kuppingercole ANALYSTS

Fraud Reduction Intelligence Platforms - eCommerce

John Tolbert

August 14, 2025

LEADERSHIP COMPASS 2025

This report provides an overview of the Fraud Reduction Intelligence Platforms for eCommerce and merchants market and a compass to help you find a solution that best meets your needs. It examines solutions that provide an integrated set of security and compliance capabilities designed to protect financial, banking, and payments applications. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to monitor, assess, and reduce these risks.

Contents

Executive Summary 4
- Key Findings 7
- Market Analysis 7
- Delivery Models 9
- Required Capabilities 9

Leadership 12
- Overall Leadership 12
- Product Leadership 14
- Innovation Leadership 16
- Market Leadership 18

Product/Vendor evaluation 20
- Spider graphs 20
- Akamai – Account Protector, Bot Manager, Brand Protector, Content Protector, Client-Side Protection & Compliance 22
- Arkose Labs – Bot Manager, Device ID, Edge and Scraping Protection, Arkose Email Intelligence, and Arkose Phishing Protection 25
- Bureau – Device Intelligence & Behavioral AI, Identity & Document Verification 28
- Experian – CrossCore 31
- Group-IB – Fraud Protection 34
- Gurucul – REVEAL Fraud Analytics 37
- HID – Authentication Platform, Risk Management Solution, Identity Verification Service 40
- HUMAN Security – Human Defense Platform 43
- IBM – Trusteer: Pinpoint Detect and Pinpoint Assure; and Safer Payments 46
- ID Dataweb – AXN Platform 49
- LexisNexis® Risk Solutions – LexisNexis® Dynamic Decision Platform® , LexisNexis® RiskNarrative™ Platform, LexisNexis® ThreatMetrix®, LexisNexis® BehavioSec®, LexisNexis® Phone Finder, LexisNexis® Fraud Intelligence Solutions Suite, LexisNexis® InstantID®, LexisNexis® TrueID®, LexisNexis® FlexID, LexisNexis® Instant Verify

International, LexisNexis® IDVerse®, LexisNexis® Compliance Lens, LexisNexis® WorldCompliance™ Data Plus 52
Outseer – Fraud Manager, 3-D Secure, FraudAction 55
Ping Identity – P1 Protect, P1 Verify, P1 Authorize, and P1 DaVinci 58
Sift – Platform 61
Sumsub – Fraud Prevention 64
Transmit Security – Mosaic Platform 67
XTN Cognitive Security® – Cognitive Security Platform® 70
Vendors to Watch 73
Amazon 73
Brandefense 73
Deduce 73
Equifax 73
F5 74
Feedzai 74
FICO 74
Forter 74
GBG 75
LynxTech 75
Microblink 75
Nice Actimize 76
OneSpan 76
Ravelin 76
Reality Defender 76
Seon 76
Telesign 77
Thales 77
TransUnion 77

Executive Summary

Fraud remains a significant and evolving threat to businesses, non-profit organizations, and government agencies worldwide. While banking, finance, payment services, and retail continue to be primary targets, other sectors—including insurance, gaming, telecommunications, healthcare, cryptocurrency exchanges, government assistance agencies, travel and hospitality, and real estate are becoming increasingly vulnerable. Cybercriminals constantly refine their Tactics, Techniques, and Procedures (TTPs) to exploit weaknesses in security controls, identity proofing, and transaction verification. Banks, other financial institutions, merchants, and payment service providers must use advanced fraud detection systems to prevent various types of fraud.

Types of Fraud

Account Takeover (ATO) Fraud

ATO fraud occurs when fraudsters gain unauthorized access to a legitimate user's account to conduct illicit activities. Attack vectors include:

- Credential stuffing and password spraying using breached credentials.
- Malware-based attacks (e.g., Man-in-the-Middle [MitM] or Man-in-the-Browser [MitB]).
- Social engineering scams leveraging phishing, smishing (SMS phishing), and vishing (voice phishing).
- Remote Access Trojans (RATs) that enable fraudsters to control compromised devices.
- Rootkits and info-stealer malware that give unauthorized access to PII and user credentials to fraudsters.
- SIM swap fraud, in which attackers transfer a victim's phone number to a new SIM to intercept OTPs and reset account access.
- Session hijacking, where fraudsters either use MitM tactics or purchase long-lived valid sessions on the dark web.

Account Opening (AO) Fraud / New Account Fraud (NAF)

AO fraud and NAF are terms often used interchangeably, and both forms involve the use of stolen personal data to create fraudulent accounts. NAF may also include synthetic fraud (see below). Fraudsters may exploit breaches of personally identifiable information (PII) from financial, healthcare, educational, and government sources to fabricate a complete digital identity. These fake accounts are commonly used to:

- Access credit lines, loans, and instant financing.
- Conduct promotion abuse.
- Funnel money through mule accounts to facilitate money laundering.
- Commit Buy-Now-Pay-Later (BNPL) and small business loan fraud.

Synthetic Identity Fraud

Distinct from AO fraud but part of NAF, synthetic identity fraud involves the creation of entirely new digital personas by combining real and fictitious identity attributes. Rather than exploiting a single stolen identity, fraudsters generate synthetic profiles by:

- Assembling non-existent or mismatched social security numbers (SSNs) or other official ID types with real addresses and phone numbers.
- Exploiting gaps in identity verification processes.
- Gradually building a credit profile through small transactions and loans before executing larger-scale fraud (a technique known as "busting out"). Synthetic identities are harder to detect because they do not correspond to real individuals who would report fraudulent activity.

Emerging Fraud Trends and Scams

Fraud tactics continue to diversify across digital channels. Categories include:

Digital Impersonation Scams:

- Fake investment platforms (cryptocurrency, gold, foreign currency exchange, and real estate scams).
- Deepfake audio/video used in corporate payment scams, customer account enrollment attacks for AO/NAF.
- AI-assisted social engineering for crypto and romance scams and business email compromise (BEC).
- CEO/CFO fraud involving payment redirection.
- Fake job listings designed to harvest PII and banking details.
- Fake government, welfare, and tax refund notices designed to steal personal information.

Payment and Financial Fraud:

- Card-Not-Present (CNP), Card-Not-Received (CNR), counterfeit card, and skimmer fraud.
- Malicious invoice payment redirection targeting businesses.
- Fraudulent real estate escrow redirection using compromised email accounts.
- Unauthorized BNPL transactions exploiting weak identity verification.
- Authorized Push Payment (APP) fraud where victims initiate transactions at the behest of fraudsters, often in cases of crypto, romance, invoicing, or purchase scams.

Automated and Bot-Driven Fraud:

- Automated credential stuffing and brute force attacks.
- Arbitrage, such as Inventory hoarding (Grinch bots), that disrupt retail stock availability.

- Fake account creation bots that execute promotional abuse.
- Gift card cracking, where bots guess activation codes for financial gain.
- Fake reviews, social media manipulation, and ad fraud bots.

Cryptocurrency Fraud:

- Fake Initial Coin Offerings (ICOs) designed to defraud investors.
- Wallet-draining malware and clipboard hijacking of crypto addresses.
- Fraudulent exchanges and aggregators tricking users into depositing funds.

Fraud Mitigation Strategies

Organizations combat fraud through layered security approaches that leverage:

- Fraud Reduction Intelligence Platforms (FRIPs): Enhancing fraud detection through six key components:
  - Identity verification.
  - Credential intelligence for compromised account detection.
  - Device intelligence to track devices previously used for fraud and to aid in discovery of anomalous behavior.
  - User behavioral analytics to assess deviations from normal activity.
  - Behavioral/passive biometrics to identify individual users via their normal interactions with their devices, discover coercion, and flag fraudulent interactions.
  - Bot detection and mitigation to prevent large-scale automated fraud.

- Real-time risk analytics: Assessing transaction and behavioral anomalies from sources described above to provide decisions, risk scores, and context for customer applications.
- Risk-based Authentication (RBA) within CIAM systems: Strengthening identity verification by considering credential intelligence, device reputation, and behavioral biometrics, often in conjunction with FRIPs.

As fraud tactics evolve, organizations must continuously adapt their detection and prevention frameworks, leveraging Machine Learning (ML) driven fraud intelligence, real-time transaction analysis, and identity verification enhancements to mitigate financial and reputational risks.

Businesses across the world of all sizes and across most industries are negatively affected by fraud. Non-profit organizations and government agencies are also increasingly targeted. All organizations are at risk of loss from the many different kinds of fraud perpetrated today.

This report focuses on FRIP solutions that can help merchants, eCommerce, and other organizations including non-profits and government agencies. Much of the fraud that affects these industries originates from bots; thus behavioral biometrics and bot detection are of high importance. Organizations outside of finance are similarly concerned with ATO, NAF, and scam prevention. However, these organizations may have less rigorous requirements for IDV or name/watchlist screening (generally speaking, although varying levels of IDV are

needed in different scenarios), which is a focus for banks and FinTechs, and was an area of focus in the Leadership Compass FRIP – Finance.

For information about the Leadership Compass process, see our KuppingerCole Leadership Compass Methodology.

Key Findings

As fraudsters change their TTPs and find new nefarious ways to exploit victims, FRIP solution providers continue to innovate to help their customers deter fraud.

- Merchants and other non-finance organizations are increasingly looking for at least lightweight methods of increasing identity assurance.
- Dedicated threat intelligence teams can help vendors and service providers create, refine, and deliver the most accurate information to deter bots.
- AI-powered photo, audio, and video deepfakes are a growing problem, and some solutions are addressing these vectors.
- Scams like those described above (investment, crypto, romance, impersonation, etc.) are now the most common types of fraud encountered, even outpacing ATOs.
- Info-stealer malware has risen in popularity amongst fraudsters, which helps them get valid credentials and PII for ATO and NAF.
- SMS phishing (smishing) attacks, for example with messages purporting to be from toll payment processors and delivery services, are on the rise.
- Behavioral biometrics has become more commonplace in FRIP solutions, with some vendors OEM-ing capabilities from others. Some are using more innovative methods than others.
- Some solutions provide user-friendly unobtrusive CAPTCHAs, which benefit both their customers and the customers' consumers with better security and user experiences.
- Leading-edge FRIP solutions are adding GenAI capabilities to their investigative interfaces to assist fraud analysts in their investigations and to provide reports.
- Advanced bot management is not present in all solutions.

Market Analysis

The market for Fraud Reduction Intelligence Platforms is growing proportionally with the rise in frequency and complexity of fraud itself.

The FRIP market is somewhat active in terms of mergers and acquisitions. In October 2024, Experian agreed to acquire ClearSale in Brazil, adding significant market share in a large market.

In April 2024, Entrust completed its acquisition of Onfido, a prominent identity verification company specializing in AI-driven solutions.

LexisNexis Risk Solutions acquired IDVerse in 2025 and is integrating IDVerse's identity verification and document authentication functions (including document liveness detection) into its Dynamic Decision Platform.

In this edition of the Leadership Compass on FRIP for eCommerce, we have new vendors participating that have not been in previous versions, including Bureau and Sumsub. We anticipate further growth in the FRIP market.

The application of FRIPs differs significantly between the financial services sector and eCommerce environments due to variations in regulatory obligations, fraud typologies, and customer interaction models. Financial institutions prioritize IDV, AML, and KYC measures, and name/watchlist screening, all of which are essential for onboarding, transaction monitoring, and regulatory reporting. These controls are designed to detect illicit financial activity, prevent account laundering, and verify the legitimacy of transacting parties. In contrast, eCommerce platforms focus on preserving transactional integrity, preventing monetary and non-monetary abuse, and protecting the user experience. This includes advanced bot detection and management, device intelligence, behavioral anomaly analysis, and defenses against policy exploitation such as coupon stacking, return fraud, and loyalty manipulation. While both domains share a need for behavioral analytics and credential intelligence, their implementations differ in scope, priority, and technical integration points.

Feature/Focus Area	Financial Services	eCommerce
IDV	High priority for regulatory compliance, which requires strong identity assurance	Used selectively to lower risks depending on industry and business
KYC	Mandatory for account origination and periodic follow-ups	Less commonly used unless extending credit
AML and Sanctions Screening	Required by regulations	Less rigorous requirements
Credential Intelligence	Prevents ATO, insider abuse, mule networks	Prevents ATO and synthetic identities
Device Intelligence	Supplements IDV and session tracking for identity and authentication assurance	Core to identity continuity and fraud signals
User Behavioral Analytics	Applied to transaction risk scoring	Applied to sessions, checkouts, and returns
Behavioral Biometrics	Supplements IDV and ATO detection	Primary means for bot detection and secondary means for policy abuse detection
Bot Detection and Management	Bot detection needed for normal operations	Highly relevant for detecting and handling a variety of bot-driven attacks
Policy Abuse Detection	Focus on internal fraud or misuse	Core for loyalty, discount, return fraud

Table 1: Differences between feature priorities between FRIP solutions for finance and eCommerce

Bias in machine learning-based fraud scoring systems is an increasingly prominent concern, particularly when models incorporate behavioral biometrics and other probabilistic features.

These systems can inadvertently encode demographic or behavioral biases into scoring logic, resulting in elevated false positive rates for certain user segments, such as those using non-standard devices, assistive technologies, or browsing patterns that deviate from the models' dominant training distribution. Such disparities raise questions about fairness, proportionality, and user recourse, especially when automated decisions affect access to essential services or financial products. Regulatory frameworks like the EU AI Act and GDPR emphasize the need for transparency, explainability, and the right to contest automated decisions, requiring organizations to justify how risk scores are computed and to audit for discriminatory impact. As behavioral signals become more deeply embedded in identity and fraud detection workflows, enterprises must implement governance practices that assess model performance across cohorts, provide interpretability mechanisms, and align with emerging standards for ethical AI use in high-risk contexts.

Delivery Models

Most FRIP services are offered as SaaS, with customer applications calling the protected APIs of the FRIP solutions. Some vendors offer software that customers can run on-premises or in private clouds.

IDV components are a combination of built-in services, apps, SDKs, and APIs. IDV apps are typically mobile apps that can take photos of authoritative government IDs or documents and selfies (for photo matching) and use NFC to scan embedded chips. Some vendors lean heavily on third-party services for IDV functions.

The device intelligence and behavioral biometrics components are most commonly implemented as JavaScript. The .js files run on the browsers and apps of the customers' customers, harvesting many attributes for analysis. Alternatively, some vendors provide SDKs that can pull similar information for their customers to use to build apps and sites.

Compromised credential intelligence, if performed only in-network, only uses data about failed and suspicious logins and transactions from within the FRIP solution provider's ecosystem of customers. A few vendors expand their capabilities by pulling risk signals from external sources such as haveibeenpwned, VeriClouds (acquired by Enzoic), and SpyCloud.

User Behavioral Analysis and bot detection and management capabilities, if present, are hosted by the FRIP (unless customers choose to run it themselves). UBA depends on identity and transaction data, and bot detection is most effectively implemented via behavioral biometrics, and augmented by rules, cyber threat intelligence (CTI), and ML detection algorithms.

