficial.
- Risk engine is not customer configurable.
- No ITSM integration

Leader in

FORTER
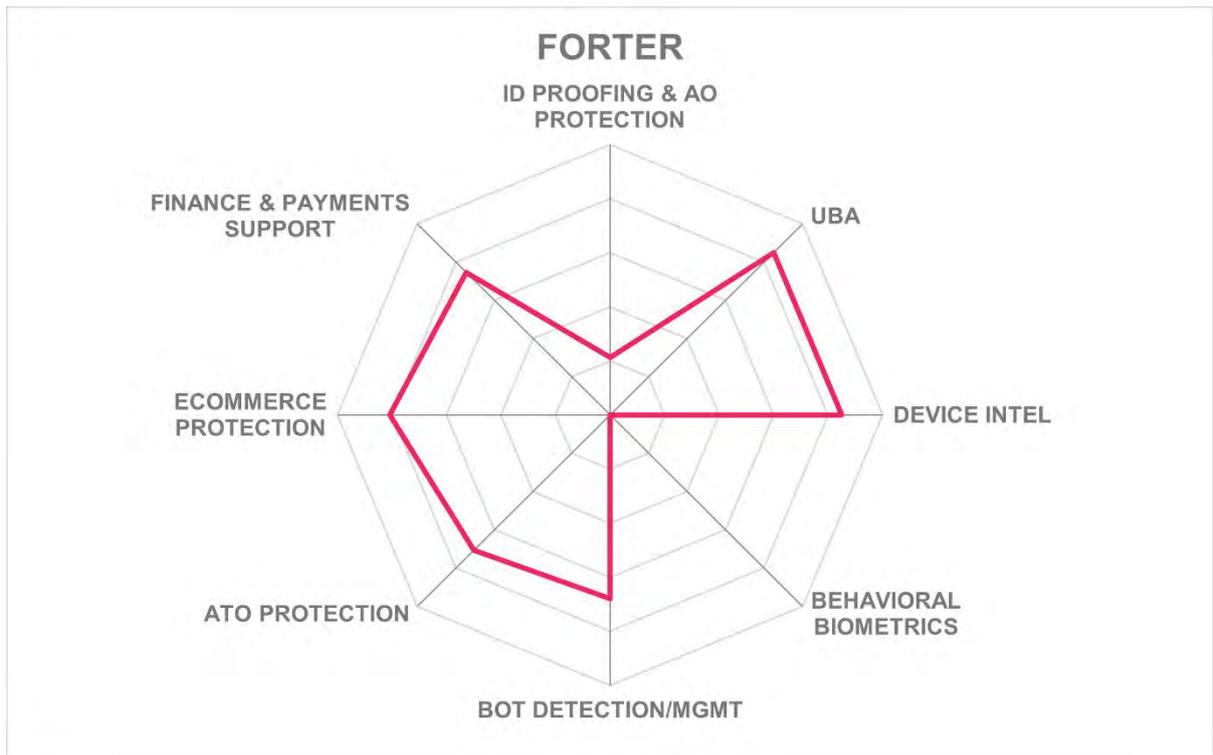
GBG – Fraud and Compliance Solution

GBG is headquartered in Chester, UK, and was founded in 1989. GBG is a fraud prevention specialist. In 2019, they acquired IDology, and in 2021 they acquired Acuant. GBG's suite of solutions has strong identity verification functionality and UBA, with credential intelligence, device intelligence, and behavioral biometrics capabilities coming from partners. The company is focused on the finance and gaming industries. GBG's solution is hosted by customers either on-premises or in public or private cloud providers, and is also available as SaaS. The Fraud & Compliance Solution includes the Instinct, Predator & Next Generation Financial crime Studio, Compliance Platform, and ExpectID). Costs are calculated per-user or per-transaction.

GBG has extensive identity verification features with links to many authoritative attribute sources. GBG also interoperates with Equifax, Experian, Jumio, and Prove. A mobile identity and document verification app enables remote onboarding and customer due diligence. GBG facilitates age verification, AML, KYC, mule account detection, and OFAC/PEP/Sanctions screening. It does not specifically address 3DS2 or PSD2. GBG can detect Card Not Present and counterfeit/stolen card fraud. Credential intelligence comprises in-network and external ID reputation sources.

IP address, geo-location, geo-velocity, and device ID/fingerprint are analyzed. Other device intelligence and extensive behavioral biometrics may be provided via partner solutions. GBG performs user behavioral analysis, which includes looking at transaction amounts, frequency, and patterns. Their platform can receive and process external sources of user data as well. Some types of bots that impact ecommerce platforms can be detected by their GeoTrace service, which relies upon IP reputation.

Customers can create and modify policies via an intuitive flow-chart style interface. Customer fraud analysts can easily drill down into details and history for investigations. Many reports are present out-of-the-box, and customers can define new report types as needed. Full case management is available, but there is no integration with external ITSM systems. GraphQL, Kafka, MQ, REST, and SOAP APIs are available for customer application integration, which can be secured with JWT or SAML authentication. Caller name and phone number matching, account longevity, account status, and SIM swap detection risk information can be passed on to customers' call center software.

GBG is a provider of identity verification services to other FRIP solutions. GBG is ISO 27001 and PCI-DSS certified. GBG has deep identity verification services, including a remote onboarding / mobile document verification app, and leverages partnerships for other key parts of their FRIP offering. Bot detection could be enhanced by additional intelligence sources and evaluation methods. The solution is primarily customer-hosted and not a SaaS. Their target markets are finance and gaming. Organizations in those industries that need FRIP solutions focused on identity proofing for AML, KYC, and sanctions screening should take a look at GBG's Fraud and Compliance Solution.

Security	Neutral
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 10: GBG's rating

Strengths

- Excellent identity verification features
- Mobile identity and document verification app for remote onboarding and KYC
- Extensive screening for AML, mule accounts, and OFAC/PEP/sanctions
- Easy-to-use policy authoring and investigative interfaces

Challenges

- Lacks behavioral biometrics.
- Though focused on finance, it does not have specific support for 3DS2 or PSD2.
- No ITSM integration

Leader in

GBG
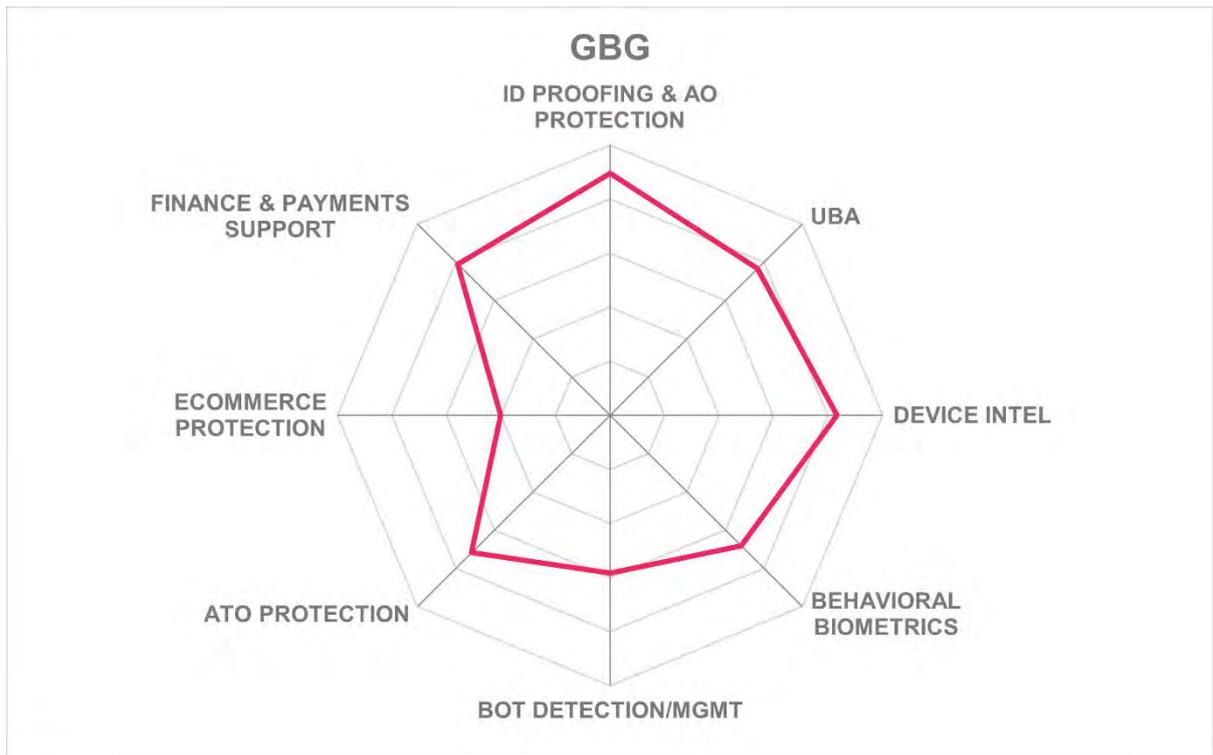
Group-IB – Fraud Protection

Privately held Group-IB was founded in 2003 and their global HQ is located in Singapore. Beyond FRIP services, Group-IB offers threat intelligence, Attack Surface Management, business email protection, and anti-piracy products. Group-IB Fraud Protection has functionality in compromised credential and device intelligence, UBA, behavioral biometrics, and bot detection. Their services are hosted in their own facilities and a public IaaS provider in the APAC, EU, and NA 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, with per-transaction fees for PSD2 and 3DS2.

Group-IB partners with Sumsub to provide built-in identity proofing, remote onboarding and legal document verification integration with their platform. Customers can also utilize their services with customization to aid in AML, KYC, mule account detection, OFAC, PEP, PSD2, and 3DS2 compliance. For payments clients, Group-IB Fraud Protection can detect CNP, Card Not Received/Stolen Cards, and counterfeit cards. Group-IB leverages in-network compromised credential intelligence for the benefit of all their customers.

Group-IB Fraud Protection has comprehensive device intelligence capabilities via their SDK and JavaScript. Attributes evaluated include IP addresses and reputations, geo-location and geo-velocity, device fingerprint/ID/type, device security posture and reputation, and IMEI/SIM card info. For user behavioral analysis, this solution can consider (if provided via API from customer applications) all pertinent data points including transaction details such as amounts, payees, and patterns. The SDK also harvests behavioral biometrics, encompassing all expected characteristics. Their solution can recognize user behavior across multiple devices as well as recognize multiple users per device.