Required Capabilities

This Leadership Compass analyzes FRIP solutions for eCommerce organizations that reduce:

- Account TakeOver (ATO) fraud
- Account Opening (AO) / Synthetic Identity Fraud / New Account Fraud
- Payment transaction fraud

- Fraud that affects credit card accepting merchants
- Scams that affect business users and individuals
- Website, platform, policy, and subscription abuse
- Bot-perpetrated attacks such as DDoS, credential stuffing, hoarding bots, and more

The following are a list of key capabilities that FRIP solutions for web-facing organizations need:

Solution Basics

Well-documented APIs for customer app integration
API management and security
JavaScript and SDKs for client telemetry harvesting
MFA and RBAC for administrators
Toolkits for customizing connectors
Auditing, reporting and dashboarding
Scalable service architecture & high-availability deployment
Use of ML and DL algorithms for risk analysis
Integration with customer ITSM
ISO 27001 and SOC 2 Type 2 certification
Features for 3DS2.x compliance
Features for EU PSD2/3 compliance

Credit Card and Payment Fraud Reduction

Detection and prevention of CNP and other forms of credit card fraud
Detection and prevention of APP and BNPL fraud
Detection and prevention of scams

Identity Verification

Integration with third-party identity verification and authoritative attribute providers

Credential Intelligence

Use of credential intelligence from within the vendor’s network of customers
Inclusion of credential intelligence from external Identity Providers or third-party sources

Device Intelligence

IP reputation
Geo-location & geo-velocity detection
Mobile network and Wi-Fi network analysis
Device ID, type, and fingerprint
Device reputation
Device posture checks, including OS version and malware detection
SIM swap detection
Known user on unknown device checking
Device jailbreak/rooted checking

User Behavioral Analysis

Login context analysis, including frequency and time of logins and login locations
Transaction details and historical analysis, transaction types, amounts, item analysis, velocities and frequencies, locations, proximity to suspicious behavior such as phishing, relationships to known high-risk accounts, account creation clusters, and more
Data privacy compliance, including the use of privacy enhancing technologies including de-identification, pseudonymization, redaction, encryption, and others

Behavioral Biometrics

Obfuscated JavaScript and secure SDK implementation
Wide range of features and modalities which can be examined from computers and mobile devices

Bot Detection & Management

Ability to detect bot vs. human users
Ability to identify bot intentions (good, gray, or malicious)
Ability to deploy unobtrusive or user-friendly challenges
Policy-based bot handling, including redirection and throttling

Risk Engine

Customer configurable risk policy authoring
Risk score and/or decisions output
Score rationale output
Integration with third-party authentication services
Integration with customer IAM systems
Integration with customer Line of Business (LOB) applications

Innovative Capabilities (Selection)

Credential and device intelligence signals sharing
Deepfake detection
Detection of CNR, counterfeit card usage, and skimmers
Detection of complex scams, such as crypto and romance scams
Emphasis on unobtrusive methods for fraud detection
Use of Generative AI (GenAI) in the fraud analyst interface, including Natural Language (NL) queries, case descriptions, and executive reporting
No-code/low-code policy authoring interface
Map, timeline, and identity/transaction graph views for fraud analysts
ABAC and/or PBAC for administrators
Integration with call centers
Integration with customer Security Information and Event Management systems (SIEM)
Support for detecting sophisticated smishing, vishing, and quishing

Take-down services

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 identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

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

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

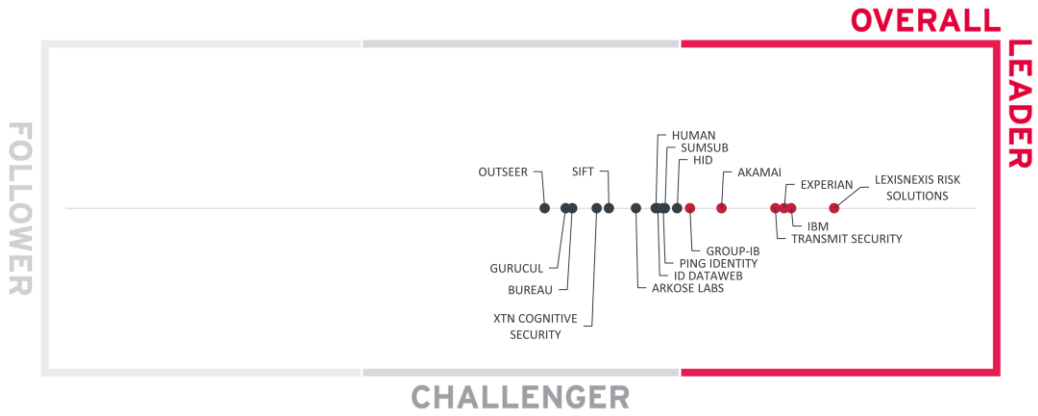


Figure 1: Overall Leadership in the FRIP for eCommerce market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

LexisNexis Risk Solutions leads the field, with IBM, Experian, and Transmit Security close by in the Overall Leadership rank. Akamai and Group-IB are also Overall leaders in this edition of the Leadership Compass for FRIP – eCommerce. The leaders have the largest market

share, product completeness, and innovation. There are some overlaps with the Overall Leaders in the Leadership Compass FRIP – Finance, as LexisNexis Risk Solutions, IBM, Experian, and Transmit Security are named as Overall Leaders in that report. The fact that these companies are leaders in both editions demonstrates that not only do they have significant market share, but also that they can address a wide variety of fraud protection use cases.

The majority of the vendor field appear in the Challengers section. Since this report focuses on FRIP for eCommerce and merchants, there are some new companies in this report that were not in previous versions. Additionally, because of the focus on eCommerce use cases, the positioning of vendors and products is somewhat different than earlier Leadership Compasses on FRIP as well as the recently published LC FRIP – Finance.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- Akamai
- Experian
- Group-IB
- IBM
- LexisNexis Risk Solutions
- Transmit Security

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. 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 2: Product Leadership in the FRIP for eCommerce market

Transmit Security, ID Dataweb, IBM, LexisNexis Risk Solutions, Akamai, Experian, Group-IB, Human, Arkose Labs, and Ping Identity are the Product Leaders. This report focuses on solutions that deter the most common fraud types experienced by eCommerce merchants

generally: bot-perpetrated attacks, ATOs, NAF, and policy abuse. The leaders identified here are those which provide technical solutions that address the majority of these use cases, including sophisticated orchestration of additional third-party services where needed.

The rest of the vendors appear in the Challengers section. Many excel at multiple areas of the required capabilities but may be missing one or more essential functions. Since many consumer-facing businesses utilize multiple fraud detection and prevention components, organizations that are looking for granular services must consider the individual strengths and challenges of all the vendors surveyed here plus their ability to orchestrate other solutions. A more detailed analysis follows in section three.

Product Leaders (in alphabetical order):

- Akamai
- Arkose Labs
- Experian
- Group-IB
- HUMAN
- IBM
- ID Dataweb
- LexisNexis Risk Solutions
- Ping Identity
- 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. 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 discovered in the course of our research. The vertical axis shows the degree 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 3: Innovation Leadership in the FRIP for eCommerce market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

The Innovation Leaders are LexisNexis Risk Solutions, Transmit Security, IBM, Experian, Group-IB, Sumsub., and ID Dataweb. Most vendors appear in the Challenger area, and there are no Followers. It is important to note that Challengers also usually have one or more innovative features, and each should be considered when looking for FRIP solutions.

Innovative features in FRIP for eCommerce include having multiple capabilities to detect many different kinds of bot-driven attacks, such as credential stuffing, inventory hoarding, ticket scalping, and more; the ability to manage bots since not all bots are bad; the ability to detect and prevent different forms of policy abuse; using GenAI for assistance in building queries, cases, and reports; intuitive interfaces for analyst investigations; easy-to-use orchestration facilities; cutting-edge modalities for behavioral biometrics; deep device level analysis; and more.

Innovation Leaders (in alphabetical order):

- Experian
- Group-IB
- IBM
- ID Dataweb
- LexisNexis Risk Solutions
- Sumsub
- Transmit Security

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the number of transactions evaluated, the 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 the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, 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 4: Market Leaders in the FRIP for eCommerce Market

Market Leaders in FRIP for eCommerce include LexisNexis Risk Solutions, Experian, Akamai, and IBM. All are large companies that are doing well at helping customers protect against fraud. They also have mature and relatively full-featured offerings in the FRIP for eCommerce space, which helps drive their market share.

The majority of the firms are Challengers in the FRIP for eCommerce market. Many of them are FRIP specialists. Given the increasing amount of and variety of fraud affecting merchants, there is room for growth for all these vendors.

Market Leaders (in alphabetical order):

- Akamai
- Experian
- IBM
- LexisNexis Risk Solutions

Product/Vendor evaluation

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

Spider graphs

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

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 third-party services, although this is still uncommon.

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/velocities, transaction locations, payees, exceptions for known travel, transaction item analysis, transaction proximity to other suspicious activities (such as phishing or smishing), discernment of multiple transaction attempts from multiple users from a single device or IP, relationships to known high-risk accounts, and user profile changes. UBA is a key method for preventing ATO, credit card and other payment fraud, and scams.

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 NAF, credit card, and other payment fraud.

Behavioral Biometrics – This measures the presence and sophistication of behavioral biometrics within the solution. Behavioral biometrics are 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 bot attacks as well as a secondary means for preventing NAF and some types of scams.

Bot Detection - 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 challenge methods that require end user interaction, activity signatures, cyber threat intelligence, and manual analysis. Alternatively, some innovative solutions use challenge methods that are invisible to the end user.

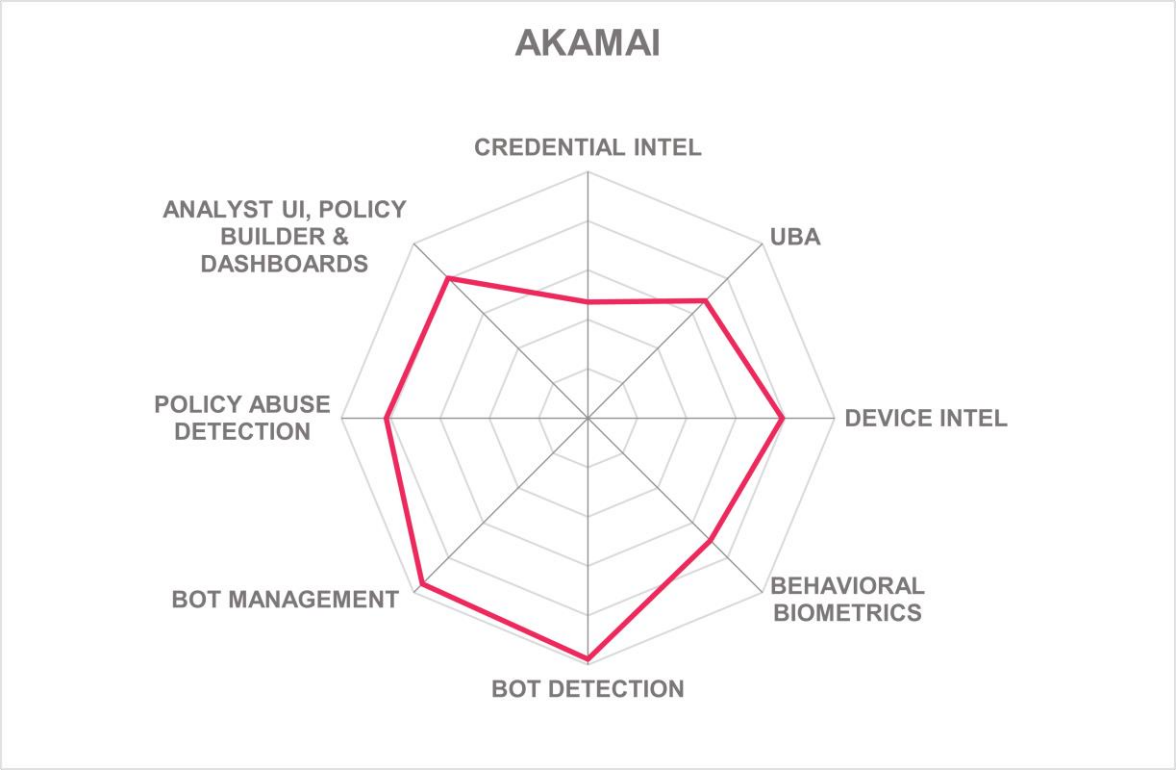
Bot Management - Bot management addresses how the vendor services aid customers in handling bots. Common options are challenging, redirection, and throttling. Advanced bot management includes the ability to deploy sophisticated proof-of-work and/or user-friendly, unobtrusive challenges that improve transaction security but not at the expense of the user experience. Other bot management techniques include redirecting known or suspected bots, throttling, and enforcing allow- and denylists. Bot detection and management can help prevent automated ATO and NAF attempts.

Policy Abuse Detection – This heading rates the variety of policy, platform, website, and subscription abuse types that vendor solutions purport to deter, and the methods employed for such deterrence. Examples of policy abuse include fake reviews/comments/ads/jobs/etc., chargebacks, excessive inventory checking, refund/return abuse, promotions abuse, and more.

Analyst UI, Policy Builder & Dashboards – This metric considers solutions' management and analyst interfaces. Analyst UIs include case management, search features (which may be enhanced by GenAI), timeline/map/graph views, and the ability to drill down into details and pivot on attributes. Policy builders are generally of two types: a modern flowchart style into which authors can drag-and-drop elements and select attributes and name/value pairs; or an older, sequential list of conditions, selected via drop-down lists and connected with logical operators. The flowchart style is preferred due to its more intuitive nature. Dashboards should present the most pertinent info in an efficient way and allow customization per user. Dashboards enable analysts to correlate and visualize emerging fraud trends, highlight new abuse vectors and attacker infrastructure shifts, and track known and suspected fraudulent credentials, devices, and payment instruments. The Dashboard rubric also includes a measure of the types of standard reports available, and the ability to customize reports as needed. This quality of this component is essential for facilitating investigations, providing succinct but useful information, and crafting risk evaluation policies.

Each of the product/service sections below follows a similar structure in order to make it easier for readers to compare features between vendors. Note that this differs from the Leadership Compass – Fraud Reduction Intelligence Platforms for Finance, in that, IDV, name/watchlist screening, support for advanced financial fraud detection, and support for financial framework compliance are mostly omitted (although built-in IDV capabilities are mentioned). Rather, this report focuses on the remaining basics plus the ability to manage bots and detect various forms of policy abuse against websites.

Akamai – Account Protector, Bot Manager, Brand Protector, Content Protector, Client-Side Protection & Compliance



Leader in

Akamai Technologies is a cloud and security provider headquartered in Cambridge, Massachusetts, in the US. 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's globally distributed infrastructure, 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 part of their Content Delivery Network (CDN) platform, rather than an API-driven SaaS, and are run from their own facilities and public Infrastructure as a Service (IaaS) providers across global datacenters. Android and iOS SDKs are available for customer app integration, and JavaScript is used for browser interactions. Costs are based on legitimate traffic volumes for web application security products with zero-overage fixed fees. There is a separate fee for SDK usage. Customer applications call Akamai services via the REST API, and JavaScript Object Notation (JSON) formats are supported.

The platform uses in-network credential intelligence only. This limits its ability to detect NAF and synthetic fraud. In terms of device intel, Akamai examines the basic parameters and can identify known users on new devices. The platform does not support jailbreak or malware detection or SIM swap detection directly. The UBA functions evaluate various attributes like login locations, failed login patterns, transaction locations/patterns/velocities, proximity to suspicious behavior, multiple transaction attempts from multiple users from a single IP, account creation clusters, and relationships to other known high-risk users to discern suspicious activity and prevent ATOs. Data retention policies are compliant with global privacy regulations like GDPR, CCPA, and can be defined per customer. Akamai employs behavioral biometrics, instantiated as SDKs for Android, iOS, Cordova, Ionic, Flutter, React Native, and Xamarin, examining features such as keystroke, swipe, scrolling, gyroscopic, accelerometer, and app usage analysis. Their behavioral biometrics enable bot management capabilities, which also utilize embedded pixels for bot detection, allow distinctions between benign and malicious activities, and support configurable allow/deny lists with throttling, redirection, and challenge-response mechanisms.

Bot Manager can detect, prevent, or manage a multitude of bot types, including inventory/grinch bots, jingle bots, competitive price checkers, headless browsers, social media bots, account creation and credential stuffing bots, and ticket scalping bots. It can also stop bots from leaving fake reviews and comments, inserting malicious ads, posting fake goods on auction sites, committing discount policy, guest checkout, and loyalty program abuse. Akamai also has specific protections against online insurance claims fraud, pharmacy auto-refill abuse, fraudulent appointment bookings for health care systems, online betting, and media content scraping. Akamai employs advanced techniques to identify, classify, and manage AI- and LLM-driven scraper bots. Their solutions are used across nearly all industries.

Akamai's Account Protector helps to mitigate CNP fraud by monitoring abnormalities in user behavior during payment flows. The solution also detects malicious card testing attempts and provides some capabilities for screening for money mule account creation and BNPL fraud. Akamai offers extensive industry-specific support, notably in the travel/hospitality, retail, and insurance sectors.

Their risk engine allows for graphical visualization and configuration of risk evaluation policies. The policy builder interface is intuitive, with sliders for adjusting the weight of risk factors. It can output risk scores with explanations for customer apps. The results from the risk engine can also be packaged as HTTP headers and JSON. Akamai supports REST APIs and webhooks for data exchange, but better API authentication methods should be supported. Akamai does not have ITSM connectors. Akamai's solutions do not currently offer integration with call center systems. Their fraud analytics interface includes customizable, widget-based dashboards for real-time monitoring and a variety of report types, including anomaly and fraud type detection, but it is not designed as a case management platform. Furthermore, the analyst interface employs GenAI to generate executive reports and summaries and supports NL queries.

Akamai is certified against ISO 27001/27017/27018, SOC 2 Type 2, AU IRAP, and UK Cyber Essentials. As a multi-cloud native solution with edge datacenters across four

continents, Akamai's FRIP services are highly scalable. Akamai offers training and support in many languages. Akamai relies on clients to manage consent for processing data attributes and assumes consent through customer relationships. The company employs privacy-enhancing technologies such as data anonymization, pseudonymization, aggregation, redaction, and encryption to secure data. Akamai has customers across various industries, such as insurance, healthcare, travel/hospitality, gaming, retail and eCommerce, media, electronic service providers, advertising, government agencies, telecommunications, and utilities. Akamai's suite of products are well-suited for protecting eCommerce and merchants of many types, due to their thorough bot detection, categorization, and management capabilities. Any modern business with public web presence should strongly consider Akamai's Account Protector, Bot Manager, Brand Protector, Content Protector, Client-Side Protection & Compliance products, particularly those which are already using their CDN.

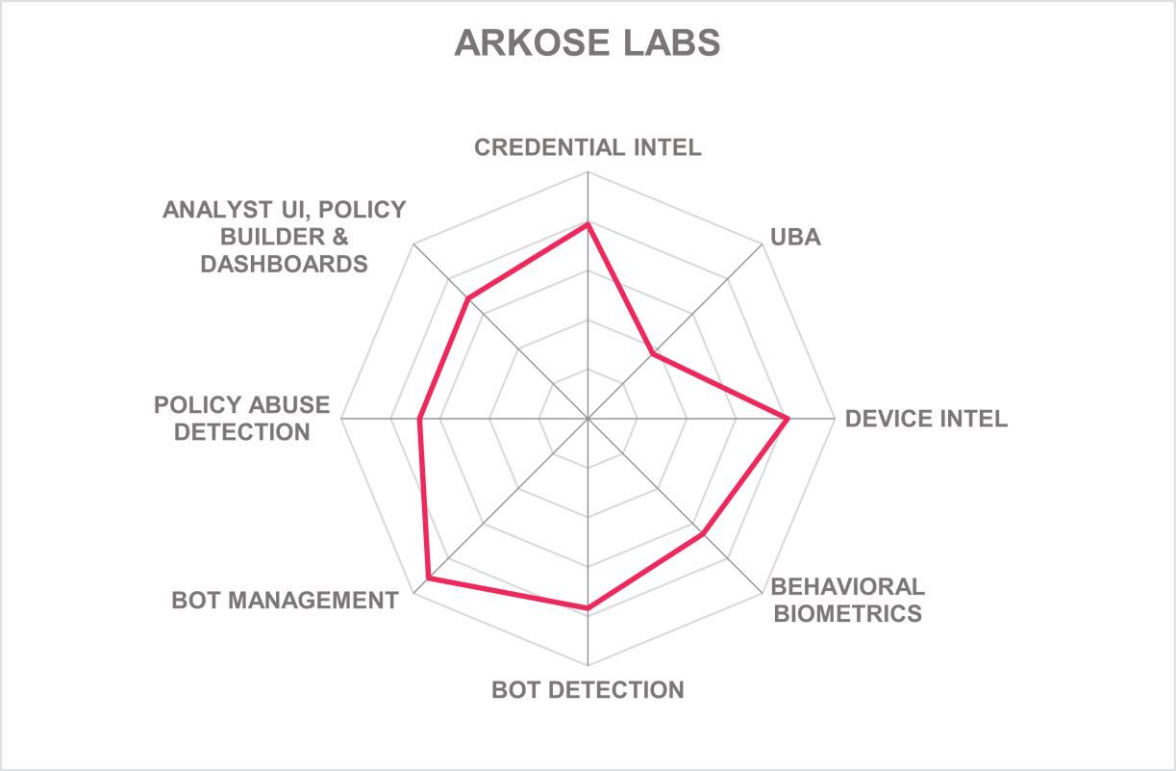
Strengths

- Multiple security certifications
- Highly scalable and performant FRIP services available globally
- Documentation, services, training, and support for many languages
- Fixed fee based on traffic volumes with zero overage protection cost model
- UBA can help prevent some types of credit card fraud
- Uses GenAI for summaries and reports
- Addresses a wide range of bot-perpetrated fraud types
- Prevents many kinds of bot-driven policy abuse
- Advanced bot management capabilities are present, including options for AI/LLM bots

Challenges

- Limited ability to detect NAF and crypto/romance scams
- No call center integrations
- Stronger API authentication mechanisms needed
- Does not address logistics fraud use cases

Arkose Labs – Bot Manager, Device ID, Edge and Scraping Protection, Arkose Email Intelligence, and Arkose Phishing Protection



Leader in

Arkose Labs is a mid-stage startup established in 2016 in San Francisco, California in the US. Arkose Labs has Arkose Bot Manager, Arkose Email Intelligence, Arkose Device ID, Arkose Edge, Arkose Scraping Protection, and Arkose Phishing Protection in their product suite. Their FRIP solution is focused on reduction of ATO and NAF as well as card testing, inventory hoarding, page scraping, loyalty card abuse, API 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 and mitigation. The service is hosted in public IaaS in datacenters around the globe. JavaScript is used for web interactions, and Android and iOS SDKs are present for customer app integration. The pricing model is based on per-transaction rates.

The platform does not evaluate external compromised credential intelligence sources, but it does recognize known good users, which helps to eliminate friction for customers and reduce risk. Arkose Labs' platform includes Email Intelligence, which can prevent NAF (and synthetic identity fraud) from invalid email addresses and domains, and it can detect invalid users at popular email providers such as Gmail, and Microsoft Outlook and Hotmail. Email Intelligence interdicts both volumetric and low-and-slow registration attacks. For device intelligence, it examines device IP addresses, reputations, geolocation, IDs, fingerprints, and performs device posture checks. Additionally, Arkose Device ID offers dual device identification methods, leveraging deterministic and probabilistic identifiers, for long-term recognition and to generate updatable session identifiers; and it generates invisible proof-of-work challenges to protect customers from malicious devices. Arkose Labs performs basic UBA and provides data for third-party applications to do advanced UBA, but does not engage in transaction analysis. Configurable data retention policies can align with privacy regulations. Their SDKs for Android, iOS, and ReactJS support a limited range of behavioral biometric modalities. Arkose Bot Manager has detection measures including both activity signatures and behavioral biometrics. One of Arkose Labs' strong points is its ability to deploy highly intuitive and innovative visual and audio CAPTCHAs, and various challenge methods including proof of work. Mitigation methods are configurable by customers. Its device intelligence and innovative CAPTCHAs power its ATO detection and prevention capabilities.

Arkose Labs can detect and stop many kinds of bot attacks, such as inventory hoarding/grinch bots, jingle bots, price checking bots, social media bots, headless browsers, ad click bots, ticket scalping bots, and account creation and credential stuffing bots. Arkose Labs can prevent bots from posting fake review/comments and jobs. It can detect the use of automation to accomplish ATOs or fake accounts that can lead to loyalty program, guest checkout, and discount policy abuse. Arkose Phishing Protection, a service within Arkose Bot Manager, can deter Adversary-in-the Middle (AitM) attacks, and thus ATOs, by requiring valid tokens from protected clients. Arkose Labs protects many large dating apps and sites by preventing users from interacting with bots on those sites. It is not focused on scam detection. Arkose Labs is used across many industries, including insurance, health care, travel/hospitality, gaming, retails, media, advertising, and utilities. Arkose offers a $1 million warranty.

Arkose Labs does not look for credit card fraud, but it detects chargeback/refund abuse in automated payment fraud and mitigates malicious card testing.

Call center integration is not available. Customers can utilize REST APIs and webhooks, protected by strong API authentication measures, with risk scores and threat categories delivered as JSON. Management interfaces offer detailed reporting, though it lacks ITSM integration. Customers primarily use other products for case management and investigations, with Arkose Labs plumbed into those other tools via API. GenAI can facilitate case description and report generation.

Arkose Labs is ISO 27001/27018 and SOC 2 Type 2 certified. The platform scales effectively, protecting tens of millions of transactions daily using automatic horizontal scaling in IaaS. Their 99.9% uptime SLA and extensive language support enhanced usability.

Training options include onboarding and workshops. To protect consumer privacy, Arkose Labs uses anonymization, pseudonymization, obfuscation, and encryption. Arkose Labs has customers across sectors such as finance, insurance, healthcare, travel, retail, gaming, media, telecommunications, and government. They also have integrations with Microsoft Xbox, Sony PS5, and various printers, set top boxes (STBs), and Smart TVs. Arkose Labs has excellent ATO prevention and bot detection and management features. Adding credit card transaction fraud detection features would be beneficial. Any organization that is looking to reduce ATOs and bot attacks while significantly improving the customer experience with invisible challenges should have Arkose Labs on their shortlist.

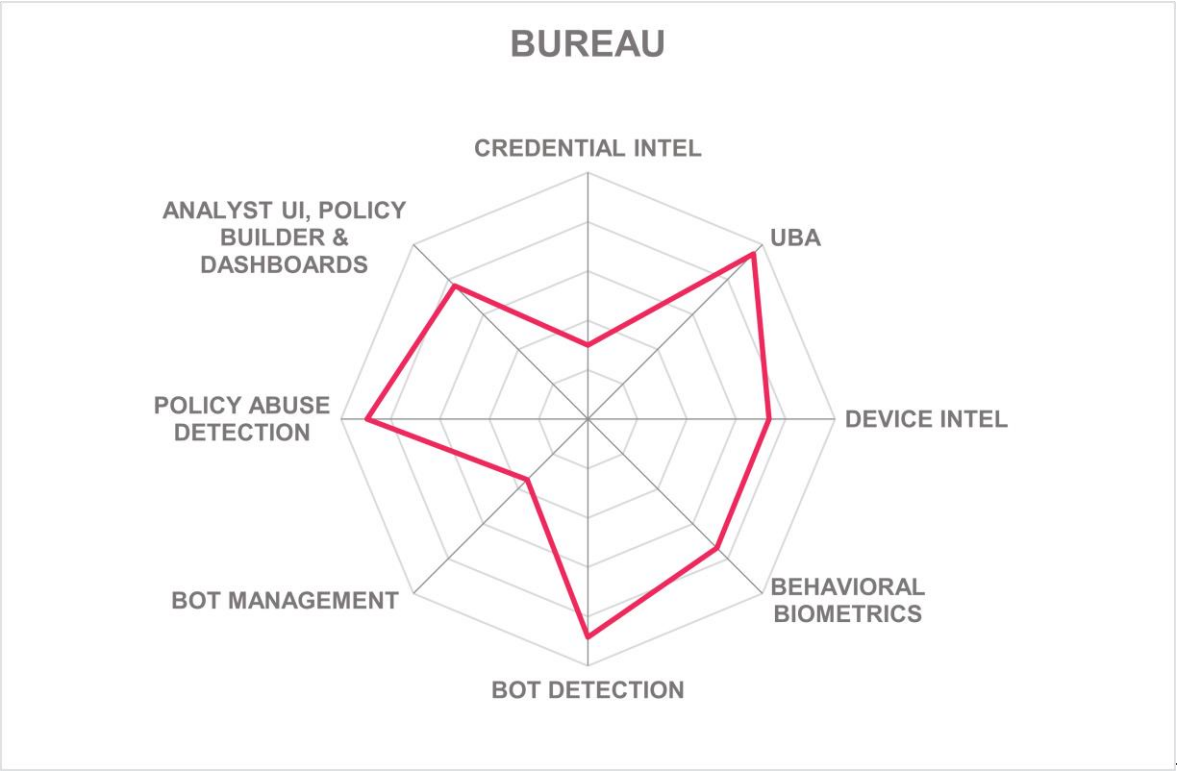
Strengths

- Excellent unobtrusive visual, audio, and proof-of-work CAPTCHAs improve the user experience while reducing fraud.
- Very good bot detection and advanced bot management capabilities.
- Direct integration with popular consumer devices.
- Sophisticated session protection includes TLS fingerprinting and JA3 analysis.
- Improved device intelligence (Arkose Device ID) and behavioral biometrics.
- Includes Email Intelligence that helps prevent NAF and synthetic identity fraud at the time of sign-up.
- Protects against many types of policy abuse.
- Used across a wide variety of industries.
- Use of GenAI for case descriptions and reports.
- $1M fraud detection warranty.

Challenges

- UBA does not include transaction level analysis; compromised credential intelligence could be expanded from Email Intelligence to include additional signals.
- Focused on the bot validation phase, rather than credit card fraud (CNP) analysis, but it can detect card testing attacks to prevent validated cards from progressing to actual fraud.
- Additional behavioral biometric modalities would be useful.

Bureau – Device Intelligence & Behavioral AI, Identity & Document Verification



Bureau was established in 2020 in San Francisco, California. They are a mid-stage startup focused on several aspects of fraud prevention, including IDV, device intelligence, UBA, behavioral biometrics, and bot detection. The majority of their customers are in India, Middle East, and Southeast Asia. The backend service is SaaS, which runs from a single Tier 1 IaaS provider from data centers in the US, India, and other locations in Asia. The client portion is delivered by JavaScript and SDK. Service pricing is a mix of per-user and per-transaction fees, and fixed cost contracts are also available.

Bureau has IDV features, including an app and SDKs (Android, iOS, Flutter, and React Native) for remote onboarding, which do selfie-to-ID photo matching, duplication checks, and OCR scanning with deepfake detection and iBeta2 certified selfie liveness detection. Integrations with multiple third-party IDV services are also available. Bureau supports AML compliance through extensive name/watchlist screening and KYB via LEI lookups. It can detect mule accounts, NAF and synthetic identity fraud.

Compromised credential intelligence is not directly evaluated; rather, Bureau's UBA looks for anomalies indicative of the use of stolen credentials. Device intelligence attributes examined include IP/IP ranges, geo-location, geo-velocity, MNO and Wi-Fi network information, characteristics of SIM/virtual SIM, and device ID/type/fingerprint/reputation. It can perform device posture checks, detect jailbreaks, and determine if a known users is on a new device. It can detect SIM swaps in some markets where they have partnerships with MNOs. Bureau's UBA is quite detailed, assessing login times/patterns/locations, transaction types, amounts, payees, items purchased, velocity and frequency, long-term patterns, proximity to suspicious events, identity verification anomalies, account creation clusters, and relationships to known high-risk accounts. Data retention periods are customer configurable. Their behavioral biometrics implementation includes the standard modalities plus a few innovative ones. These behavioral biometrics, along with embedded pixels and activity signatures, form the basis of their bot detection capabilities.

Bureau can detect a wide variety of bot-driven attacks, including jingle, inventory hoarding/grinch, price checking, social media bots, ad insertion/click, account creation and credential stuffing, file downloading, and ticket scalping bots. Although bot detection seems thorough, bot management is not present. Through browser fingerprinting and Behavioral AI intelligence, it can detect headless browsers. It looks for policy abuse including the posting of fake reviews/comments/goods for sale, guest checkout, loyalty program, and discount policies. In terms of credit card use cases, Bureau looks for stolen card usage, BNPL abuse, card testing, chargeback and refund abuse, and fake delivery fraud.

Customers can create and edit risk policies via drag-and-drop orchestration, selection of conditions and values, and applying logical operators to those conditions. Templates are available. Thus the interface is flexible but can be complicated. Customers can also change the weighting of risk factors. It outputs risk scores and can be configured to return rejection rationales. Bureau also supports packaging of risk results as JWT claims. Webhooks and REST APIs are supported, but API security needs to be strengthened. The dashboard is not configurable by customers. Standard fraud and case management reports are available. The analyst interface features a highly useful identity graph view. Connectors for ITSM and call center software are not available.

Bureau states that they have achieved ISO 27001 and SOC 2 Type 2 certifications. The API is protected by rate-limiting functions and IaaS WAF and other tools. They utilize standard IaaS auto-scaling to ramp up for peak customer demand. Initial setup services are limited to providing SDK documentation and walkthroughs. Documentation and support are provided in English. Customers are responsible for data and consent collection.

Bureau combines good IDV, device intel, UBA, and behavioral biometrics functions into a single solution, which also supports orchestration of third-party services. It currently lacks compromised credential intelligence, bot management, and credit card fraud detection. It can detect the most common bot-perpetrated attacks and several forms of policy abuse. Service and support should encompass more languages and time zones. Although the majority of their customers are in Asia and the Middle East, organizations in any region who need detailed UBA may want to consider Bureau's features.