UBA, behavioral biometrics, and traffic metadata are analyzed within the Fraud Protection Preventive Proxy, and the bot detection and management component. Bot management options are granular and can be configured by customers, providing options such as deny-list, allow-list, challenge, and redirect. This solution provides protection against most common ecommerce and web property operator fraud issues such as payment skimmers, inventory checking and hoarding bots, price checking bots, headless browsers, fake reviews and comments, fake posts and goods, social media bots, account creation and credential stuffing bots, gift card cracking, mobile malware, Buy Now Pay Later, and Authorized Push Payments.

Customers can determine storage periods for such data, and it can be depersonalized for privacy regulatory compliance. Multiple unsupervised and supervised ML algorithms are used with their detection models. Policies and weighting of attributes within policies are configurable by customers in an easy-to-use no-code interface. REST, Kafka, IBM MQ, and Rabbit MQ APIs are supported for customer integration. Several API authentication methods can be implemented. Case management is provided within their application, and there are no out-of-the-box connectors for 3rd-party ITSMs. Many reports are available within their console, and customers can create more or export data for analysis in other programs. Group-IB has recently added a fraud analysis dashboard, based upon their reverse engineering of many fraud types, which is arranged similarly to the familiar MITRE

ATT&CK™ matrix. Call center integration is available, complete with call-to-web session mapping and anti-smishing/vishing technology.

Group-IB asserts ISO 27001 and PCI-DSS certification. Group-IB Fraud Protection has advanced features in device intelligence, user behavioral analysis, behavioral biometrics, and bot management. The GUI is modern and easy for fraud analysts to use. Group-IB also has fraud analysts on their staff assigned to each customer. They do not cover North America at present. Support additional standards and connectivity for other IT and security systems would be beneficial for some customers. Organizations in the EMEA and APAC regions that need comprehensive FRIP capabilities should include Group-IB on their consideration shortlist.

|	
Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 11: Group-IB's rating

Strengths

- Extensive device intelligence capabilities
- Wide range of compliance regimes supported, from AML, KYC, OFAC, PEP, etc.
- Strong customer authentication for PSD2 and 3DS2
- Protection against CNP and stolen/counterfeit credit cards for payments service clients.
- Behavioral biometrics can recognize multiple users per device and single users across multiple devices.
- Multiple methods for bot detection and highly configurable bot management options
- Broad coverage of use cases for protecting ecommerce and other web operators
- Dashboard contains TTP matrix for various types of fraud campaigns

Challenges

- Identity proofing not built-in, but partnerships with 3rd-party services can be leveraged.
- Little or no sales or support for North America
- No ITSM connectors
- SLA and latency guarantees are comparatively weak.

Leader in

GROUP-IB
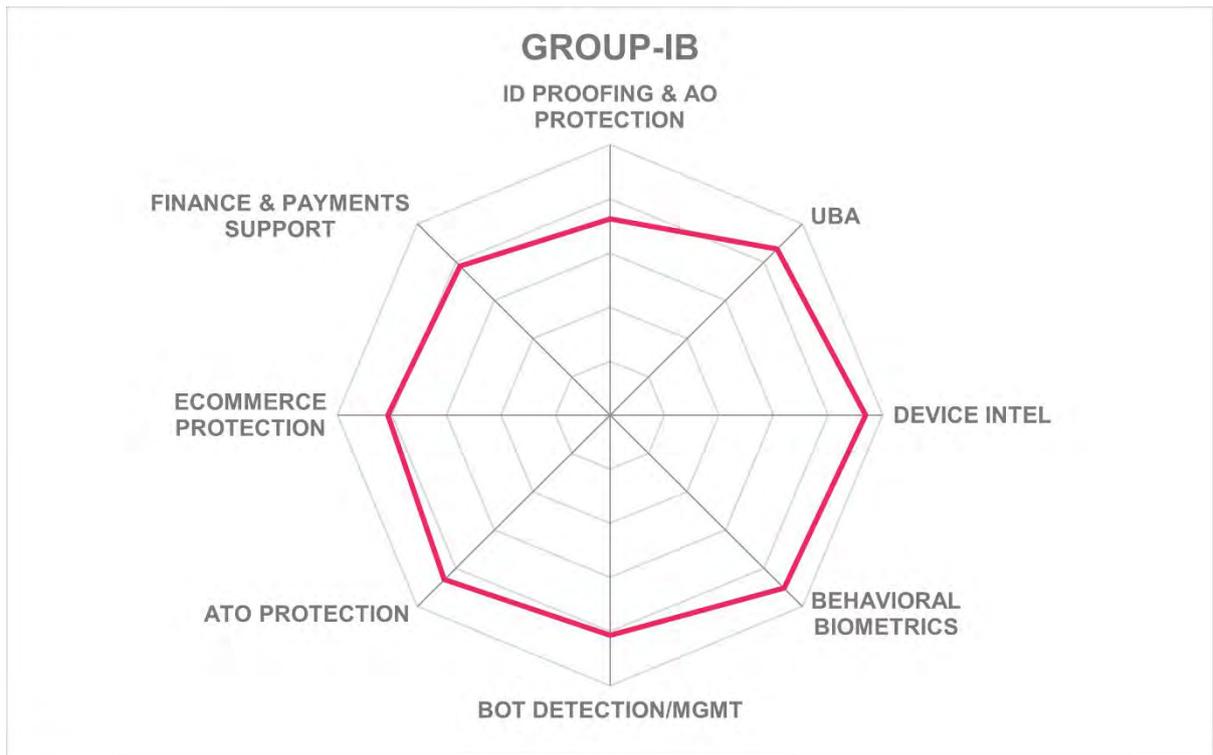
Gurucul – Fraud Analytics

Gurucul was founded in 2010 and is a privately-owned company headquartered in Los Angeles. Gurucul has a suite of products and services including SIEM, UBA, Open XDR, Network Traffic Analysis, Network Detection & Response, and Fraud and Risk Analytics. For FRIP components, Gurucul Fraud Analytics platform has credential and device intelligence, UBA, and bot detection. The solution architecture is centered on their data lake and analytics, meaning customers can configure their business applications and 3rd-party FRIP services to gather and send information to Gurucul's Fraud Analytics data lake. Gurucul's SaaS runs in a public IaaS provider with global data centers. The solution can be deployed by customers as VMs or containers in their own data centers or in any public IaaS. Service pricing is based on the numbers of accounts monitored.

Gurucul does not include identity proofing services. Customers could add 3rd-party services on via APIs. Gurucul could assist customers with various forms of compliance such as AML, KYC, OFAC, etc., but this requires customers to acquire services and data sources beyond what is provided with the platform. External but not internal sources of credential intelligence are utilized.

For device intelligence, Gurucul evaluates IP address and reputation, geo-location and geo-velocity, and device type/ID/fingerprint. Device posture checks are not performed, and it can only use indirect methods to look for signs of malware involvement in transactions. Gurucul's forte is in UBA. It has advanced ML-based detection models that consider a wide range of attributes, including transaction details such as amounts, payees, locations, times, etc. Behavioral biometrics are not part of the base solution but could be added on from other vendors. Bot detection is enabled through UBA and network traffic analysis but can be enhanced with 3rd-party behavioral biometrics. Gurucul can provide basic protection against some types of fraud that are commonly experienced by retail, ecommerce, and other industries; more advanced capabilities in these areas would require behavioral biometrics.

Gurucul's risk engine can be tuned by customers via a well-designed interface. Fraud analysts will find conducting investigations is straightforward, starting from the dashboard. Gurucul Studio allows extensive editing of detection models and filters. Secure REST APIs are how customer apps communicate with Gurucul Fraud Analytics. Risk scores and detailed rationales can be provided to customer applications. Evaluation results can be packaged into other formats such as SAML tokens, JWT claims, and OAuth2 grants. Call center integration is available. Gurucul has case full case management and can interoperate with most of the major ITSM solutions.

Gurucul is HIPAA and PCI-DSS certified but has not achieved ISO 27001 or SOC 2 Type 2 for its cloud-hosted services. Gurucul Fraud Analytics has a different approach in this market: their emphasis is on acquiring data and using their sophisticated detection capabilities on that data, rather than deploying their own identity proofing services and behavioral biometrics functions. Having those capabilities as part of their own solution would improve their overall offering. Organizations that need advanced risk analysis and are comfortable with adding 3rd-party FRIP components if needed should consider Gurucul Fraud Analytics.

|	
Security	Positive
Functionality	Weak
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 12: Gurucul's rating

Strengths

- Excellent implementation of ML detection models for UBA
- Call center integration
- Evaluation results can be rendered in multiple formats such as SAML, JWT, or OAuth2 tokens/claims.
- Gurucul Studio allows customers to extensively edit and create new detection models from templates.
- Analyst interface is easy to use.
- Ships with data masking templates for privacy regulatory compliance
- ITSM integration

Challenges

- No identity proofing or use of in-network credential intelligence
- No behavioral biometrics
- Bot detection and management are hampered by lack of behavioral biometrics.
- Does not perform device health checks.
- Lacks ISO 27001 and SOC 2 Type 2 certifications.
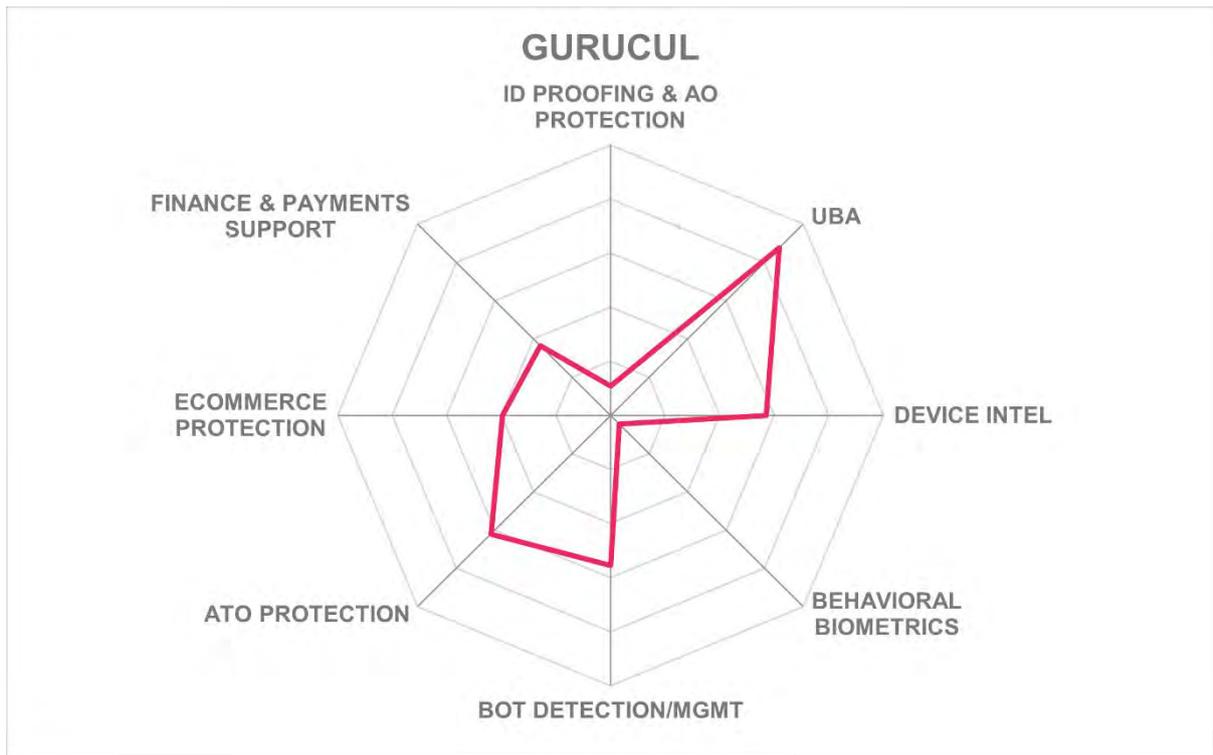
HID Global – HID Approve, Authentication Service, Risk Management, and Identity Verification