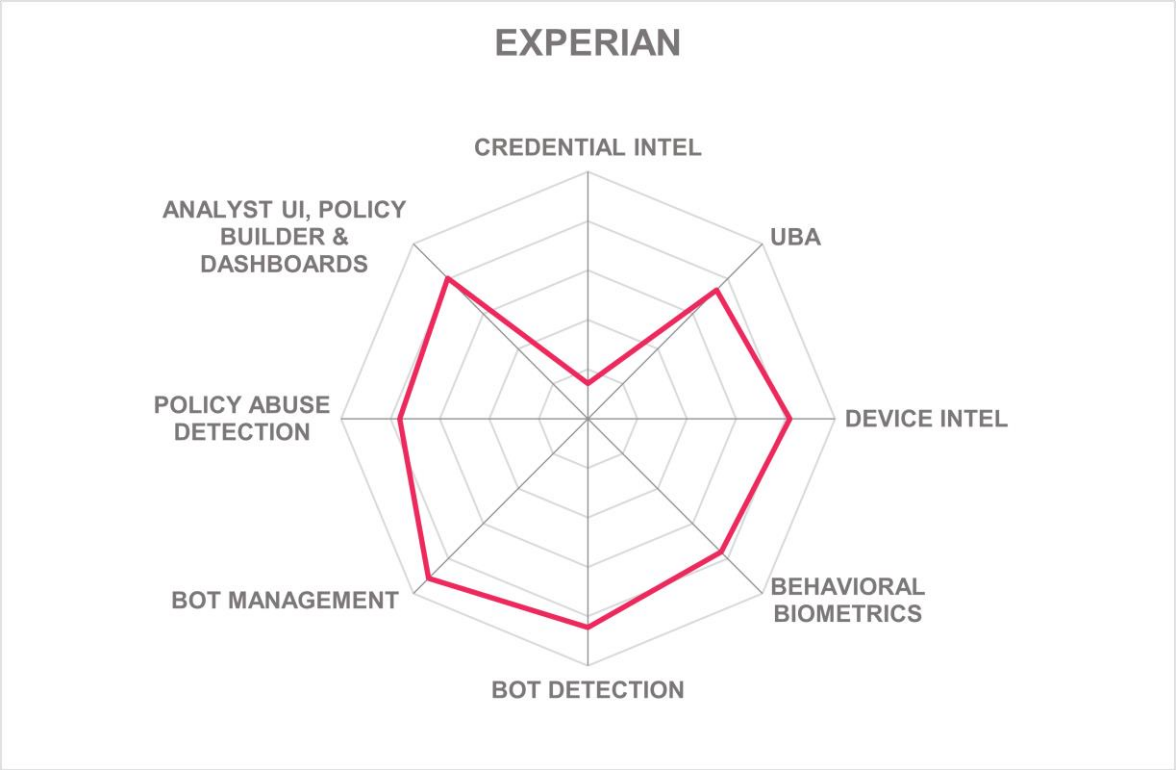
Strengths

- Built-in IDV services
- Deeply granular UBA evaluates many transaction attributes, including some that are not addressed by competitors
- Good behavioral biometrics
- Bot detection covers most of the common attack types as well as policy abuse detection
- Excellent analyst interface facilitates investigations

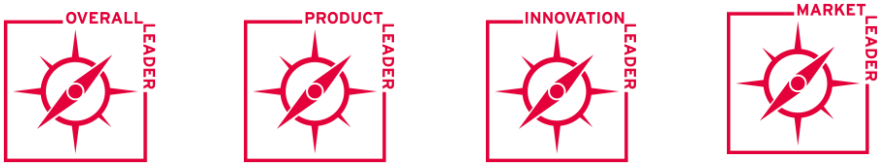
Challenges

- Does not consider compromised credential intelligence
- Bot management is missing
- Should provide more extensive setup services
- Omits some types of credit card fraud detection
- Most presence in India and Southeast Asia, but growing

Experian – CrossCore



Leader in



Experian was founded in 1996 and is headquartered in Dublin, Ireland. It is one of the “Big Three” credit rating agencies, processing information on 200 million businesses, 10+ billion credit applications, and over 1.5 billion people worldwide annually. It provides credit history information to financial institutions, and analytics and marketing information for other customers. For fraud prevention, CrossCore on Experian Ascend Platform addresses IDV, UBA, device intelligence, behavioral biometrics, and bot detection. CrossCore on the Experian Ascend Platform, which is a unified fraud, credit, and analytics platform, and is designed to aggregate various fraud sources to consolidate decision making for Experian customers at both account opening and transaction time. CrossCore runs as SaaS in globally distributed datacenters in their own facilities and across multiple IaaS providers. It

can also run on-premises or in customers' private clouds. JavaScript and SDKs capture user information for analysis. Pricing is based on numbers of users or transactions, or numbers of servers (for on-prem and private clouds), and by the types of fraud covered. Bundle pricing is also available.

Experian provides robust IDV services built into CrossCore on Ascend Platform, leveraging extensive consumer data as well as integrating with third-party IDV providers. The solution offers a mobile app and SDK for identity document validation (OCR and barcode capture), innovative liveness detection methods, and NFC reads of chipped credentials, offering excellent IDV support for all kinds of consumer-facing organizations. CrossCore does not yet have compromised credential intelligence, but this is on the roadmap. It has thorough device intelligence capabilities, including IP address and reputation, geolocation, geo-velocity, device fingerprinting and posture checks. Their solution can detect evidence of malware and can recognize when a known user accesses a new device. The UBA implementation considers frequency/time/locations of logins, transaction item analysis, transaction velocities/frequency/locations, IDV anomalies, account creation clusters, proximity to suspicious events, and relationships to known high-risk accounts. Customers can define their data retention policies. Experian's behavioral biometrics can analyze the most common modalities, and customers can utilize third-party solutions as well. The sum of device intelligence, UBA, and behavioral biometrics address ATO detection and prevention. This provides the basis for their bot detection and management functions, thereby allowing customers to maintain allows/deny lists and ban, throttle, or redirect bot traffic as needed.

Experian can discover inventory checking/hoarding, jingle, social media, account creation and credential stuffing, ad click, and ticket scalping bots. It can detect and alert on bot-driven fake review/comment posting, fake goods for sale posting, and discount/guest checkout/loyalty program abuse. For managing bots, customers can maintain allow/deny lists and ban, throttle, or redirect bot traffic as needed.

CrossCore on Experian Ascend Platform detects and prevents CNP fraud by examining products/SKUs, bill-to/ship-to discrepancies, anomaly detection, and geolocation checks. It can also detect CNR and counterfeit card fraud using device intelligence and behavioral biometrics. The platform mitigates chargeback and refund abuse, as well as malicious card testing attempts. CrossCore can detect NAF and synthetic identity fraud through a combination of identity verification and risk assessments.

The platform's risk engine offers graphical visualization and configuration of risk evaluation policies with customizable weighting of risk factors. CrossCore provides non-prescriptive risk assessment outputs to customers to inform their decisions. Results can also be packaged as SAML assertions, JWT claims, or HTTP headers. REST APIs with JSON/XML payloads are supported, and those connections are protected by strong authentication methods. Case management is available in their adjunct products, FraudNet and Hunter. No connectors are available for third-party ITSMs. CrossCore includes limited call center integration capabilities through third-party partnerships. Data can be exported as .csv files, and dashboards are configurable by customers. GenAI assists in creating case and event descriptions, reports, and interactive query capabilities, in order to expedite fraud detection and management workflows.

Experian has certifications for ISO 27001, SOC 2 Type 2, PCI DSS, and HIPAA. The platform has the capacity to handle millions of transactions daily via auto-scaling across its IaaS infrastructure. Customizable SLAs are offered. Experian provides extensive training for administrators and offers support in multiple languages, including English, German, and Mandarin. The product supports many industries, such as finance, healthcare, retail, and telecommunications. Experian employs data protection technologies such as anonymization and encryption. Experian, as a leader in all categories, is a contending FRIP solution for any organization with public web presence.

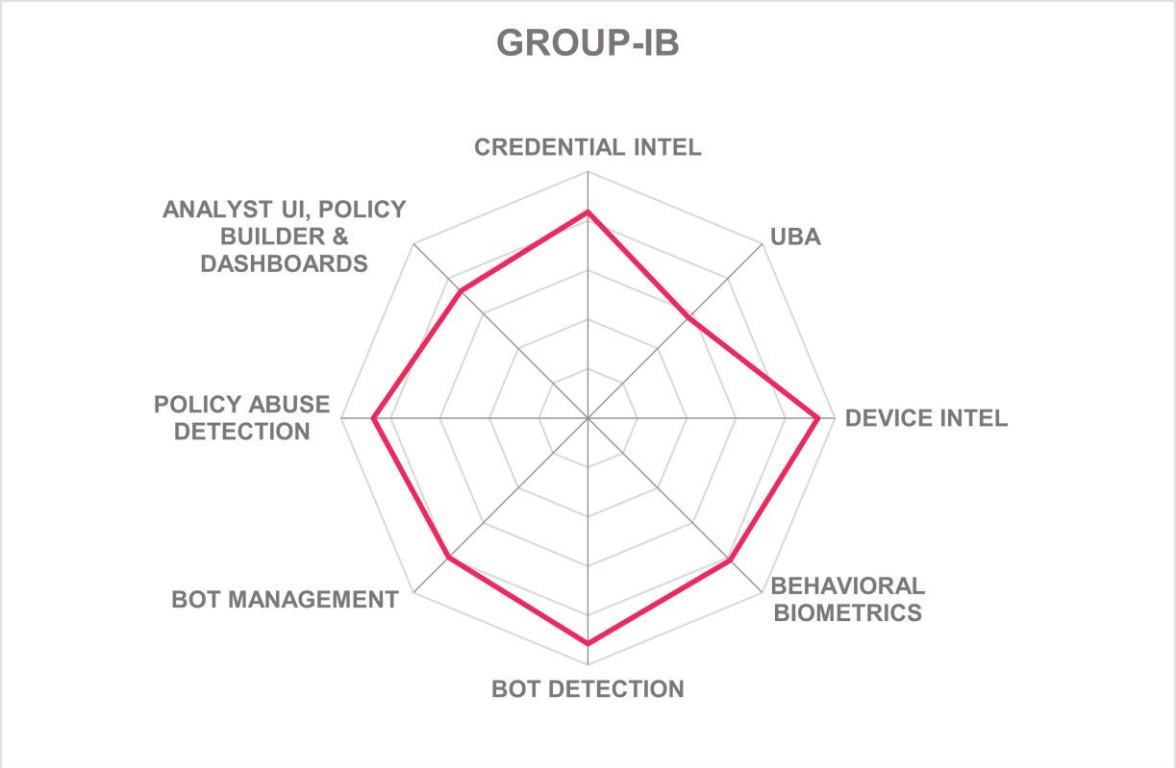
Strengths

- Excellent IDV features including remote onboarding app with innovative liveness detection features and third-party IDV service connectors.
- Device intelligence encompasses most observable attributes
- Good support for credit card fraud detection includes granular analysis of transaction details
- Risk analysis output can be packaged as SAML, JWT, or HTTP headers
- Provides protection against many kinds of bot attacks
- Helps customers prevent many forms of site policy abuse
- Many security certifications
- Widely used across many industries

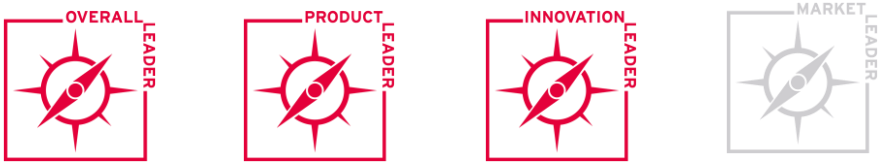
Challenges

- Compromised credential intelligence is still in work
- UBA functions should evaluate additional transaction parameters
- Webhooks and WebAuthn APIs not supported
- No ITSM integrations

Group-IB – Fraud Protection



Leader in



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. The client-side components are instantiated as JavaScript and Android and iOS SDKs. Options for deploying at customer sites or on customer private clouds are available. Subscription costs depend on the number of active users per contract period.

Group-IB's threat intelligence product, which uses dark web monitoring, powers their compromised credential intelligence functions. They exchange credential information with

Europol and Interpol. Their implementation of device intelligence looks at the full range of available attributes and it can detect known users on new devices, jailbroken devices, and SIM swap attacks. For UBA, Group-IB's solution analyses login attempts, account creation clusters, and relations to known high-risk accounts, but does not get further into transaction details. Device intel, credential intel, UBA, and their new BioConfirm feature (biometric authentication) enable ATO detection. The SDKs and JavaScript provide behavioral biometrics, including the basic and a few advanced modalities. The behavioral biometrics features, in conjunction with signatures and embedded pixels, comprise their bot detection capabilities. Customers can allow- or deny-list bots, but advanced bot management is left to the customers to implement.

Group-IB can detect, prevent, and/or manage man different types of bots, including inventory hoarding/grinch bots, jingle bots, price checking bots, headless browsers, ad click bots, account creation and credential stuffing bots, ticket scalping bots, and email harvesting bots. Group-IB protects client websites against malicious ad insertion, gift card cracking, fake reviews/comments, fake job postings, fake goods posted on auction and sales sites, discount policy abuse, loyalty program abuse, and guest checkout abuse. Group-IB also helps protect users against crypto, travel, and dating/romance scams. It can also detect shipment diversions. Their solution is used by companies in the insurance, health care, travel/hospitality, gaming, retail, media, advertising, telecom, and utilities industries.

For credit card fraud protection, the platform can identify and prevent CNP fraud and card-testing tactics. It addresses chargeback and refund abuse through monitoring and behavioral analysis.

Group-IB has the ability to detect if the user is on a call, get the caller ID, and determine if remote access tools are involved. It can share this information with customers' call center software if configured properly. They have expended considerable research effort to be able to detect anti-detect browsers, which are increasingly used by fraud rings, and virtual camera software, which is used for deepfakes. The risk engine is customer configurable; risk factors can be weighted as needed, and it outputs scores and/or decisions and explanations. It cannot output decision results as tokens. REST is the only API type supported, and strong authentication is required for API access. The dashboards and analyst interface are well-designed with multiple views, including user, device, and account graphs, to make investigations easier. A connector for Atlassian JIRA is available.

Group-IB report they have both ISO 27001 and SOC 2 Type 2 certifications. They use standard IaaS auto-scaling techniques to meet fluctuating customer demands. The SLA for service uptime is lower than the industry average. Documentation and support are available in the most common languages. Initial setup support is provided, and fraud analyst support can be provided by their professional services team. For data privacy, only pseudonymization techniques are used. Group-IB is still building back after the split with the Russian entity. They are mostly focused on the finance world but also have a significant presence in i-gaming and other industries. Their target regions are EMEA and APAC. The investigative interface is top-notch. Any organization in those regions that is looking for advanced fraud investigation tools will want to check out Group-IB's features in more detail.

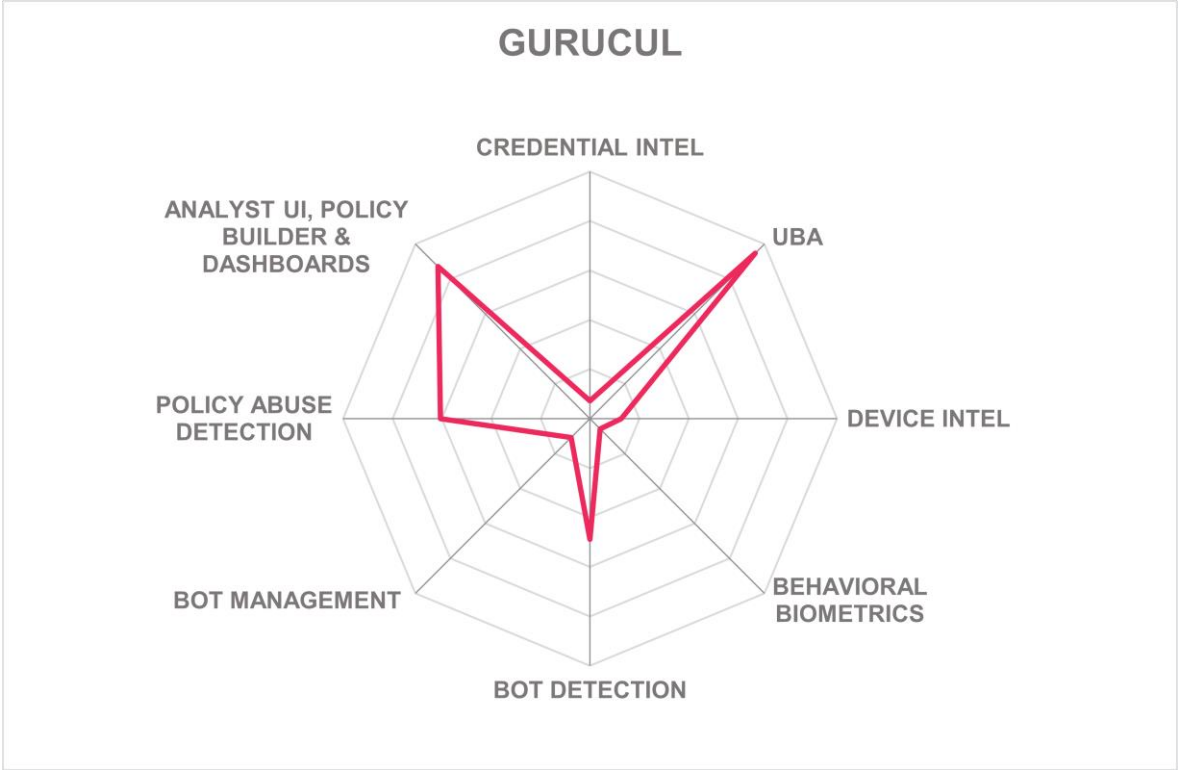
Strengths

- Excellent analyst UI with highly functional device/user/transaction graph
- Dedicated support for each client
- Credential intelligence sharing with Europol and Interpol
- Extremely detailed device intelligence capabilities including active call detection
- “Anti-detect” browser and virtual camera detection
- Detects credit card fraud and scams; BioConfirm can stop CNP fraud
- Protects against a wide range of bot-perpetrated attacks and policy abuse
- Broad language support

Challenges

- UBA/transaction analysis should evaluate more risk factors
- Additional API types could be supported to improve interoperability
- Additional privacy enhancing technologies should be employed to facilitate compliance with global privacy regulations

Gurucul – REVEAL Fraud Analytics



Gurucul was founded in 2010 and is a privately owned company headquartered in Los Angeles, California in the US. Gurucul has a suite of products and services including SIEM, UBA, Open XDR, Network Traffic Analysis (NTA), Network Detection & Response (NDR), 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 third-party FRIP services to gather and send information to Gurucul's Fraud Analytics data lake. Gurucul has hundreds of connectors through which login and transaction data can be imported for analysis. They do not provide JavaScript or SDKs for clients. Gurucul's SaaS runs in a public IaaS provider with global datacenters. The solution can be deployed by customers as VMs or containers on-premises or in any IaaS cloud/environment. Service pricing is based on the number of accounts monitored.