HID Global is a subsidiary of ASSA ABLOY Group AB of Stockholm. HID's US headquarters is in Austin, TX. HID 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 suite of products listed in the title bar offers fraud prevention components including ID proofing, credential and device intelligence, behavioral biometrics, UBA, and bot detection. The financial industry is their main focus. It can be installed on customer premises or in IaaS, and their SaaS is hosted in AWS in both EU and NA regions. Pricing options include per-registered user, per-server, and per-transaction.

HID provides identity assurance verification and credential issuance services. Government and enterprise customers can utilize HID for authoritative attribute lookups, remote document verification, and electronic credential assignment. For remote document proofing scenarios, the mobile app can scan and register the authoritative documents, take selfies, and perform real-time biometric matching. More than 4,500 document types are supported. HID can interoperate with most 3rd-party identity proofing services as well. HID supports AML, KYC, mule account detection, PSD2 and 3DS2 compliance. The Authentication Platform utilizes in-network compromised credential intelligence.

For device intelligence, HID's SDKs can pick up IP address, geo-location & geo-velocity, and device fingerprint/ID/type/hygiene. Device and IP reputations are also considered in the risk analysis. HID's UBA functions encompass full transaction history details and discerns patterns. Data storage periods can be extended if customers need that. Behavioral biometrics are mediated by JavaScript and SDK; and the full expected range of biometrics attributes are analyzed. HID employs ML-enhanced (including Deep Learning algorithms) to examine gathered intelligence and biometrics. Bot detection functions are enabled by recognition of bot signatures and behavioral biometrics. Bot management is mostly limited to allow- and deny-listing. Support for ecommerce fraud commonly perpetrated by bots is not present, but HID can detect CNP, Authorized Push Payment, SMS hijacking, suspicious extensions on users' browsers, and various MITM attacks.

HID's risk engine allows customers to prioritize risk factors and set thresholds. The policy authoring interface is flow-chart style. The fraud analyst interface is very easy to work with. All common report types are present, and customers can create additional reports if needed. The solution has built-in case management, and a connector for JIRA Atlassian ITSM is available. Webhooks are supported. Customer apps communicate with HID Global's services via REST, OData, SOAP, and WebAuthn APIs. JWT, OAuth, and key exchange can be used for API authentication. Results of evaluations can be packaged as JWT claims, OAuth2 grants, and OIDC flows as well. Call center integration is available.

HID attests and/or has certified on FIPS 140-2, ISO 9001/27001/27018/27019, and SOC 2 Type 2. HID is a market leader in Passwordless Authentication solutions. In fact, some implementation partners package HID Authentication Platform to serve as the consumer

front-end for their "bank-in-a-box" offerings. More sophisticated bot management should be possible and would extend the solution offering into the broader ecommerce space. The remote ID document verification for onboarding, strong identity proofing, device intelligence, and transaction level UBA features make HID worth considering as a FRIP solution for financial and government customers.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 13: HID Global's rating

Strengths

- Identity proofing and strong credential issuance capabilities present, including some government IDs.
- Secure mobile app for remote document verification
- Easy-to-use flow-chart style policy authoring GUI
- Detailed but intuitive fraud analyst interface.
- Device intelligence and behavioral biometrics are collected using secure their SDK and/or JavaScript, including some uncommon attributes.
- UBA includes transaction histories and patterns.
- Wide range of secure API types supported for flexible customer integration.
- FIDO 2.0 and FIPS 140-2 certified components

Challenges

- Bot management could be enhanced to include additional response types.
- Sanctions screening is not present but is on their near-term roadmap.
- Lacks counterfeit/stolen card detection capabilities.
- Does not address most bot-induced ecommerce fraud beyond financial use cases.

Leader in

HID GLOBAL
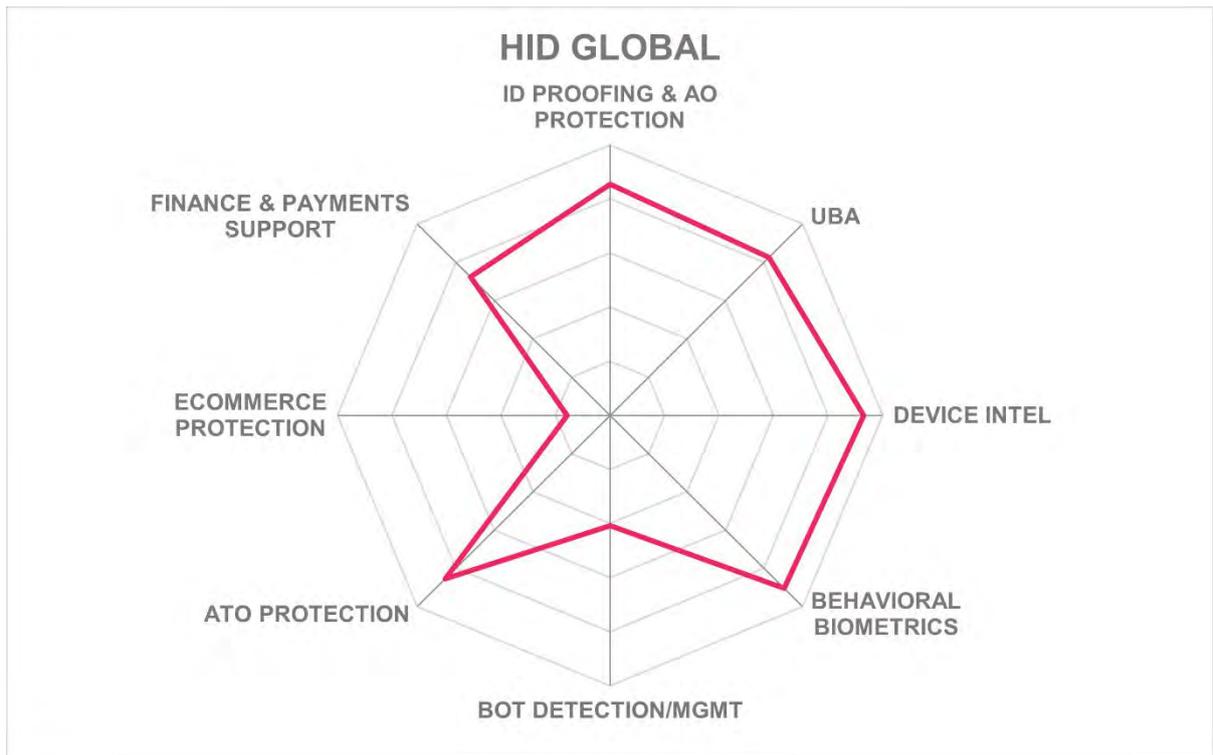
HUMAN – Human Defense Platform

HUMAN Security was formed in 2012 in New York and has offices across the US and in Singapore, Israel, and the UK. In summer of 2022, HUMAN merged with PerimeterX, another bot management specialist, and acquired Clean.io, a malvertising protection specialist. The company is privately held and covers many industries including retail, ecommerce, government, insurance, media, SaaS, ticketing, travel, and finance. The Platform is composed of Bot Defender, Account Defender, Code Defender, Credential Intelligence, Media Guard, and CleanAD (for malvertising protection). These products address the credential and device intelligence, UBA, behavioral biometrics, and bot detection and management components of FRIP. The company's Satori Threat Intelligence and Research team enables specialized take down services. Their Human Defense Platform is hosted in two Top Tier IaaS providers in multiple data centers on three continents. Pricing is based on numbers of transactions.

HUMAN's Human Defense Platform does not include identity proofing, but it is under consideration for future inclusion. It can apply UBA and behavioral biometrics to assist in making determinations about AML, KYC, and OFAC compliance. CNP and counterfeit/stolen card detection and support for 3DS2 and PSD2 are not provided. Extensive in-network and external credential intelligence sources are evaluated.

IP addresses and reputations, geo-location and geo-velocity, device fingerprint/ID/type and security posture are the primary device intelligence attributes that are evaluated. It can also figure out if a known user is using a new device or a trusted device. HUMAN's UBA functions examine most user actions and transaction details with the exception of transaction amounts. It does not automatically make adjustments for user travel, however in these cases the detection will rely on device intelligence and UBA. HUMAN deploys JavaScript to collect behavioral biometric data including keystroke/mouse, mobile touchscreen, touchscreen, and gyroscopic analysis; some pertinent network attributes are not considered. Bot detection is based on signatures, embedded pixels, and behavioral biometrics, leveraging 350 algorithms that continuously adapt to changing threat conditions with support from the Sartori threat research team. Bot management options include issuing proof-of-work challenges, hidden JavaScript challenges, and CAPTCHAs. Responses to the challenges can lead to allow- or deny-listing and/or throttling. The Human Defense Platform protects against most bot-launched ecommerce fraud types such as inventory checking and hoarding, price checking, headless browsers, fake reviews/comments/job postings, social media and ad-clicking bots, account creation and credential stuffing, ticket scalping, overlay apps, and Buy Now Pay Later.