Compromised credential intelligence is not provided, but customers could configure those feeds and Gurucul Fraud Analytics could evaluate that. Since JavaScript and SDKs are not provided, it cannot directly collect device intelligence or behavioral biometrics; however, it can analyze the common attributes if customers are using other, separately procured

sources of device and behavioral biometrics information. This means that bot detection would also indirectly be possible, and bot management would be left to downstream applications. If technical requirements are met, Gurucul can infer the presence of inventory hoarding/grinch bots, jingle bots, price checking bots, headless browsers, ad click bots, and account creation and credential stuffing bots. It can help with determining if reviews and comments are bot-generated by looking for posts from the same IP addresses. It can detect account ban evasion techniques. Loyalty program and guest checkout abuse can be detected. Gurucul helps insurance companies with finding claims fraud. Gurucul Fraud Analytics is one of the few products that can be configured to look for most types of logistics fraud.

Detection of ATO events by Gurucul is possible but would also depend on third-party product integration. It can look for synthetic identity fraud in data from customer transaction and IAM systems. Within Gurucul Fraud Analytics, customers can set data retention policies on imported data to meet their business and regulatory requirements. If complete transaction logs are provided, Gurucul Fraud Analytics detect the various flavors of credit card fraud and provide input to 3DS2 ACS and PSD2 SCA systems.

Gurucul's competitive advantage is in UBA. It has advanced ML-based detection models that consider a wide range of attributes (if delivered from third-party sources), including login patterns, transaction details such as amounts, payees, locations, times, item analysis, transaction velocity and frequency, identity and address inconsistencies, relationships to known high-risk accounts, and more. 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. Call center integration is possible, and there are connectors for multiple ITSM solutions. REST APIs are supported, and results of risk analyses can be packaged into SAML assertions, JWT claims, OAuth2 grants, and HTTP headers.

Gurucul has obtained ISO 27001 certification and is working on SOC 2 Type 2 now. They offer assistance for initial setup and fully managed services. The supported languages are English, German, French, Spanish, Chinese, and Arabic. Privacy regulatory compliance depends on how customer applications are configured. Gurucul Fraud Analytics is powered by its highly flexible and capable UBA functions. It is not a complete FRIP solution, as it relies on external components, including in some cases other FRIP solutions. Organizations that need a good investigative interface or the level of sophistication in transactional risk analysis and scoring may want to consider Gurucul Fraud Analytics in conjunction with other products.

Strengths

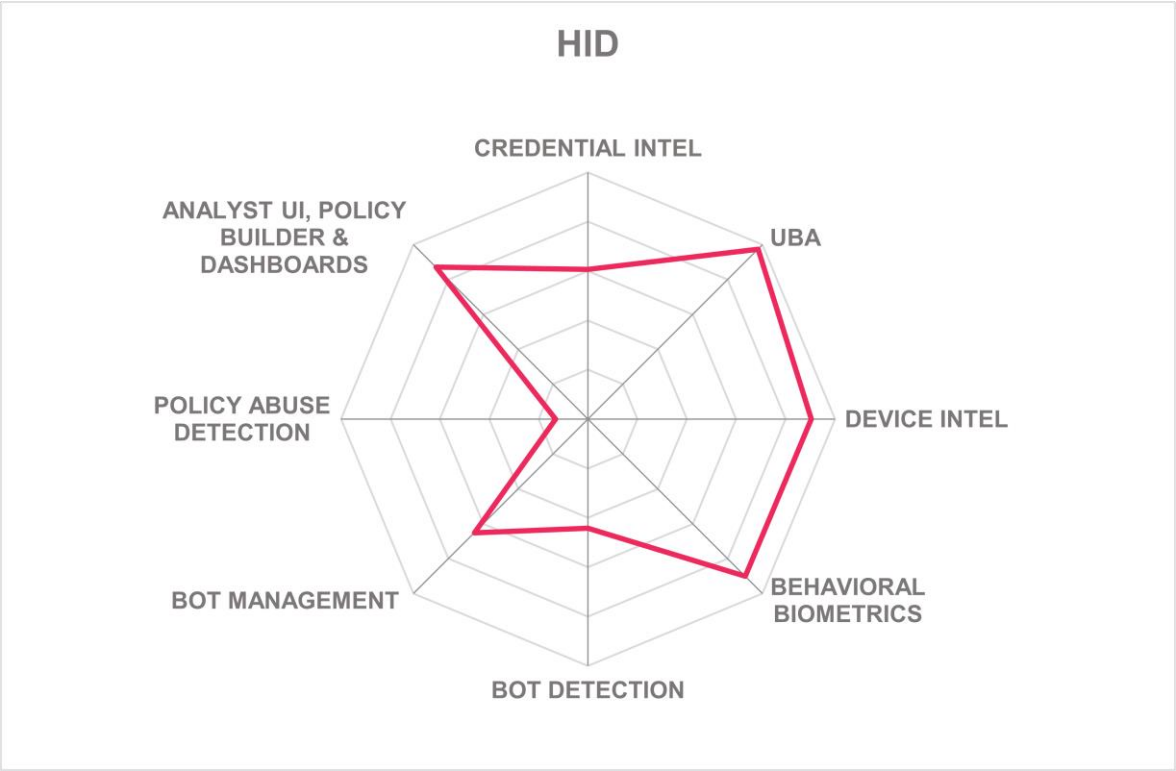
- Excellent ML-based UBA functions are applied to transactional risk analysis
- Hundreds of connectors for third-party security, identity, LoB/transaction processing solutions, call center, ITSM, and many other solutions
- Risk scores can be output in multiple standard formats
- Gurucul Studio™ allows customers to extensively edit and create new detection models from templates.

- Detects some forms of bot-perpetrated attacks and policy abuse
- Can be configured to look for logistics fraud and insurance fraud

Challenges

- Not a full FRIP solution; does not provide JavaScript or SDKs for telemetry collection
- Lacks compromised credential intelligence
- Device intelligence, behavioral biometrics, and bot detection are not present, although it can analyze such data if provided by third-party products

HID – Authentication Platform, Risk Management Solution, Identity Verification Service



HID is a subsidiary of ASSA ABLOY Group AB of Stockholm. HID's headquarters are in Austin, Texas in the US. With over 4,500 employees worldwide and international offices that support more than 100 countries, the company develops highly secure solutions for IAM. These include physical access controls systems, smart identity card manufacturing, credential issuance and management, biometric authentication, 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 Identity Verification Service (IDV) and the Risk Management Solution (RMS), supported by the Authentication Platform, delivers advanced fraud detection and prevention, which combines ID proofing, credential and device intelligence, behavioral biometrics, and UBA. HID's Authentication Platform is available for both consumer and workforce, and supports a wide range of higher security authenticators, including phishing-resistant FIDO2-certified smart cards and security keys. It can be installed on customer premises or in IaaS, and their SaaS is hosted in a Tier 1 IaaS provider in both EU and NA regions. Client-side components are

delivered via JavaScript and Android and iOS SDKs. Pricing options include per-registered user, per-server, and per-transaction, depending on the deployment model.

The HID Identity Verification Service includes a mobile app for document analysis and matching as well as facial recognition with passive liveness detection. The solution leverages in-network compromised credential intelligence through HID's RMS. The client-side elements can collect the full range of device intelligence attributes (including device type, location, time, and more) and perform device posture checks. It can determine if malware is present and if known users are using new devices. HID's UBA is exhaustive, considering login patterns and transaction details such as amounts, payees, items, locations, velocity and frequency, proximity to suspicious behaviors, and relationships to known high-risk accounts. Behavioral biometrics are provided via an integrated OEM partner and the modalities include all the basics plus a few innovative techniques. The ML-enhanced detection features provided by its device intel, UBA, and behavioral biometrics capabilities enable ATO captures. The combination of behavioral biometrics and activity signatures enable bot detection. Allow- and deny-listing make coarse-grained bot management possible.

HID offers protection against headless browsers, account creation and credential stuffing bot attacks, ticket scalping bot, email address harvesting bots, and file downloading bots. It does not address inventory hoarding bots, jingle bots, price checking bots, or social media bots. It also does not provide protection against fake review/comments/goods or loyalty program abuse, discount policy abuse, guest checkout abuse, or gift card cracking.

HID Approve supports EMVCo 3DS2 and EU PSD2 compliance and can detect CNP, CNR, APP, and BNPL fraud. HID Approve and passkeys can be used to authenticate payments instead of weaker methods such as SMS OTP. Their solution can detect synthetic identities and NAF. Moreover, HID can protect government customers against benefits fraud. Together with HID's RMS, itcan also be instrumental in detecting crypto, romance, and travel scams and insurance fraud. HID Global solutions are used in many industries, including finance, insurance, health care, travel/hospitality, gaming, retail, media, and telecom.

HID's suite can work with call center software, enabling active call detection and providing real-time call risk info to customer fraud analysts. The risk engine allows customers to configure policies easily and set weights on risk factors. API types supported include REST, SOAP, Webhooks, and WebAuthn, and multiple strong API authentication mechanisms are available. Risk decisions can be packaged as JWT claims, OAuth2 grants, and OIDC flows. Case management is built-in, and connectors are available for JIRA and Salesforce Ticketing. The dashboard is configurable. Many reports are available and more can be created if needed.

HID's SaaS solutions use IaaS auto-scaling mechanisms and are protected against DDoS and protocol-specific attacks. They have achieved a number of security certifications, including ISO 27001/27018, SOC 2 Type 2, and CSA Star Level 2. Training, initial setup and incident handling are available. Documentation and support are available in English, German, French, and Spanish. HID uses PII de-identification, pseudonymization, redaction, and encryption for privacy protection. HID has strong IDV features and card issuance

capabilities as well as good UBA. Adding coverage for more bot-driven attacks and policy abuse detection and prevention would be useful. Organizations that are looking for excellent UBA and good investigative interfaces should take a look at HID Global's product suite.

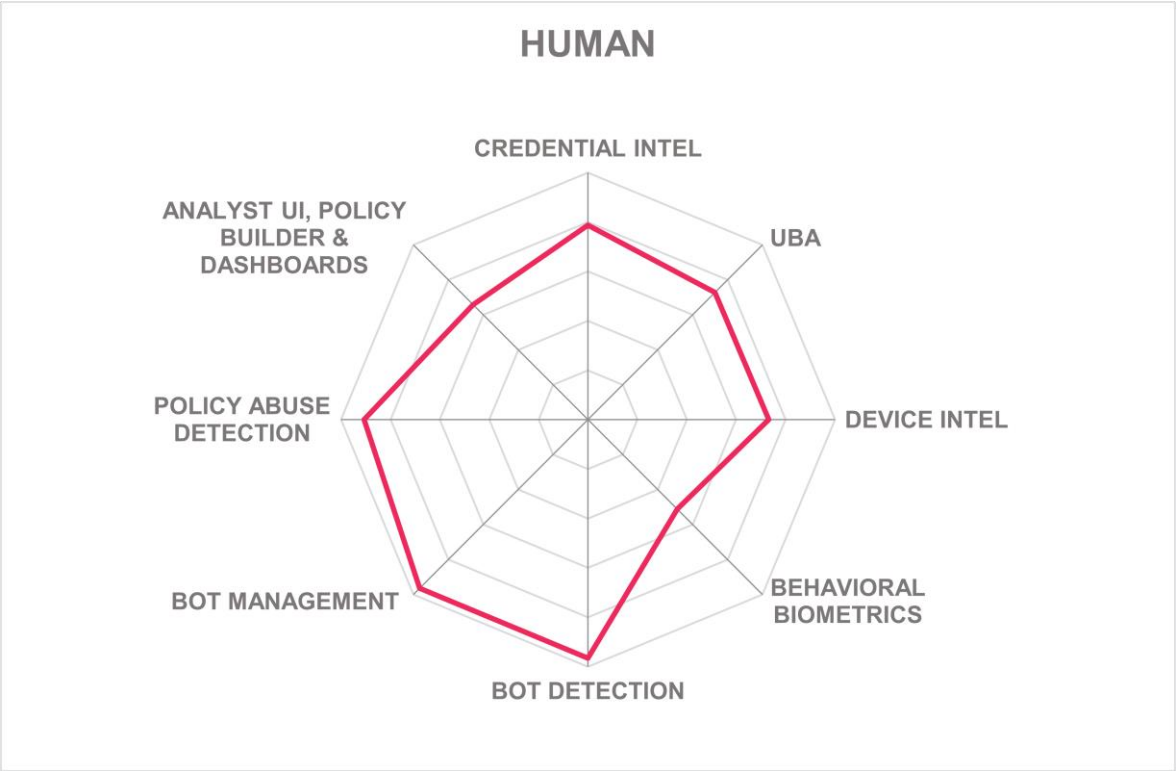
Strengths

- Detects government benefits, credit card fraud, and synthetic ID fraud
- Intuitive drag-and-drop flowchart style rule builder
- Analyst interface pulls together disparate information sources to expedite investigations
- Examines the full list of available device attributes for superior intelligence
- Deep UBA functions look at widest range of transaction details
- Good behavioral biometrics with active call detection for real-time scam detection
- Enables risk-adaptive and EU PSD2 compliant authentication to prevent payment fraud

Challenges

- Does not ingest third-party sources of compromised credential intelligence
- Does not look for chargeback abuse or card testing
- Bot handling limited to allow/deny-listing
- Omits coverage for multiple types of bot attacks
- Lacks policy abuse protection

HUMAN Security – Human Defense Platform



Leader in

HUMAN Security was formed in 2012 in New York City in the US and has offices across the US and Europe, as well as in Israel, Canada, India, and Argentina. 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 HUMAN Sightline Cyberfraud Defense, Client-side Defense, Ad Fraud Defense, Ad Quality Defense, Malvertising Defense, and Ad Click Defense. 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. Its Human Defense Platform is hosted in two Top Tier IaaS providers in multiple datacenters on three continents. JavaScript and Android and iOS SDKs comprise the

endpoint components. Pricing is based on the number of users for the Account Protection product, and by the number of requests for the Application Protection product.

HUMAN uses internal and dark web monitoring for compromised credential intelligence. It evaluates most device attributes, including IP, device type/fingerprint, software signatures, geo-location and geo-velocity, and limited device posture checks. Its UBA surveys many login and transaction details, including types, amounts, item analysis, patterns, proximity to suspicious events, and relationships to known high-risk accounts. HUMAN has behavioral biometrics covering most of the common modalities, and their Satori threat intelligence examines traffic and creates bot activity profiles for detecting them. It does have advanced bot management capabilities, including sophisticated invisible, proof-of-work, and human/non-human CAPTCHA challenges as well as redirection and throttling. The combination of device intel, UBA, and behavioral biometrics help prevent ATOs.

HUMAN protects against API abuse, inventory hoarding, jingle bots, price checking bots, headless browsers, ad insertion and ad click bots, social media bots, account creation and credential stuffing bots, ticket scalping, malvertising, file downloading bots, gift card cracking, SEO poisoning, and email address harvesting bots. It can identify and remediate fake reviews, comments, good posted on auction or sales sites, and fake streams/plays (for media clients). It also can prevent many forms of policy abuse, including against loyalty programs, discount policies, guest checkout policies, and account ban evasion. HUMAN can detect and prevent diversion of goods after sales by looking for changes such as altering the delivery address, security questions, or disabling tracking notifications.

HUMAN looks for some types of credit card fraud, specifically CNP transaction attempts, and can help prevent chargeback/refund abuse, and malicious card testing by bots. It does not directly discover synthetic identity or NAF but HUMAN can detect fake accounts irrespective of the type of scam with its combination of detection techniques.