Customers can request changes to risk factor weighting, which are performed by the internal operations teams, as the risk engine is not directly addressable by customers. However, a robust policy engine is provided to allow customers capabilities to define their own rules for internal or partner tools. By default, risk scores and recommendations are not output to customers as the solution handles all mitigation actions automatically on behalf of customer applications. App integration is possible via REST APIs, which are constrained to JWT authentication and authorization. However, most deployments are through customers' CDNs, ecommerce platforms, load balancers, CDNs, load balancers, app SDK/middleware,

serverless or cloud frameworks, or IAM systems. Support cases are managed via their console and Slack or email, and it can integrate with Atlassian JIRA. HUMAN's Human Defense Platform does not have call center integration. HUMAN's Human Defense Platform provides robust activity reports, and the dashboard can be customized. The analyst interface is well-designed and presents a lot of information that can easily be filtered and navigated.

HUMAN's Human Defense Platform is ISO 27001 and SOC 2 Type 2 certified. US FedRAMP certification is in work. HUMAN's Human Defense Platform has some omissions in key areas of FRIP, such as identity proofing, regulatory compliance support, and support for some payments security services. Their strengths are in their different approaches to bot and fraud detection and management which enables them to protect against most fraud types experienced by ecommerce vendors and other web property operators. Bot take down services offered by HUMAN also distinguish this offering. Companies and government agencies that are looking for FRIP services that are specialized at deterring these fraud types should carefully review what HUMAN's Human Defense Platform has to offer.

|	
Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

Table 14: Human Security's rating

Strengths

- Leverages in-network and dark web research for compromised credential intelligence.
- Can detect known users on new devices from across its customer base.
- Bot management options include unobtrusive JavaScript and proof-of-work challenges as well as take-down services.
- Extremely low reported latency
- Highly scalable service processing trillions of transactions per day
- Fast deployments predicated on embedding in CDNs, ecommerce platforms, load balancers, or application SDKs and middleware.
- Easy to navigate and use the analyst interface.

Challenges

- No identity proofing.
- PSD2 and 3DS2 not supported.
- CNP and stolen/counterfeit card detection not present.
- UBA omits some transaction details.
- Bot detection does not utilize behavioral biometrics.

Leader in

HUMAN SECURITY
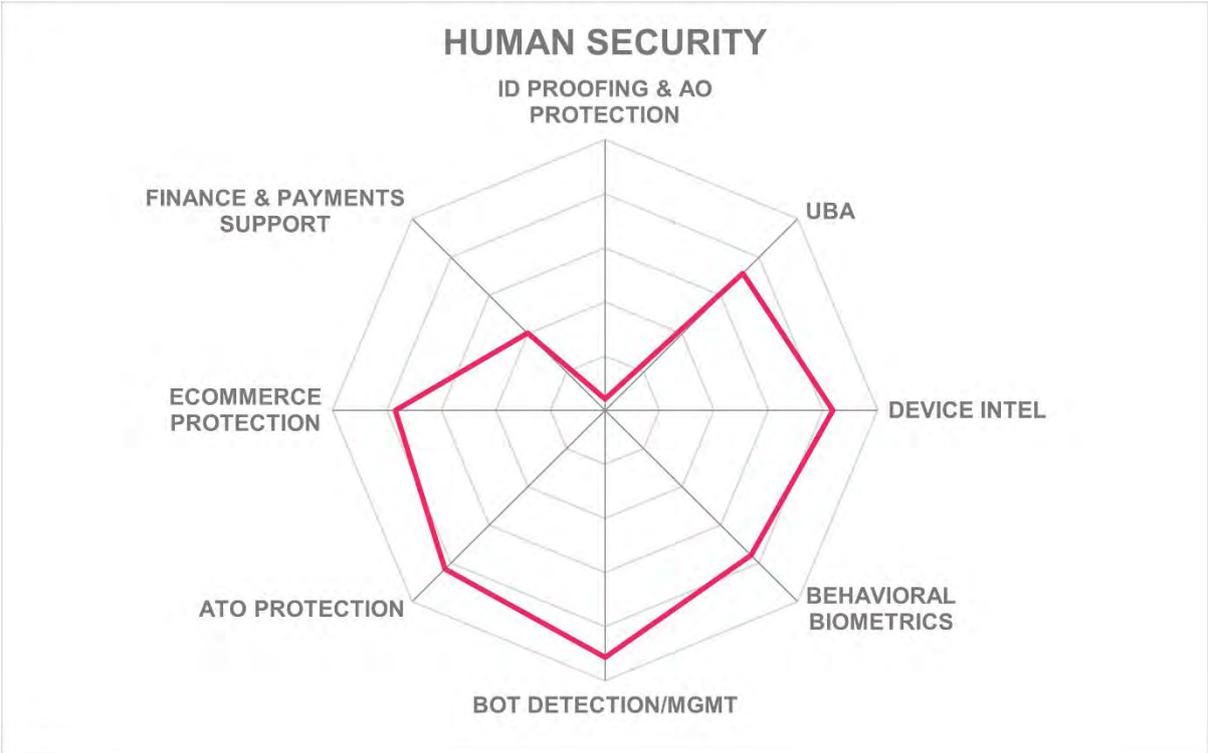
IBM – Trusteer: Pinpoint Detect and Pinpoint Assure

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. Pinpoint Detect and Pinpoint Assure are the components of Trusteer, their solution for fraud reduction. The integrated suite covers all aspects of FRIP. IBM services are hosted in AWS data centers on three continents. Licensing options include per-session or by numbers of active users.

IBM offers industry-specific profiles and support for AML, KYC, OFAC, PEP, 3DS2 and PSD2. Trusteer is used in payment services for detecting CNP and counterfeit/stolen cards. Trusteer now has identity proofing built-in, with a mobile remote onboarding app, and integrations with Telesign and AWS Rekognition. Their service utilizes both in-network and 3rd-party credential intelligence in risk decisions. Trusteer's device intelligence is comprehensive, pulling all available attributes and adding external sources for IP and device reputation. Their UBA functions examine login context, transaction detail including amounts and patterns, profile changes, and client page navigation patterns. Data retention periods are configurable, and the solution supports GDPR and the "right to be forgotten". The client SDK collects the full range of behavioral biometric factors, including many that are unique to their implementation, such as higher-order insights from geometrical analysis, mobile accelerometers and gyroscopes, and touchscreen pressure. Behavioral biometrics, threat intelligence, and signatures provide the basis for their bot detection features. Trusteer informs customers of bot probability and allows for advanced bot management, including allow- and deny-listing, throttling, and redirection. The solution protects against some common fraud types that plague ecommerce and web property owners such as inventory hoarding, price checking, headless browsers, malvertising, ad-clicking, account creation and credential stuffing bots, gift card cracking, mobile malware, aggregators, and Authorized Push Payment fraud.

The risk engine is powered by their advanced ML detection models. Customer applications connect via REST APIs, which are secured by JWT or client certs. Evaluation results can also be packaged as JWT claims. Customers admins use their TrustBoard to manage fraud thresholds and policies as well as see account risks and KPIs. The analyst interface provides all expected information and is straightforward to use for conducting investigations, Trusteer has case management built-in, and can export data as CSV files that could be imported by external ITSM systems. IBM has call center integration, including phone-to-web session mapping, the ability to collect SIM information from MNOs, and detect SIM swaps.

IBM Trusteer has achieved many security certifications including ISO 27001/27017/27018, SOC 2 Type 2, and FFIEC. Trusteer scales well and covers all aspects of FRIP, with highly innovative features in device intelligence, user behavioral analysis, behavioral biometrics, and bot management. Adding support for detecting certain types of ecommerce fraud would be helpful for those market segments. IBM Trusteer should be on the short list for most types of organizations looking for FRIP services.
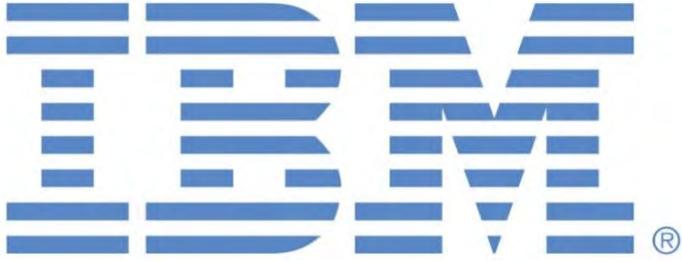
|	
Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 15: IBM's rating

Strengths

- New identity proofing features for onboarding and AML, KYC, and sanctions screening
- Thorough device intelligence features supplemented with external reputation feeds.
- UBA considers transaction details and history as well navigation patterns.
- Behavioral biometric analysis considers standard modalities plus innovative higher-level combinations.
- Excellent bot detection and granular bot management capabilities
- IAM integration with IBM Verify, Okta, and Ping Identity
- Analyst interface is well thought out and expedites investigations.

Challenges

- Does not support detection and prevention of certain ecommerce fraud types.
- Additional strong API authentication types may be beneficial.
- Support for packaging evaluation results in OIDC or OAuth2 could be useful for some customers.

Leader in

IBM
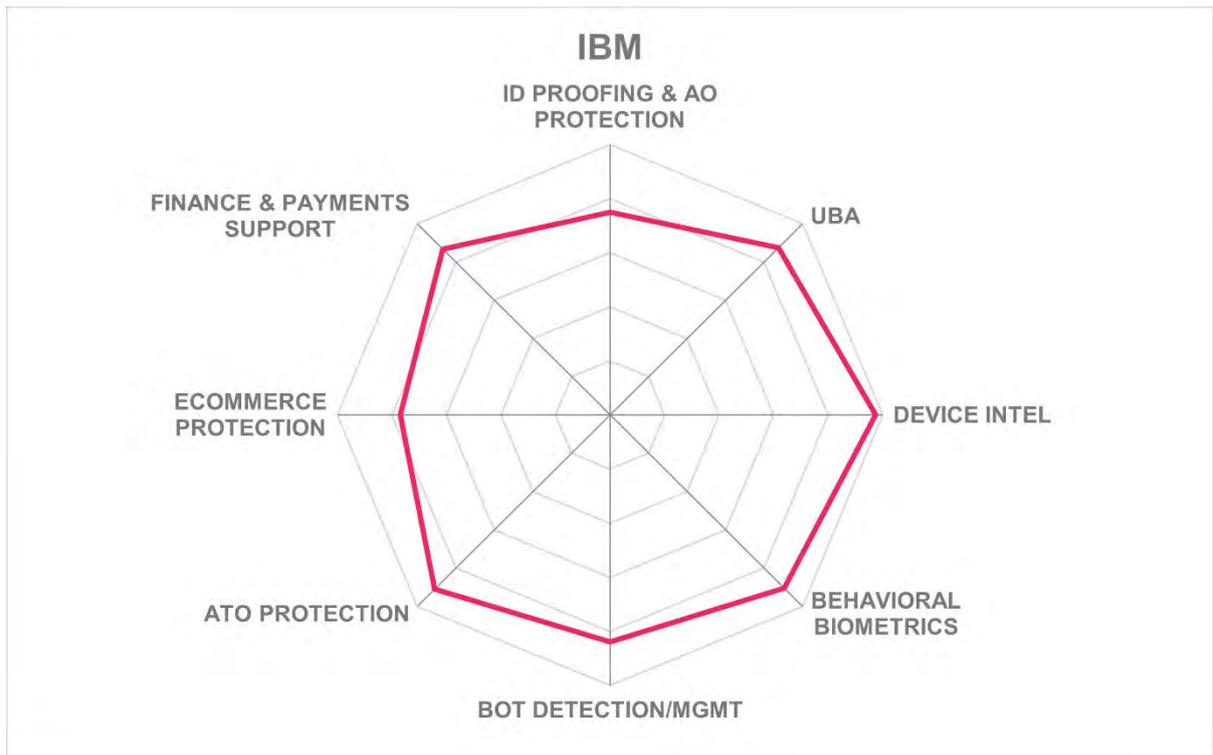
ID Dataweb – AXN Platform

ID Dataweb was founded in 2011 and is headquartered in Northern 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. The solution is SaaS-based and is hosted in a public IaaS provider. Licensing is a combination of number of active users and per-transaction fees, depending on the type of attribute services requested.

ID Dataweb has comprehensive identity proofing services, integrating multiple government and private sector attribute sources (including MobileMatch and BioGovID), and providing remote document verification with facial recognition via a mobile SDK. AXN solves many ID proofing use cases ranging from employment verification, supply chain management, medical license verification, student status validation, and criminal watchlist checks. These identity proofing features facilitate AML, KYC, LEI, OFAC, PEP, PSD2, and the conditional challenges component of 3DS2.x compliance. AXN leverages in-network and multiple external sources of credential intelligence.

Apps built using their secure inline API service calls (integrated into standard workflows) collect a myriad of device intel attributes including geo-location and geo-velocity, IP address, device ID/fingerprint/type, security posture, and IMEI/SIM. In-browser malware, SIM swaps, and rooted devices can be detected. The UBA functions examine login patterns, transaction details and historical patterns, user profile changes, and time-on-page metrics. JavaScript enables behavioral biometrics, which include evaluation of keystroke and mouse movements, touchscreen pressure and swipe analysis, and gyroscopic and network characteristics. Behavioral biometrics, embedded pixels, and activity signatures provide the basis for bot detection. For bot management, AXN can allow-list, challenge, and make recommendations to customers on how to handle different bot types. AXN can detect and alert on the most prevalent bot-perpetrated ecommerce and website fraud types such as inventory hoarding and price checking, headless browsers, fake goods/reviews/comments/posts, malvertising, social media and ad-click bots, account creation and credential stuffing, ticket scalping, and card cracking.

ID Dataweb has enhanced their risk engine since the last report. Customers can select attribute sources and modify their own evaluation rules in a flowchart style workflow editor. Handling recommendations and reason codes can be provided in addition to risk scores. OIDC, REST API, and Webhooks allow multiple ways for customer apps to interface with AXN. ID Dataweb offers multiple API authentication methods for maximum security and flexibility. Connectors are available for Auth0, ForgeRock, HYPR, OneTrust, Ping Identity, SailPoint, and SecZetta. AXN can integrate with call center software, for verifying calls and mapping calls to sessions. The analyst GUI is highly intuitive, showing the logic in step-by-step investigations. Executive level reports are present, and more can be configured if needed.

AXN is ISO 27001 certified. SOC 2 Type 2 certification is in work and planned for completion in April 2023. ID Dataweb is a smaller company but continues to grow its customer base and areas of operation. AXN provides a complete FRIP solution with extensibility and the ability

orchestrate other FRIP component services as required. More sophisticated detection mechanisms would be useful. Any organization that needs a FRIP solution should carefully consider ID Dataweb AXN for their built-in and extensible capabilities

|	
Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 16: ID Data Web's rating

Strengths

- Extensive identity proofing features, including mobile-based remote identity and document verification.
- Facilitates compliance with most common and pertinent regulations such as AML, KYC, OFAC, PEP, PSD2, and conditional challenges required by 3DS2.
- Uses internal and multiple external sources of credential intelligence.
- Broad list of device intel and user behavioral attributes examined.
- Updated risk engine with easy flow-chart style policy authoring interface.
- API support includes OIDC and Webhooks as well as standard REST API.
- Pre-built integrations for leading IAM & CIAM solutions.
- Self-service proof-of-concept demos for prospective customers.

Challenges

- UBA and behavioral biometric analysis rely on rules rather than ML detection models.
- Data retention policies are not automatically configured for privacy regulatory compliance.
- Does not look for CNP or other credit card fraud types.
- Bot management could allow for more options.
- Smaller vendor mostly focused on North American market

Leader in

ID DATAWEB
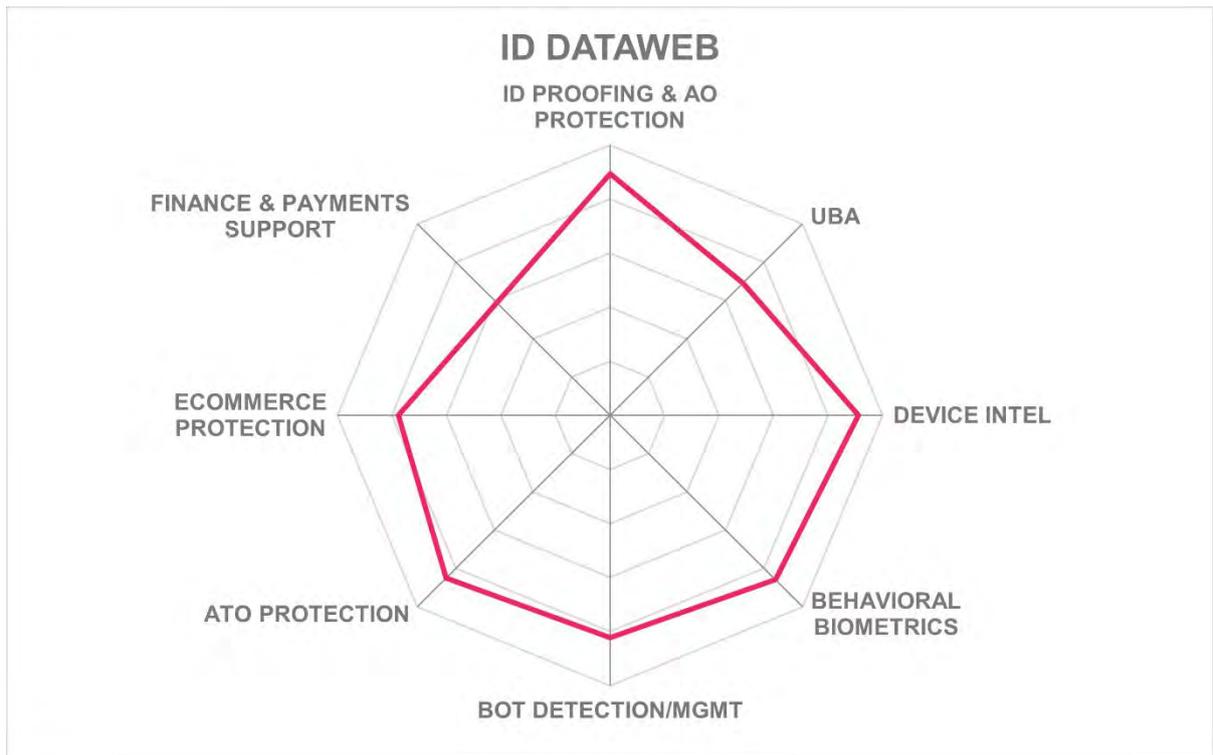
LexisNexis® Risk Solutions – Dynamic Decision Platform, RiskNarrative™, and more

LexisNexis Risk Solutions formed in 1998 from progenitor companies that started in the 1960s. LexisNexis Risk Solutions has an array of solutions accessible via the LexisNexis Dynamic Decision Platform (DDP) that contribute to their overall FRIP offering: Fraud Intelligence, InstantID®, TrueID® with Portrait Match, MultiFactor Authentication, ThreatMetrix®, BehavioSec®, Emailage®, PhoneFinder, and WorldCompliance®DataPlus. LexisNexis Risk Solutions addresses all the major fraud reduction technologies. Their solutions are hosted in their own facilities plus multiple public IaaS providers across three continents. Pricing is based on numbers of transactions or API calls plus fixed fees for professional services and tuning.

LexisNexis ThreatMetrix, Emailage, InstantID, Fraud Intelligence, PhoneFinder and MultiFactor Authentication provide identity proofing services. Customers can configure additional 3rd-party attribute sources through their DDP and RiskNarrative platforms if required. LexisNexis TrueID also has access to 6,600 government ID types in 200 countries, such as driver's licenses, passports, national ID, voter IDs, military IDs, etc. LexisNexis Risk Solutions has a mobile SDK to enable remote identity and document verification against these many sources. In-network credential intelligence is gathered and evaluated.

LexisNexis Dynamic Decision Platform (DDP), RiskNarrative, Bridger Insight XG, ThreatMetrix, and Financial Crime Digital Intelligence modules provide thorough capabilities for AML. ThreatMetrix aids in detecting mule accounts. LEI lookups are supported as needed. InstantID is used for KYC. The Compliance Lens screening solution delivered through RiskNarrative leverages WorldCompliance Data. This data includes OFAC, EU, BOE, FBI, PEP SEC, and nearly 1,200 other global enforcement lists. ThreatMetrix has a dedicated 3D Secure API that facilitates 3DS2 support, and in conjunction with ThreatMetrix, PSD2 Strong Customer Authentication is addressed. ThreatMetrix, Phone Finder, and Emailage assist with detecting and preventing CNP and counterfeit/stolen credit card transactions.