HUMAN’s risk engine has a drag-and-drop rule builder that accepts granular conditional logic. Risk factors are tuned by their own internal operations team. The API is REST-based and supports JWT authentication. HUMAN has case management in the dashboard and analyst interface. It can also accept and create cases from email, Slack Connect, and JIRA. Call center software integration is not available out-of-the-box, but customers can use the Account API to retrieve real-time risk info and pipe it into their solutions. A large number of standard reports are present, including customer plots against industry benchmarks. The analyst interface is efficient, with timeline and graph views for easier investigations, and flexible enough to allow customization if needed.

As a cloud-native solution, HUMAN scales linearly according to load. They have achieved ISO 27001 and SOC 2 Type 2 security certifications. Their services are protected against DDoS and protocol-specific attacks. Training and support services are available in English only. HUMAN uses multiple privacy enhancing technologies to protect customer and consumer data, including encryption, de-identification of data, pseudonymization and redaction. HUMAN offers excellent bot management in addition to bot detection. Organizations that need to protect their web assets and customers against many different flavors of bot attacks and policy abuse should thoroughly evaluate HUMAN’s FRIP solution.

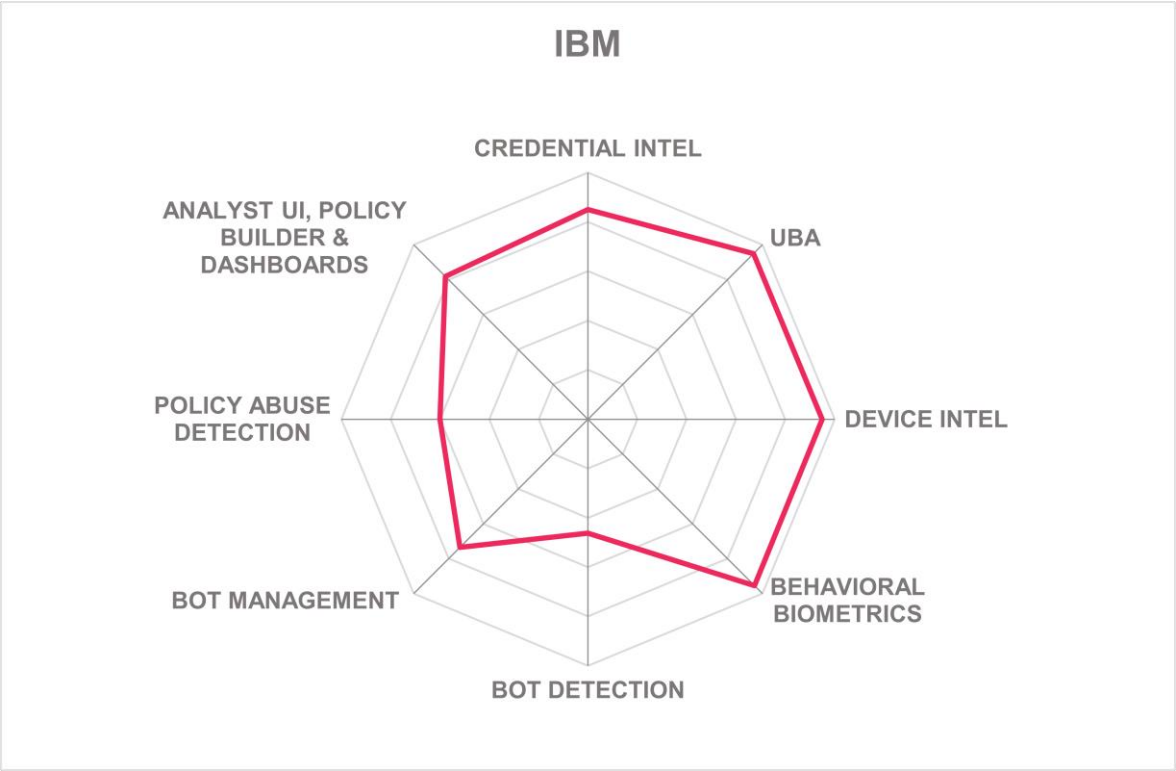
Strengths

- Looks for credit card fraud and chargeback abuse.
- Leverages in-network and dark web research for compromised credential intelligence.
- Detects and prevents a wide range of bot-driven attacks.
- Advanced bot management options include unobtrusive JavaScript and proof-of-work challenges as well as take-down services.
- Excellent policy abuse detection and prevention capabilities.
- Good analyst interface facilitates investigations; the rule-builder interface is flexible and relatively easy to use.
- Can detect crypto, travel, and romance scam types.

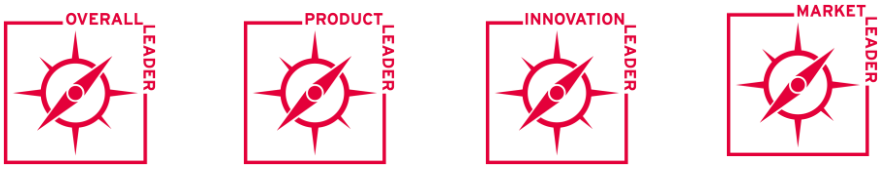
Challenges

- Needs stronger authentication mechanisms for administrators.
- Data retention policies are not configurable.
- Evaluating additional transaction details would be useful for some customers.
- Additional behavioral biometrics modalities should be considered.

IBM – Trusteer: Pinpoint Detect and Pinpoint Assure; and Safer Payments



Leader in



IBM is a global technology and consulting company headquartered in Armonk, New York in the US. 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, IBM's solution for fraud reduction. The integrated suite covers all aspects of FRIP. IBM services are hosted in public IaaS datacenters on three continents. Client-side components include JavaScript, mobile SDKs, and proxies. Pricing options include per-session or by the number of active users.

Trusteer has some built-in IDV features, including a mobile remote onboarding app with basic liveness detection, and integrations with Telesign and AWS Rekognition. IBM uses both in-network and external sources for compromised credential intelligence. Their implementation of device intelligence is complete, covering all expected device attributes, which also allows for SIM swap detection. It has active call-in-progress detection. IBM's solutions excel at UBA, looking at login and a long list of transaction details, including types, amounts, payees, item analysis, velocity and frequency, proximity to suspicious events, relationships to known high-risk accounts, and more. IBM also has very thorough behavioral biometrics, including all basic and some innovative modalities, which inform their bot detection capabilities (along with threat intelligence and activity signatures). Moreover, IBM supports bot management, making recommendations for bot handling to customers over the API, supporting allow- and deny-listing, and redirection. These features combined help prevent ATOs.

Their solution can detect and prevent inventory hoarding bots, jingle bots, headless browsers, ad insertion (but not ad click) bots, and account creation and credential stuffing bots. Other major categories of bot attacks are not addressed. It can prevent bots from posting reviews and comments on protected sites and prevent abuse of loyalty programs, discount policies, and guest checkout policies. Logistics fraud use cases are not covered.

The behavioral profiling engine within Safer Payments detects if users are under duress or if transactions are being initiated under false pretenses. WatsonX AI assistant then can intervene and ask questions of the user such as: "What is the purpose of the transaction?", "How did you meet the person?", "How long have you known them?", "Did they communicate by WhatsApp or Telegram?", "Did they ask you to visit a website or download an app?", or "Were you given a wallet ID?". These measures help shut down crypto/investment and romance scams. IBM's suite looks for CNP and CNR fraud, card testing, and chargeback abuse.

The risk engine can be configured by customers, including the changing of risk factor weights. The rule/policy builder uses an older drop-down menu driven approach. A rule simulator is planned. It outputs decisions, granular risk scores, and reason codes. Decision results can be packaged as JWT claims and HTTP headers. It only supports REST APIs, with limited authentication methods presently. IBM's suite can integrate with contact center software and customers can configure connections to ITSM systems. IBM has built-in case management. Many canned reports are available. The fraud analyst interface has a timeline view but no graph view currently.

IBM's services are protected by a Web Application Firewall (WAF) and API security gateways and support rate-limiting. They have obtained certifications for ISO 27001/27017/27018 and SOC 2 Type 2. The solutions also adhere to Digital Operational Resilience Act (DORA), the New York Department of Financial Services (NYDFS) regulations, and the US Federal Financial Institutions Examination Council (FFIEC) guidelines. As a cloud-hosted service, they use cloud auto-scaling to ramp up to meet peak customer demand. Training and initial setup help are provided, and additional incident handling services can be purchased as needed. The products support many languages. Data is protected using the full gamut of privacy-enhancing technologies. IBM's offering in

the FRIP for eCommerce space covers the basics very well and also has innovative features that consumer-facing organizations will find compelling. Therefore, organizations in any industry should have IBM on their list for fraud protection RFPs.

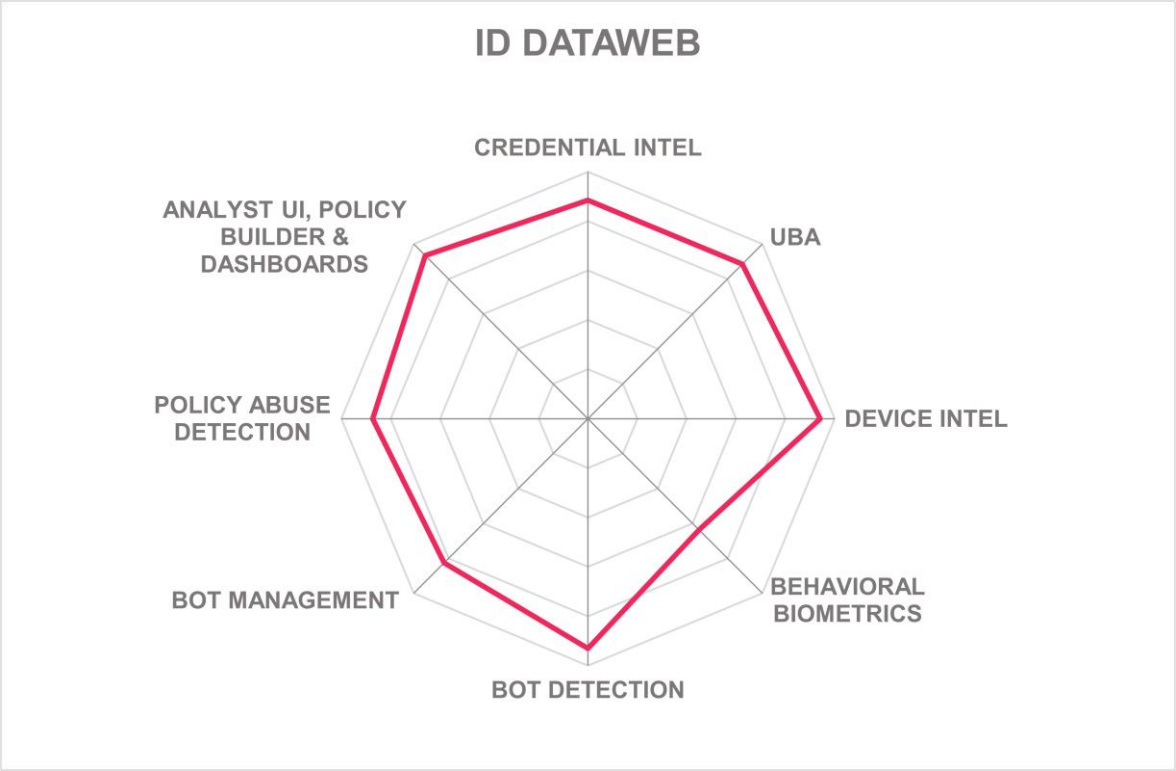
Strengths

- Supports credit card fraud detection.
- Deeply granular transaction analysis examines broad range of risk factors.
- Thorough device intel, behavioral biometrics, and WatsonX-powered AI for real-time scam detection and interdiction.
- Excellent behavioral biometrics including some leading-edge mechanisms.
- Good set of bot management options are present.
- Can be used for policy abuse protection.
- Innovative use of GenAI for natural language queries and customer scam prevention.

Challenges

- It should address a wider array of bot-driven attacks.
- Additional biometric modalities for liveness detection would enhance the product.
- Support for more API types and authentication methods would increase interoperability.
- Identity graph view for fraud analysts would be helpful.

ID Dataweb – AXN Platform



ID Dataweb was founded in 2011 and is headquartered in Northern Virginia, in the US. ID Dataweb is a late-stage startup that was initially backed by venture capital. The company's Attribute Exchange Network (AXN) product 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 via orchestration of built-in and OEM'd products. The solution is SaaS-based and is hosted in US datacenters in a public IaaS provider. The client side is made up of JavaScript and SDKs, and they also offer a fully hosted solution based on either OpenID Connect or SAML. This allows easy integration with most identity tools which also support identity standards. Service pricing is per-transaction, depending on the type of attribute services requested.

ID Dataweb excels at identity verification. It has a mobile app for remote onboarding and IDV that uses leading-edge, iBeta certified liveness detection methods. ID Dataweb uses internal compromised credential signals and can ingest external sources. Its SDKs, JavaScript, and partner integrations pull in the complete range of expected device attributes for analysis. Moreover, it can detect jailbroken devices, known users on new devices, and SIM swap attacks. ID Dataweb performs granular UBA, considering login patterns and many

transaction details, including types, amounts, payees, item analysis, velocity and frequency, location, proximity to other suspicious behaviors, multiple attempts from multiple users on the same device, and relationships to known high-risk users. For behavioral biometrics, ID Dataweb uses an OEM'd leading product to evaluate the most common modalities for risk. These functions work together to deter ATOs. Behavioral biometrics plus activity signatures and embedded pixels comprise their bot detection functions.

AXN can detect and categorize nearly all the common bots, including inventory hoarding, jingle, price checkers, headless browsers, ad click and insertion, social media, account creation and credential stuffing, file downloading, email address harvesting, and ticket scalping bots. It can address many forms of policy abuse, including fake review/comments posting, fake goods for sale posting, account ban evasion, discounts, and loyalty programs. They also have specific functionality for insurance claims fraud prevention. Customers can allow-list and redirect bots, but other bot management functions are not directly present.

AXN does not address most credit card fraud types, although clients can set up IDV to reduce chargeback fraud. It also does not look for crypto, travel, or romance scams. AXN can detect NAF, synthetic identity fraud, and government benefits fraud.

ID Dataweb facilitates risk intelligence integration with call center software, including provide caller ID, location information, and carrier information. Moreover, MobileMatch can send OTPs to user devices for real-time proof-of-possession. Other integrations are possible via REST (with strong authentication options), Webhooks, and OIDC support.

ID Dataweb has upgraded its decision engine since the last report. The risk engine can output decisions, risk scores, and reason codes; it can also package results as SAML assertions, JWT claims, OAuth2 grants, OIDC flows and HTTP headers. The solution provides many templates which can be modified, and it allows for policies to be constructed via adding conditions and connecting them with logical operators. A flowchart design might make it easier to understand complex policies. Dashboards are configurable, and users enable to drill down into identity and transaction details for investigations, but it does not have an identity graph view or full fraud analyst interface. GenAI is used for creating exec level reports.

ID Dataweb has garnered multiple certifications, including Kantara NIST 800-63 rev 3 IAL attribute services, ISO 27001, SOC 2 Type 2, and HIPAA. As a cloud-hosted service, they leverage IaaS horizontal and vertical scaling techniques to meet customer demand. Documentation and support are available in many languages. Deployment and incident handling support are provided. AXN does not store PII and uses encryption for privacy regulatory compliance. ID Dataweb has a well-rounded approach for FRIP, including detailed UBA, device intelligence, orchestration of third-party services, and excellent IDV capabilities. Organizations that need excellent UBA and device intelligence and that have other bot management solutions should strongly consider ID Dataweb.