ThreatMetrix harvests the full set of available device intel attributes including IP address, geo-location, geo-velocity, IMEI/SIM information, device fingerprint/ID/type, device reputation and security posture checks. It can detect known users on new devices. ThreatMetrix maintains unique identifiers uniting digital and physical identity attributes that help their clients to differentiate between trusted customers and fraud risks. ThreatMetrix performs deep UBA, examining login patterns, and real-time transaction details against historical patterns. The SDK and JavaScript can also read and evaluate behavioral biometric patterns. Behavioral biometrics, in concert with threat intelligence and bot signatures, provide the foundation for their bot detection and management features. Bot management options are allow/deny-listing and throttling. Threat Metrix Bot Detection API and behavioral biometrics enable prevention of most of the common bot-based attacks against ecommerce and other web properties, including inventory checking/hoarding, headless browsers, fake reviews/comments, social media bots, account creation and credential stuffing bots, ticket scalping, gift card cracking, Buy Now Pay Later, and Authorized Push Payment fraud.

ThreatMetrix is configured via the Dynamic Decision Platform, which allows easy customization of risk attribute sources and weightings through a drag-and-drop workflow editor. Risk scores and reason codes are generated by their risk engine. Customers can communicate with LexisNexis Risk Solutions via the REST API. Results are shared back in the portal and as JSON. The Dynamic Decision Platform portal is also secured with SAML. Customizable dashboards allow for audience specific views of the threat landscape. Customer analysts use the Case Manager within DDP. Lexis Nexis Risk solutions can interoperate with Atlassian JIRA and ServiceNow ITSMs also. Investigations are expedited by smart visualizations of events indexed on graphs of LexID Digitals (their unique identifiers that link digital identifiers, entities, and devices). PhoneFinder and Emailage are used by customer call center staff to verify phones and active sessions.

LexisNexis Risk Solutions have obtained SOC 2 Type 2 certifications. Their infrastructure allows for maximum scalability. Their FRIP solutions are comprehensive. The number of discrete services that provide the full FRIP is rather large, and customers may benefit from more combined, easier-to-consume packages. Any organization in any industry should have LexisNexis Risk Solutions on their shortlist when searching for fraud reduction technologies.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 17: LexisNexis Risk Solutions' rating

Strengths

- Comprehensive identity proofing built-in as well as support for 3rd-party services
- SDK for mobile-based remote identity and document verification
- Support for AML, KYC, mule account detection, and exhaustive sanctions screening
- 3DS2 and PSD2 support; can detect CNP and counterfeit/stolen card activities.
- Excellent device intelligence features, including detecting known users on new devices and detecting SIM swaps and IMEI anomalies.
- Full UBA examines all relevant aspects.
- Behavioral biometrics built-in
- Provides protection against not only fraud types affecting financial institutions, but also against most of the major fraud types committed against ecommerce companies.
- Multiple API types supported for easy customer app integrations.
- Call center and ITSM interoperability

Challenges

- Not ISO 27001 certified
- Additional bot management methods such as challenging and redirection may be beneficial.
- Multiple services required for full FRIP functionality; better packaging would likely make it easier for customers to manage.

Leader in

LEXISNEXIS RISK SOLUTIONS
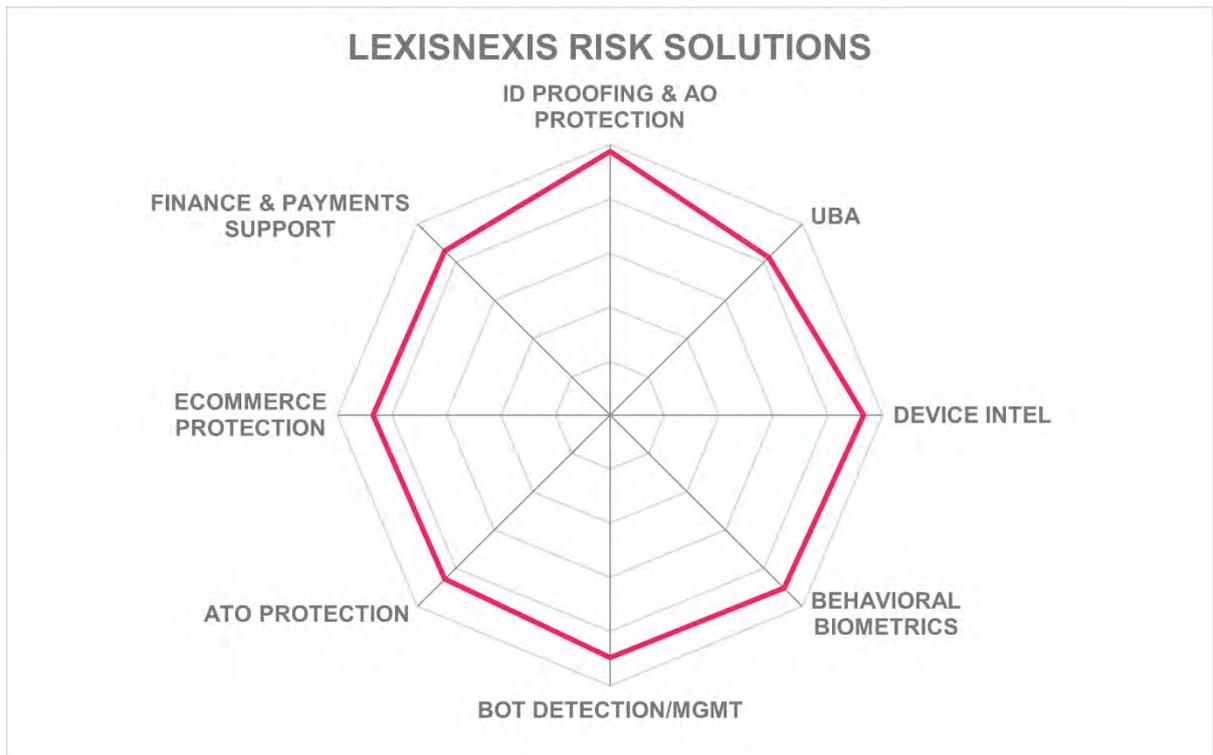
Outseer – Fraud Manager, 3-D Secure, and FraudAction

RSA was acquired by Symphony Technology Group in 2020, and in June 2021 Outseer brand was launched. Outseer is the new brand for what used to be RSA's Fraud and Risk Intelligence business unit and its FRIP offerings are comprised of the products listed above. Outseer is widely used in the financial sector, protecting over two billion consumers. 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 in a public IaaS provider in data centers in the EU and NA. There are three separate solutions within Outseer portfolio: Outseer Fraud Manager, which is widely used to prevent fraud in digital banking; 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. Outseer addresses all aspects of FRIP, in some cases through integrations with partners as detailed below. Pricing options for SaaS are per-transaction, for on-premises deployments by the number of active users, and fixed costs for fraud intelligence feeds.

Outseer does not have built-in identity proofing, but they do partner with 1Kosmos, LexisNexis, Prove, and Telesign for those services, including using 1Kosmos' mobile-based remote identity and document verification service. The Outseer suite can be used to create lists for OFAC and PEP screening. Outseer 3-D Secure is an EMV 3DS2 ACS solution and is compliant with EMV 3DS v2.0/2.1/2.2. Outseer 3-D Secure is certified by the Visa, Mastercard, Amex, JCB, and EFTPOS card networks. Outseer 3-D Secure can help customers meet PSD2 SCA requirements and can detect CNP and stolen credit card fraud attempts. Outseer collects and uses its in-network credential intelligence to prevent ATO fraud. Outseer FraudAction Intelligence is a service available via subscription that allows customers to receive intelligence feeds in the FraudAction dashboard or via APIs.

Outseer Mobile SDK collects most of the common device attributes such as IP, geo-location, geo-velocity, and device fingerprint/ID/type. Device posture checks are not performed. For UBA, Outseer analyzes transaction details and history. Outseer partners with CallSign for behavioral biometrics, which uses JavaScript to harvest keystroke/mouse, touchscreen pressure and swipe, and network characteristics to develop baselines for users. Device intelligence and UBA are powered by ML detection models. Behavioral biometrics can serve as a second authentication factor. Bot detection is limited to what can be determined from UBA; behavioral biometrics and activity signatures are not used by default can be extended by customers. Bot management options are limited to allow- and deny-listing unless 3rd-party solutions are used. Bot-launched ecommerce fraud types are not specifically targeted. However, Outseer does provide takedown services for malicious mobile apps. Outseer also protects against Real Time Payments (RTP) and Authorized Push Payment fraud.

Outseer does not have call center integration directly, but it can evaluate call and session data within its risk engine if provided by customers. The risk engine is configurable by customers, but the interface needs an update. Customer apps connect over REST and SOAP APIs, which can be secured with OAuth2 or key exchange authentication. Though results cannot be packaged in those token types listed, Outseer does have integration with some major IAM solutions. Case management is available through Fraud Manager and over APIs. Connections to external ITSMs would need to be configured by customers. Basic

reports are available in the back-office application. Additional reports can be created by customers with 3rd-party applications. The analyst interface relies on drop-down boxes and regular expression type searches and would benefit from enhancement.

Outseer Fraud Manager, 3-D Secure are SOC 2 Type 2 certified. Outseer 3-D Secure is PCI-DSS and PCI-3DS certified. ISO 27001 certification would be a plus. The management and analyst interfaces need to be modernized, and those activities are on their roadmap. The suite is optimized for and targeted at financial institutions and payment services. Organizations in those industries should definitely consider Outseer's suite when looking for fraud reduction solutions.

|	
Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Neutral

Table 18: Outseer's rating

Strengths

- Excellent payment fraud detection services: compliant with all 3DS specifications and certified by the major credit card networks.
- Detailed UBA implementation
- Malware and fraudster network takedown services
- Protects against ATO, Realtime Payment Fraud, and Authorized Push Payment Fraud
- Provides fraud intelligence as a subscription service.

Challenges

- Does not perform device hygiene checks.
- Identity proofing and behavioral biometrics are not built-in, but partnerships bring the necessary functions to their platform.
- Limited bot detection and management capabilities.
- Management and analyst GUIs need to be updated (planned)

Leader in

OUTSEER
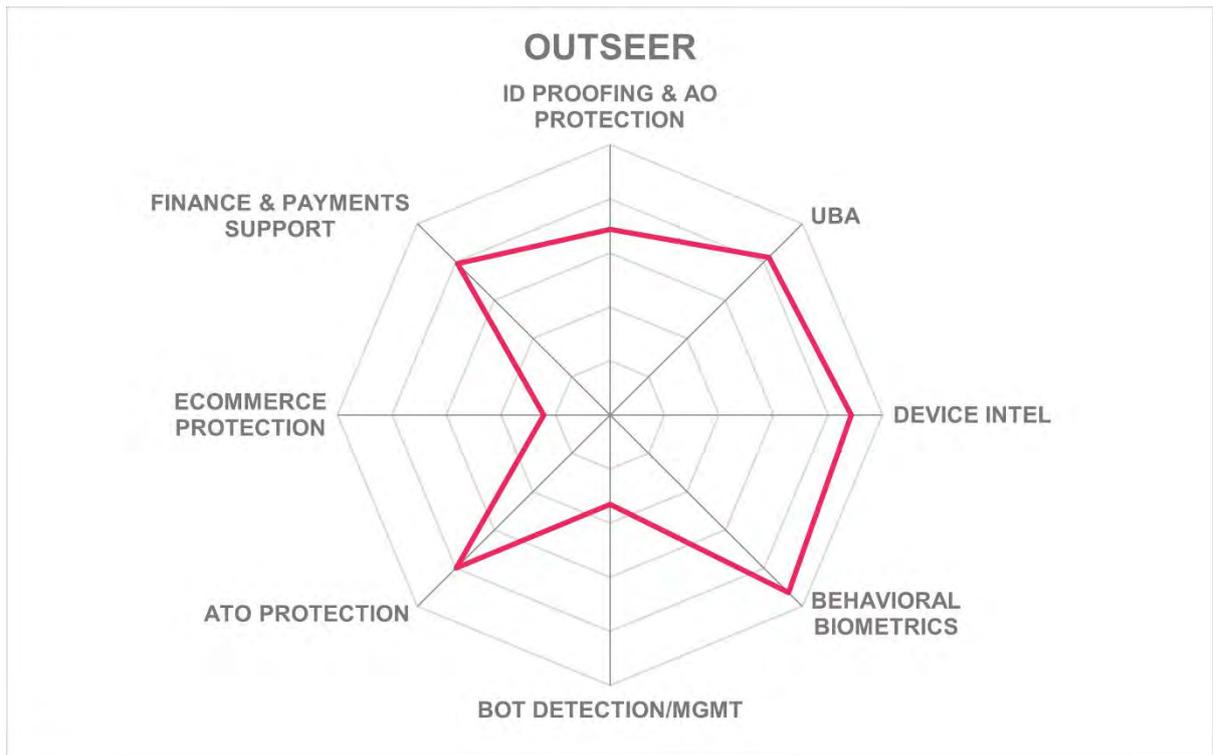
Sift – Sift Digital Trust & Safety Suite

Sift was formed in 2011, and it is headquartered in San Francisco. Sift is a fraud protection specialist, with services for payments security, content protection, ATO protection, and PSD2 compliance. Their target customers are in the fintech, ecommerce, dating, travel, and delivery service industries. Areas of FRIP covered by their suite are device intelligence, UBA, behavioral biometrics, and bot detection and management. Their services are hosted in two different public IaaS providers in three different data centers in the US. Pricing is determined by the number of billable events, where an event is defined as product and use case, such as logins, orders, account creation, risk scoring, or monthly active user.

Sift does not have identity proofing services built-in but has connectors for 3rd-party services including Jumio, OnFido, and Stripe. Credential intelligence is not evaluated. Sift can provide information to partners for AML, KYC, and sanctions screening, but Digital Trust & Safety Suite is not designed as an AML, KYC, or screening solution. Sift is a transaction and user behavior risk analysis tool that can assist customers and their applications for 3DS2.x and PSD2 Secure Customer Authentication. Digital Trust & Safety Suite can detect CNP and stolen credit card fraud.

Sift uses JavaScript to examine many device attributes, such as IPs and reputation, geo-location and geo-velocity, device fingerprint/ID/type, and IMEI/SIM. Sift can detect rooted devices but does not look for signs of malware or perform device security posture checks. For UBA, Sift considers login patterns and transaction amounts, payment methods, shipping history, and more. Sift generates tailored ML-enhanced detection models for each customer. These measures provide ATO defense. The Content Integrity product can track and examine content posted to protected sites as well. Sift pulls a very limited set of behavioral biometrics using JavaScript. Behavioral biometrics are not used for bot detection. Bot classification and management require human analysis and action. Some types of bot-based ecommerce attacks can be detected and blocked, such as inventory checking/hoarding, headless browsers, fake goods/job postings/product reviews/comments, social media and ad-click bots, account creation and credential stuffing bots, ticket scalping, gift card cracking, and Buy Now Pay Later schemes.

Sift works with customers to customize risk analysis parameters if needed. A waterfall-style interface with drop-downs and if/then logic operators allows knowledgeable customers to edit detection rules and include external sources of threat intelligence. Sift provides REST APIs and Webhooks for application integration. Dashboard show pertinent statistics and specialized metrics for their target audience, such as order components and values and chargeback rates. The analyst interface is well-designed, allowing staff to run quick queries as needed to facilitate manual investigations. The related Content Integrity service has a similar look and feel and allows customers to prevent payment circumvention and other scams. Sift does not have integration with call center software. A connector is available for Zendesk ITSM.

Sift is SOC 2 Type 2 certified. ISO 27001 certification has not been achieved. Sift leverages partnerships for some key areas of FRIP. In-house expansion and enhancement of behavioral biometrics and bot detection could be beneficial. Sift generates ML detection

models for each customer. Digital Trust & Safety Suite facilitates drilling into ecommerce transaction, user analysis, and other contextual details to detect and deter fraud. Organizations that are looking for this level of specialization for ecommerce and financial fraud as well as ATO protection, which have other solutions for identity proofing and other FRIP components, will likely want to consider Sift Digital Trust & Safety Suite.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Neutral
Usability	Neutral

Table 19: Sift's rating

Strengths

- Content Integrity service tracks user posting activities.
- Long data retention periods which improve fraud prediction accuracy.
- Sift creates bespoke ML detection models for each customer.
- UBA tracks extended attribute types relevant to ecommerce, such as billing/shipping addresses, payment types, payees, purchase history, etc.
- Good analyst interface makes investigations easier.

Challenges

- Pricing model could be simplified.
- Service hosted in US only.
- No built-in identity proofing or credential intelligence.
- Behavioral biometrics and automated bot detection functions are limited.
- Bot classification and management are manual activities.
- Stronger API authentication needed.

Leader in

SIFT
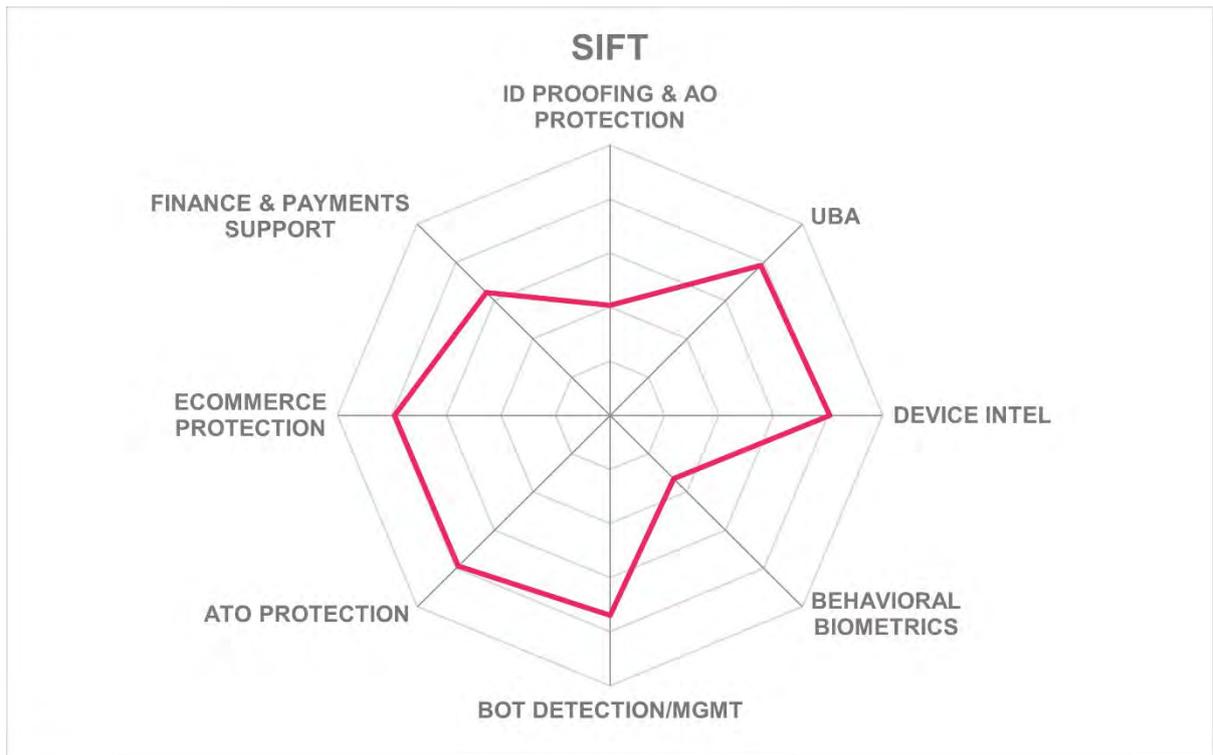
Transmit Security – Transmit Security Platform

Transmit Security was founded in 2016 and is headquartered in Tel Aviv and Boston. They are a well-funded late-stage VC-backed company. Decision and Response Services contains functionality in all the FRIP component areas defined above. Transmit also has leading products in the Passwordless Authentication and CIAM spaces. Transmit Security Platform is a highly scalable SaaS that runs in public IaaS providers across globally distributed data centers. Methods for pricing vary depending on customer volumes. SaaS pricing includes per-user and per-transaction options.

Transmit Security Identity Verification Services offers a native mobile SDK and APIs that enables facial recognition with liveness detection and ID document verification. Transmit Security can send input to and work with AML, KYC, and OFAC screening partners and payment security partners, but does not provide full service in these areas. Transmit Security evaluates in-network credential intelligence and customers can add 3rd-party sources if desired.

Device intelligence attributes that are examined include geo-location and geo-velocity, IP address and reputation, device fingerprint/ID/type, and SIM metadata if available. Transmit can detect rooted mobile devices and the influence of malicious code on end user devices to prevent ATOs. Transmit Security can detect known users on new devices. Transmit's UBA functions look at login patterns, transaction details and patterns, and can be extended by customers as needed. Moreover, Transmit Security allows customers to modify the ML detection models for their own use cases and set data retention policies. Transmit Security collects a wide range of all the standard behavioral biometrics signals via SDK and JavaScript. Behavioral biometrics, UBA, and device intelligence provide their bot detection capabilities. Working with customers and their external service providers (such as CDNs), Transmit Security has multiple bot management options including allow- and deny-listing, challenging, throttling, and redirecting bots. The Transmit Security Platform prevents certain types of bot-initiated fraud types that commonly interrupt ecommerce and finance sites such as inventory hoarding, headless browsers, malicious ad insertion, account creation and credential stuffing bots, ticket scalping, gift card cracking, fake goods/job postings, and Authorized Push Payment fraud.