Strengths

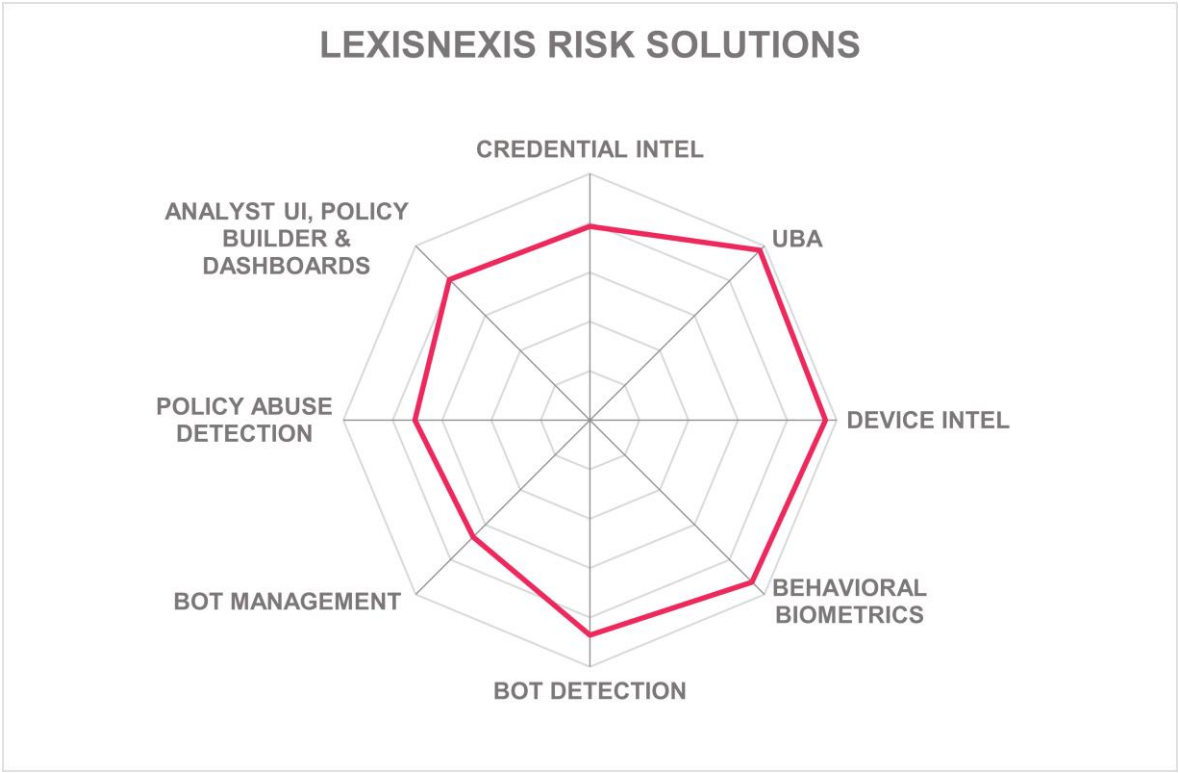
- Excellent IDV features, including a remote onboarding mobile app and SDK that incorporates innovative liveness detection techniques (via partner)

- Can detect government benefits fraud
- Just in Time Step-Up authentication and/or verification can be added to user journeys in high-risk transactions
- Protects against a wide range of common bot attacks
- Detects multiple, prevalent types of policy abuse
- Very thorough device intelligence capabilities, including SIM swap detection
- Granular UBA for transaction risk analysis
- Can output risk scores/decisions in many standard formats
- Many security certifications

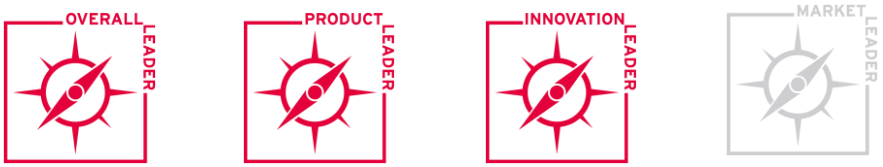
Challenges

- Does not address most credit card fraud types
- Good dashboards but not a complete fraud analyst workbench type interface
- Although instances could be deployed globally, still only hosted in US datacenters
- Lacks out-of-the-box connectors for ITSM
- Limited bot management options

LexisNexis® Risk Solutions – LexisNexis® Dynamic Decision Platform® , LexisNexis® RiskNarrative™ Platform, LexisNexis® ThreatMetrix®, LexisNexis® BehavioSec®, LexisNexis® Phone Finder, LexisNexis® Fraud Intelligence Solutions Suite, LexisNexis® InstantID®, LexisNexis® TrueID®, LexisNexis® FlexID, LexisNexis® Instant Verify International, LexisNexis® IDVerse®, LexisNexis® Compliance Lens, LexisNexis® WorldCompliance™ Data Plus



Leader in



LexisNexis® Risk Solutions was formed in 2000 when it was spun out from LexisNexis, which was founded in 1973 LexisNexis Risk Solutions offers a range of fraud and identity and financial crime compliance solutions accessible through the LexisNexis Dynamic Decision Platform and LexisNexis RiskNarrative®, which contribute to its overall FRIP offering: LexisNexis® Fraud Intelligence, LexisNexis® InstantID®, LexisNexis® TrueID®, LexisNexis® IDVerse® Authentication Hub that includes LexisNexis® One Time Password, LexisNexis® Push Authentication etc,; LexisNexis® ThreatMetrix ®, LexisNexis® BehavioSec®, LexisNexis® Emailage®, LexisNexis® PhoneFinder, and LexisNexis® WorldCompliance™ Data. LexisNexis Risk Solutions addresses all the major fraud reduction technologies. Its SaaS solutions are hosted in the company's own facilities plus multiple public IaaS providers across three continents. Client components are composed of JavaScript and SDKs. Pricing is based on the number of transactions or API calls plus fees for professional services and tuning, all depending on the combinations of services used.

LexisNexis Risk Solutions provide IDV services, including PII-based verification, document authenticity verification, fake identity detection and sophisticated liveness detection techniques to prevent the use of deepfakes. LexisNexis ThreatMetrix provides exhaustive device and digital identity intelligence and reputation features; Emailage analyzes email reputation and risk and Phone Finder discovers links between phones and identities and can also provide MNO context, SIM swap attack detection. Moreover, PhoneFinder can integrate with call center software to deliver this information, plus phone-to-web session mapping, in real-time to help deter social engineering attacks. For UBA, LexisNexis Risk Solutions can evaluate a broad range of login and transaction details, including transaction types, amounts, payees, item analysis, velocity and frequency, locations, proximity to suspicious behavior, multiple transaction attempts from multiple users on the same device, income-to-spending analysis, account creation clusters, and relationships to known high-risk accounts. Its behavioral biometrics capabilities include the major modalities and several innovative ones. These features (from ThreatMetrix and BehavioSec) work in concert to prevent ATOs. Behavioral biometrics, embedded pixels, and bot activity signatures from their Digital Identity Network form the basis of their bot detection functions.

ThreatMetrix Bot Detection API and Behavioral Biometric can find inventory hoarding, jingle bots, price checking bots, social media bots, ad click, account creation, credential stuffing, file downloading bots, ticket scalping, and email address harvesting bots and headless browsers. ThreatMetrix can uniquely identify devices being maliciously used and block offenders from uploading fake reviews and comments. Their solutions can also discover guest checkout and loyalty program abuse. To deter logistics fraud, it can assess risk for shipping and billing addresses. LexisNexis Risk Solutions offers limited bot management facilities as well.

LexisNexis Risk Solutions has a dedicated 3DS2 API for issuers and claim PCI-DSS 4.0 certification. LexisNexis Risk Solutions fraud portfolio can detect the full range of credit card fraud types, including skimmed and counterfeit card usage and malicious card testing. ThreatMetrix and BehavioSec work to detect mule accounts, NAF (including synthetic identity fraud), scams, government benefits fraud, and APP fraud.

Their risk engine is highly configurable and allows customers to weight the risk factors. It offers a range of models, including out-of-the-box flagship models (Smart Learning) and AI-powered custom models (Open Smart Learning) offering maximum flexibility for customers. Rules can have hundreds of conditions connected by logical operators. Thus, rule editing can be complicated, but they do offer professional services for this if needed. Their risk engine can output decisions, risks scores, and reason codes. It is accessible via protected REST and SOAP APIs. Webhooks are not supported. It does not support packaging of results as claims or assertions. Case management, dashboards, and standard reports are available. Customizing dashboards and reports requires their professional services, however. They are testing GenAI but rightfully want to be cautious about its introduction.

LexisNexis Risk Solutions is ISO 27001 and SOC 2 Type 2 certified. Their services use load balancing and cloud auto-scaling techniques to meet customer demand. Support services are available for deployment and incident handling. Languages supported include English, French, German, Spanish, and Japanese. Unlike some competitors, LexisNexis Risk Solutions does store consumer data. Consent collection is obtained by their customers. They use de-identification, pseudonymization, obfuscation, redaction, and encryption to protect stored PII. LexisNexis Risk Solutions is suitable for all kinds of businesses, non-profits, and government agencies that need full-featured fraud reduction capabilities.

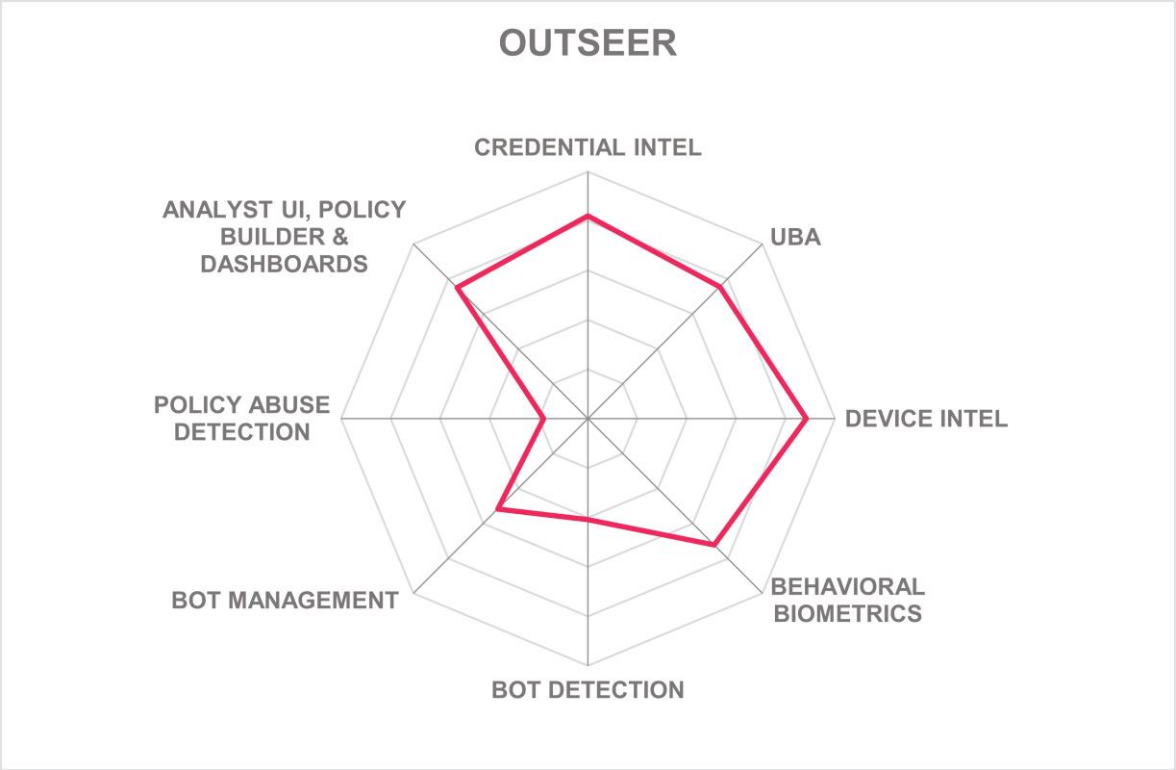
Strengths

- Full coverage of credit card fraud types.
- Can detect ATOs, NAF, and government benefits fraud.
- ThreatMetrix provides high-quality device and digital identity intelligence.
- BehavioSec delivers good behavioral biometrics.
- Granular UBA that examines a plethora of transaction details, including some that are not addressed by the competition.
- Very good range of bot attack types are discoverable.
- Customers can train their own ML fraud detection models if desired or deploy their standard ML-powered models.
- Rule simulator provides a safe way to view how policy changes would affect outcomes.

Challenges

- Multiple services required for full FRIP functionality; better packaging would make it easier for customers to consume and manage.
- Data retention policies are not configurable.
- Rule builder interface is complex.
- Dashboard and reports customization requires professional services.
- More advanced bot management options would be useful.
- Policy abuse detection capabilities should be expanded.

Outseer – Fraud Manager, 3-D Secure, FraudAction



RSA was acquired by Symphony Technology Group in 2020, and in June 2021 the Outseer brand was launched. Outseer is RSA's rebranded 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. Outseer Fraud Manager can be run on-premises on Linux or Windows with various supporting applications, Outseer Fraud Manager Cloud is hosted in a Tier 1 IaaS in datacenters in the EU and NA, and Outseer 3-D Secure is available as SaaS hosted from their own facilities. The client components are JavaScript and mobile SDKs, which collect device intel and behavioral biometrics. 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 the six core aspects of FRIP, albeit in some cases through integrations with partners as detailed below. Pricing options are per-user for the on-premises version of Outseer Fraud Manager, transaction-based pricing

for Outseer Fraud Manager Cloud and Outseer 3-D Secure, and Outseer Fraud Action has fixed costs for fraud intelligence feeds and takedown actions can be priced in bundles.

Outseer does not explicitly look for NAF or synthetic identities, although they may be discovered in the known bad account repository in Outseer Global Data Network, which is a repository of broader compromised credential intelligence that is integrated into Outseer Fraud Manager and 3-D Secure. Moreover, Outseer FraudAction gets additional credential intel from open web, dark web, and social media reconnaissance. This information is shared across their FraudAction customer base. JavaScript delivers thorough device intelligence, including all the common attributes plus device reputation, and malware and jailbreak detection are facilitated by their SDKs. UBA features examine login and transaction details such as amounts, types, payees, velocity and frequency, proximity to suspicious behaviors such as phishing, multiple transaction attempts from multiple users on a single device, and relationships to known high-risk accounts. Data retention periods are customer configurable in on-premises deployments. Behavioral biometrics include industry standard modalities and form the basis of their bot detection functions. Outseer does not specialize in eCommerce site protection, but it does identify and stop bots generally and credential stuffing bots specifically. It can protect customers against loyalty program abuse. Outseer supports allow/deny-listing and customer configurable authentication challenges for bots.

Outseer 3-D Secure is PCI DSS, and EMVCo 3DS v2.2 and v2.3.1 compliant, providing services for Mastercard, Visa, AmEx, and EFTPOS. Their 3-D Secure product is a 3DS2 ACS, which is designed to protect issuers (but not merchants). As such, it enables credit card fraud protection against CNP, counterfeit card, and malicious card testing. It can also detect ATO attempts and APP and BNPL fraud.

There are visualizations for risk engine activities via the dashboard, but the dashboard itself is not currently customizable, although there are plans to allow that. The risk engine outputs risk scores and top contributors to the risk scores, and decisions are made within the Policy Manager. It cannot package risk results into claims, assertions, or HTTP headers. Customers can write and edit their own policies, but the policy management interface is composed of drop-down conditions lists that can be combined with logical operators. It could use some revision, and this is planned within the next year. It has built-in case management. Each product has its own investigation tool. The products are accessible via REST and SOAP APIs, which are well-secured. Standard reports are available, and customers can export data for consumption and analysis by third-party solutions. Call center integrations are not available.

Outseer’s cloud services take part in annual SOC 2 Type 2 evaluations. Outseer 3DS undergoes regular PCI DSS and PCI 3DS testing. Outseer is in the process of getting ISO 27001 certification. Outseer’s solution should support stronger authentication mechanisms. Their cloud services leverage IaaS auto-scaling for high customer demand. Setup, incident handling, and ongoing support packages are available. Documentation is available in English. Customers are responsible for data and consent collection, and Outseer uses a wide range of privacy-enhancing technologies to protect it.

Outseer Global Data Warehouse is a new cloud-hosted service that offers premium fraud analytics to customers for additional fees. Outseer also has planned a major overhaul of the risk engine whereby customers will be able to bring their own fraud detection models. Outseer's products are long-established in the FRIP market and used by some very large card-issuing clients and banks. Outseer's core capabilities in ATO prevention and device intel and strengths in credit card fraud prevention make it worth considering as an adjunct solution in the eCommerce fraud prevention space.