Customers build policies in the low-code Journey Editor. It has an innovative, drag-and-drop, flowchart style interface. Data sources can be plumbed in easily and risk engine output can be sent over REST APIs that can be secured using JWT, OAuth2, OIDC, and SAML authentication. Webhooks and FIDO 2 / WebAuthn are also supported. Transmit Security enables customers to set multiple actions based on risk scores and to define evaluation result codes and equivalences among MFA methods. Risk scores can also be packaged as JWT claims, SAML assertions, OAuth2 grants, and OIDC flows. Dashboards show a variety of key metrics and can be modified if needed. The analyst interface is feature-rich but can be complex to operate. Transmit supports call center integration with Genesys, Nuance, and Pindrop, allowing call-to-web session mapping. It can also get call information from MNOs if configured. APIs are protected against attacks and can be rate-limited. Connections to SIEMs are possible over syslog. Case management features are limited, but generic connectors facilitate connectivity with ITSMs.

The Transmit Security Platform is ISO 27001 and SOC 2 Type 2 certified. The solution scales well. All functional aspects of FRIP are addressed by their solution, both through built-in capabilities and partnerships. The Transmit Security Platform has support for standards that boosts its interoperability and makes it easy to deploy. Organizations in their target audience of finance, banking, insurance, and retail should have Transmit Security on their shortlist for evaluation for FRIP services.

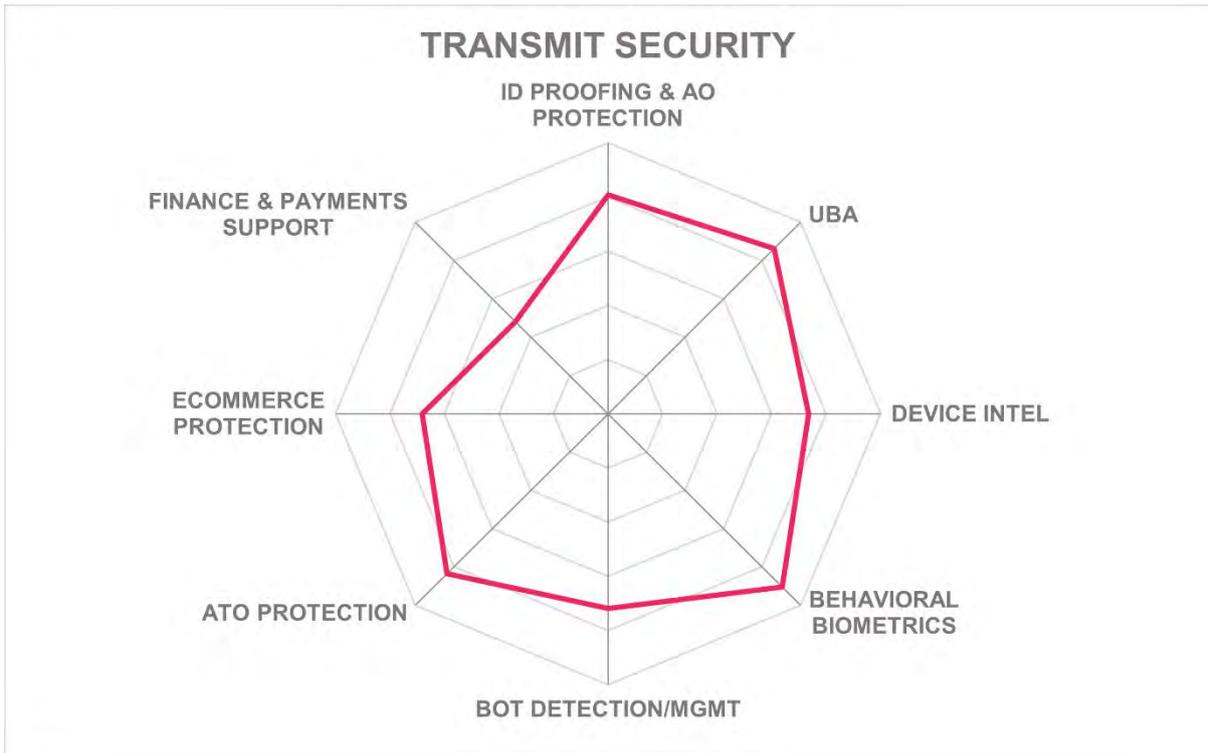|		
Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 20: Transmit Security's rating

Strengths

- Fast deployments via APIs and SDKs
- Can determine known users on new devices.
- Exhaustive and customer configurable UBA examines transaction level and contextual details and patterns.
- ML detection models can be customized if needed.
- Risk scores can be output in multiple standard token types as well as over APIs.
- Excellent API support and security
- Good call center integration features
- 24/7 security research lab and analyst services for incident response

Challenges

- Their brand is not well-known for fraud protection, although they serve some Fortune 100 clients.
- Case management should be enhanced.
- Support for detecting additional ecommerce fraud types would be useful.

kuppingercole ANALYSTS

Leader in

TRANSMIT SECURITY

ID PROOFING & AO PROTECTION

UBA

DEVICE INTEL

BEHAVIORAL BIOMETRICS

BOT DETECTION/MGMT

ATO PROTECTION

ECOMMERCE PROTECTION

FINANCE & PAYMENTS SUPPORT

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors may not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

Amazon

Amazon Fraud Detector is a service available in AWS for customers that has features for detecting online payments fraud, new account fraud, trial and loyalty program abuse, and ATO fraud. The solution is highly scalable and leverages ML detection models.

Why worth watching: Amazon hosts many ecommerce applications, providing a potentially large customer base for Amazon Fraud Detector. They also offer a Free Tier with up to 30,000 fraud predictions per month.

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 is focused on PSD2 compliance.

Why worth watching: Cleafy focuses on deterring financial fraud and has anti-malware capabilities that help with PSD2 SCA.

Equifax

Equifax is one the "Big Three" credit rating agencies, and has services across most FRIP categories, including authoritative identity proofing, AML, KYC, and OFAC compliance. They also offer MFA, risk management, and other related services.

Why worth watching: As an authoritative attribute provider, Equifax is part of the fraud protection supply chain. Equifax acquired Kount in 2021 and Midigator in 2022 which gives them additional FRIP functionality.

Feedzai

Feedzai is a fraud risk detection and risk operations specialist firm headquartered in Portugal. In 2021, they acquired Revelock, the former Buguroo, another fraud reduction intelligence platform vendor. Feedzai covers financial fraud use cases, account opening fraud, AML, KYC, and watchlist screening.

Why worth watching: Feedzai has a strong and growing market presence in the EU.

FICO

FICO is a long-established analytics and risk management company. The FICO Falcon Global Intelligence Network gathers risk signals from >9,000 global institutions. FICO Falcon Fraud Manager aids in preventing ATO and payment fraud. They also offer AML, KYC, and sanctions screening compliance solutions for customers.

Why worth watching: FICO is a major player in risk management.

Imperva

Imperva, a cybersecurity solution company headquartered in San Mateo, California, began as a provider of web application firewalls in 2002, then expanded its portfolio to include other product lines. In 2019, Imperva was acquired by private equity firm Thoma Bravo. Imperva has ATO protection, bot detection and management, and client-side protection features in the FRIP space.

Why worth watching: Imperva is a large and growing firm that can expand further into FRIP services.

Nice Actimize

Nice Actimize is a fraud and financial crime detection service provider based in Israel. They were founded in 1999. In 2020, Nice Actimize picked up Guardian Analytics, another FRIP service provider. Nice Actimize focuses on financial fraud, AML, KYC, and account opening protection.

Why worth watching: Nice Actimize has a good trajectory of acquisitions, integrations, and growth.

OneSpan

OneSpan, formerly VASCO, is headquartered in Chicago, IL, US, and has offices in Brussels, Montreal, and Zurich. They have a suite of related products that cover all aspects of FRIP except credential intelligence.

Why worth watching: OneSpan was a leader in all categories in the prior edition of this report, but was unable to participate in this round.

Ping Identity

Ping Identity has been a pioneer in identity federation and access management since its founding in Denver in 2002. Ping Identity has grown substantially and went public on the

NYSE late in 2019. Ping Identity was among the first of the enterprise IAM vendors to offer CIAM. Ping is building extensive FRIP capabilities into their CIAM offering.

Why worth watching: With a large user base in CIAM, Ping's venture into integrated FRIP services will be beneficial to their customers.

Ravelin

Ravelin was founded in 2014 and is headquartered in London. Their emphasis is on defending against online payments fraud. They also protect against policy abuse such as refund and sales promotions abuse, and supplier fraud, as well as ATO and bot-perpetrated attacks.

Why worth watching: Ravelin offers traditional ATO prevention and payments security and has specialized services for the ecommerce ecosystem.

Telesign

Telesign was established in 2005 and is based in Los Angeles. Telesign provides phone number intelligence, identity verification, MFA, and bot detection for finance, on-demand, rideshare, and gaming customers.

Why worth watching: Telesign is a service provider to several other vendors in the FRIP market and has many built-in capabilities.

ThreatMark

ThreatMark was founded in 2015 and is headquartered in Brno, Czechia. The company is in growing start-up 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.

Why worth watching: ThreatMark AFS performs continuous risk assessments encompassing device intelligence, behavioral biometrics, and UBA across sessions. ThreatMark has visually impressive and intuitive management and analyst interfaces.

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.

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. In 2022, TransUnion acquired Neustar, another large FRIP service provider.

TransUnion was covered in the previous edition of this report but was unable to participate in the update.

Methodology

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

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities 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 they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain 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 vendors whose products lag 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 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 that 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, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates 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 on 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
- Deployment
- Interoperability
- Usability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, 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 the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly, and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). 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. Vendors must support technical standardization initiatives. 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 over all markets in which a vendor is active. Therefore, 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 either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. 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 a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong positive	Outstanding support for the subject area, e.g., product functionality, or outstanding position of the company for financial stability.
Positive	Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. 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. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate 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.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the 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.

Related Research

Leadership Compass Fraud Reduction Intelligence Platforms (2021)

Leadership Compass CIAM Platforms (2022)

Executive View HID Global Fraud Prevention

Executive View BioCatch

Executive View Deduce Customer Alerts and Identity Insights

Executive View BehavioSec, LexisNexis® Risk Solutions Company

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.