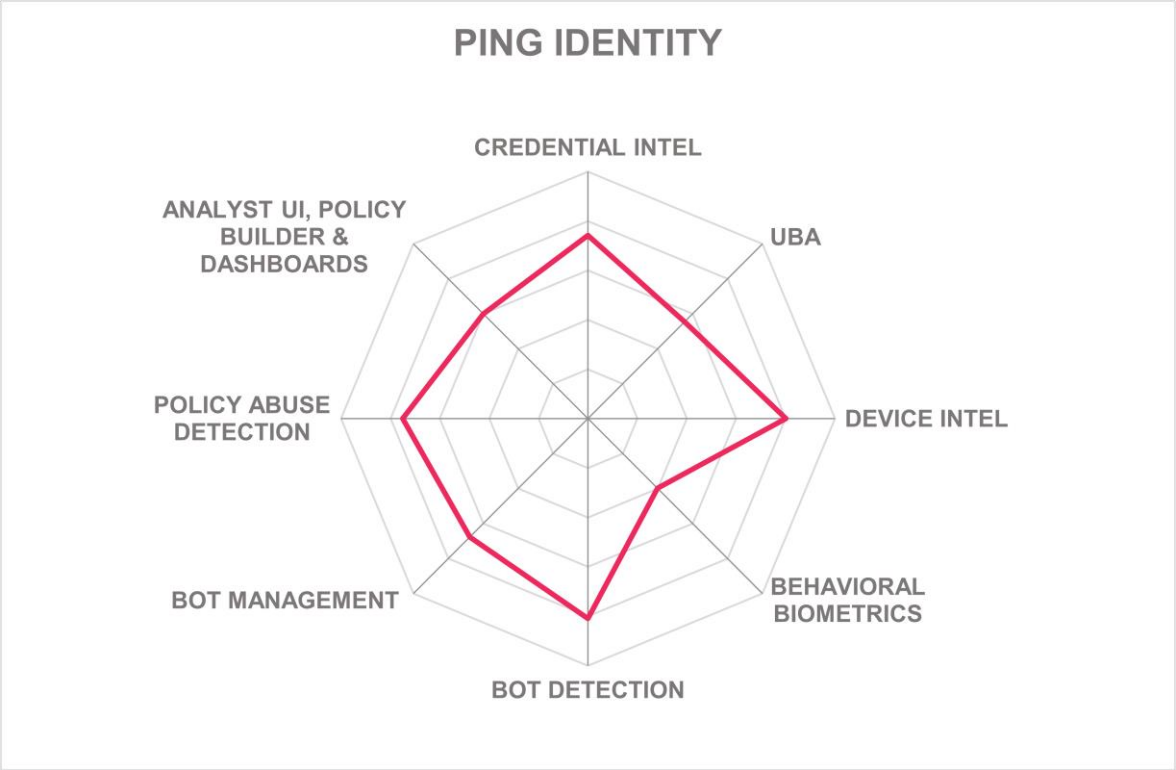
Strengths

- Outseer 3-D Secure is a certified 3DS2 access control server.
- Protects some of the largest credit card issuers.
- Detects ATOs and APP and BNPL fraud.
- Good device intel capabilities.
- Dark web and social media reconnaissance for credential intelligence.
- Fraudster network takedown services.

Challenges

- Needs stronger authentication mechanisms for administrators.
- UBA and transaction analysis should evaluate a few more risk factors.
- Additional bot management features would be useful.
- Rule authoring and investigative interfaces need modernization, and these are on the roadmap.
- Not focused on eCommerce site protection, thus it does not address most forms of policy abuse.

Ping Identity – P1 Protect, P1 Verify, P1 Authorize, and P1 DaVinci



Leader in

Ping Identity has been a pioneer in identity federation and access management since its founding in Denver, Colorado in the US in 2002. Ping Identity has grown substantially and went public on the NYSE late in 2019. Ping Identity was among the first enterprise IAM vendors to offer CIAM. Ping's entry into the FRIP space is composed of four products: PingOne Authorize, DaVinci, Protect, and Verify, all of which are part of PingOne Platform. The multi-tenant SaaS versions are hosted in Tier 1 IaaS providers from datacenters on four continents. It can also be deployed on-premises or as single-tenant cloud instances. Telemetry is collected from clients via JavaScript and SDKs. These SDKs are provided out-of-the-box for PingOne Platform customers. Pricing is determined by the number of users and transactions processed.

PingOne Verify and DaVinci offer excellent IDV features, including a mobile app/SDK for authoritative document attribute scanning, selfie-to-ID document matching, voice verification, and phone/device possession confirmation, with liveness detection that incorporates innovative methods. Moreover, DaVinci allows the inclusion of identity attribute information from a wide array of external sources. PingOne can detect deepfakes during the registration process. In-network compromised credential intelligence is used across the customer base, and individual customers can integrate external sources via DaVinci. The SDKs and JavaScript collect and analyze device intelligence attributes including IP and associated email reputation, device type/ID/fingerprint, and geo-location, geo-velocity, and behavioral attributes. From this analysis, it can identify user and traffic anomalies, device emulators, jailbreaks, and adversary-in-the-middle attacks. It can also infer when SIM swaps occur. Other device checks such as malware detection require third-party integrations. Ping Identity's implementation of UBA considers login times and locations; transaction types, amounts, and payees; and can detect multiple attempts from multiple users on a single device, but does not look at other transaction details. Their behavioral biometrics capabilities cover a subset of possible modalities. The combination of device intel, UBA, and behavioral biometrics enables ATO, NAF, and bot detection. The solution also has some bot management features including allow- and denylisting and redirection.

Ping's solutions can look for inventory hoarding, grinch, jingle, competitive price checkers, social media, account creation and credential stuffing, ticket scalping, and gift card cracking bots. It can detect headless browsers. Bot management features including allow- and deny-listing and redirection. It leverages IDV techniques to frustrate those who post fake reviews, comments, and goods for sale. Ping allows customers to set and enforce policies for guest checkout, discounts, and loyalty programs. Through Neo Verifiable Credentials, it addresses several logistics fraud types, including diversion of goods, overbilling, phantom shipments, cargo insurance fraud, false proof of deliveries, and load consolidation fraud.

Ping's solutions generally rely on signals from third-party solutions to detect the various types of credit card fraud, which then trigger responses within PingOne components. It can detect NAF, synthetic identity fraud, gift card cracking, and government benefits fraud through identity verification services orchestrated in PingOne DaVinci. PingOne Authorize can disrupt crypto/romance/travel type scams by embedding questions in the workflow, such as "What is the purpose of this payment – for a friend, a service, tech support?", "Were you called unexpectedly?", "Did it come from a pop-up or email?", or "Did they ask for remote access to your device?", etc.

The risk engine provides good visualizations of activities via well-designed dashboards, and policies are manually configured in PingOne Protect. Most customers use their products in conjunction with other vendors' FRIP solutions, so they do not have a full fraud analyst investigative interface or built-in case management, and report types are limited. Thus, the risk engine yields scores and optional reason codes but not decisions. Risk evaluations can also be packaged as SAML assertions, JWT claims, OAuth2 grants, OIDC flows, or HTTP headers. REST, WebAuthn, and Webhooks are the supported API types. Access to those APIs is protected by strong authentication methods. Ping's IDV solutions can be used to inform call center software about identity risks, but it does not have call-to-web session mapping. There are no out-of-the-box ITSM connectors.

The cloud-hosted services are protected by defense-in-depth measures, including WAF, API firewall, protocol layer monitoring, and DDoS mitigation. Their services are ISO 27001/27017/27018, SOC 2 Type 2, and Tisax certified. Training, documentation, and support services are only available in English. PingOne Platform, as a complete CIAM, does collect and process consumer data. It uses de-identification, pseudonymization, encryption, and redaction to preserve privacy. The lack of a fraud analyst interface and case management would be barriers for adoption for those who need those functions, but not for those organization who intend to use it alongside other FRIP solutions. Ping covers a wide range of bot-perpetrated fraud types, policy abuse, and even many logistics fraud use cases. Ping's products are well positioned to help merchants and organizations in eCommerce.

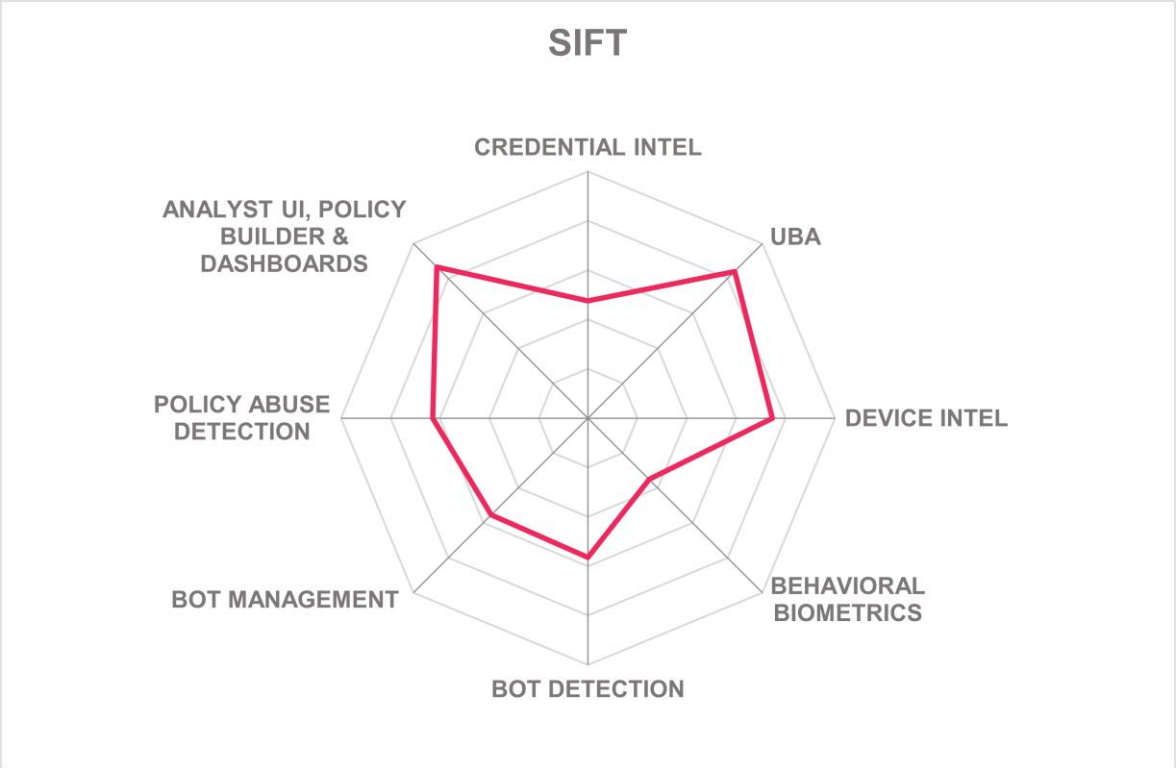
Strengths

- Most flexible deployment options, including SaaS, any cloud, on-prem, and single-tenant instances.
- Advanced scam detection and disruption features.
- Good coverage for bot-perpetrated attacks and policy abuse.
- Addresses complex logistics fraud use cases with Neo Verifiable Credentials
- Many security certifications.

Challenges

- UBA and behavioral biometrics should consider additional modalities.
- Does not have a full fraud analyst interface or case management.
- Documentation and support are only provided in English.

Sift – Platform



Sift was formed in 2011, and it is headquartered in San Francisco, California in the US. Sift is a fraud protection specialist, with services for payments security, content protection, and ATO prevention. 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 datacenters in the US. Client telemetry is gathered using JavaScript and SDKs. Pricing is determined by the number of billable events, where a billable event is defined as a combination of products invoked and use case, such as logins, orders, account creation, risk scoring, or monthly active users.

Sift utilizes compromised credential intelligence from within their customer base. Sift does not support AML, KYC, or provide name/watchlist screening services. Sift protects the account creation process with its UBA and by detecting device farms and VPN usage, which helps deter synthetic identities and mule account creation. Its UBA functions can also provide input for 3DS2 and EU PSD2 SCA and TRA. Sift can be called from Ping Identity DaVinci and Okta/Auth0 to provide risk information to help prevent ATOs.

For device intelligence, Sift evaluates a subset of attributes including IP, IP reputation, geo-location, and device ID/fingerprint/reputation, and can recognize known users on new devices. However, it does not perform device posture checks. User behaviors observed include login and transaction locations, transaction amounts, types, item analysis, velocity and frequency, proximity to suspicious behaviors, multiple transaction attempts from multiple users on the same device, account creation clusters, and relationships to known high-risk accounts. Sift generates dedicated ML detection models for each customer , which are used in combination with its global (all customers) model and its ThreatClusters (industry-specific cohort) model. Their implementation of behavioral biometrics includes the basic modalities and should be expanded. Sift takes a different approach to bot detection, relying on ATO prevention features rather than activity signatures or behavioral biometrics. It looks for specific bot attacks including inventory hoarding, account creation and credential stuffing, and ticket scalping; and methods such as headless browsers. Bot management includes allow- and deny-listing and rate limiting. It identifies and deters multiple policy abuse types, such as posting fake reviews/comments, posting fake goods for sale, and loyalty program/guest checkout/discount policy abuse.

Sift detects CNP, malicious credit card testing, and chargeback/refund abuse fraud. It does not look for new account or synthetic identity fraud. Its behavioral analysis functions enable it to alert on crypto, romance, and travel scams.

The risk engine is customer configurable. It can output risk scores or decisions. Customers can define reason codes that can be returned. REST and Webhooks are the supported API types. The APIs are secured by OAuth2. The Sift Console offers a customizable, widget-based dashboard that provides a view of a customer's fraud landscape, enabling the monitoring of key metrics like blocked users, chargebacks, and automation rule performance. Additionally, Sift provides case management and reports for fraud investigators, offering insights into individual and team case review performance, with capabilities for filtering, exporting, and analyzing key factors such as transaction anomalies and fraud types detected. Sift has recently introduced GenAI features, including ActivityIQ, which summarizes risk patterns across multiple accounts simultaneously.

Sift is ISO 27001 and SOC 2 Type 2 certified. Sift protects against DDoS attacks by leveraging a dynamically scalable load balancer to absorb and terminate malformed requests, mitigates protocol-specific attacks via application firewall rules, and safeguards against API abuse through real-time traffic monitoring, rate limiting, and implementing dynamic deny controls on incoming traffic. As a cloud-hosted service, it uses IaaS auto-scaling features to meet customer demands. Sift offers setup assistance through professional services and guidance from Customer Success Managers. Training for administrators is provided during implementation to ensure they are adept at using the platform effectively. Support services are available in English only. Sift uses pseudonymization and encryption to protect customer data.

Sift takes a different technical approach to fraud prevention. It covers a wide range of policy abuse types. Their credit card fraud detection capabilities are useful across industries.

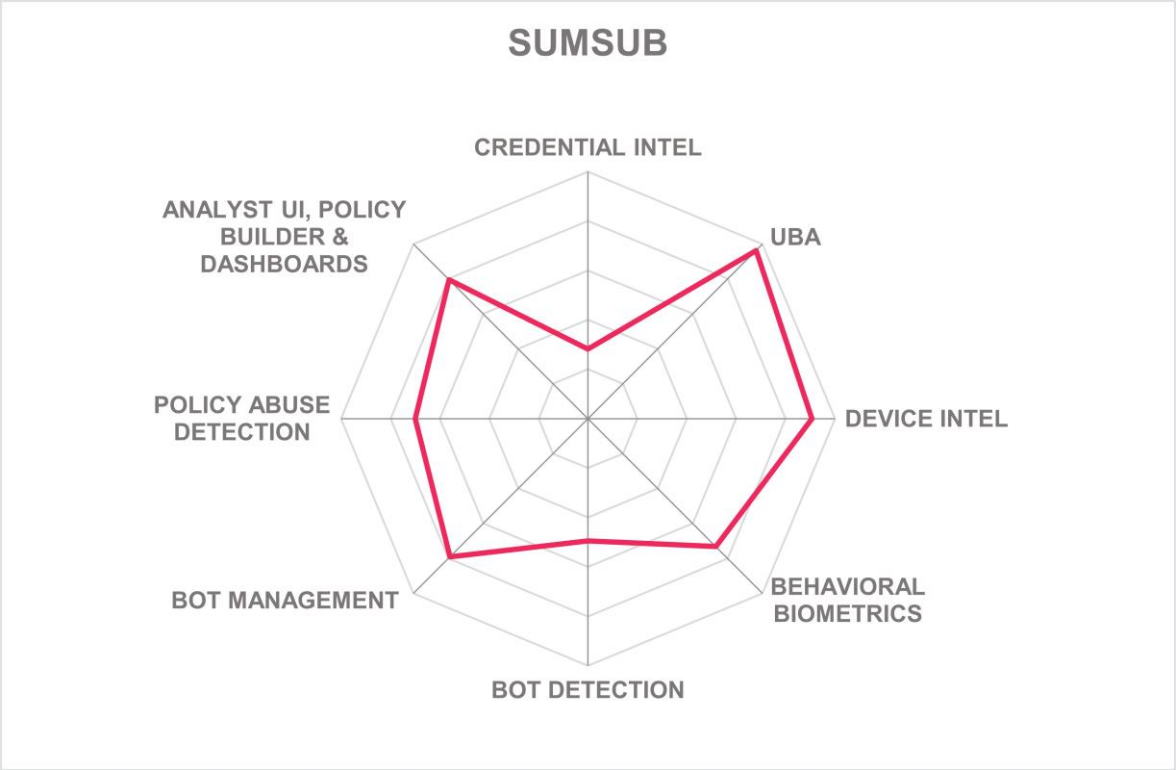
Strengths

- Fraud industry benchmarks available for merchant comparison (available to anyone).
- Fraud analyst services for customers who need assistance.
- Good implementation of UBA.
- Bespoke ML detection models for each customer.
- Supports detection of the most common forms of credit card fraud, scams, as well as chargeback abuse detection.
- Looks for several common types of bot attacks and multiple forms of policy abuse.
- GenAI-powered ActivityIQ analyzes patterns across multiple accounts at the same time.

Challenges

- Device intelligence and behavioral biometrics capabilities could be expanded.
- Bot detection and management could be improved.
- Only deployed in US data centers.

Sumsub – Fraud Prevention



Leader in

Sumsub was established in 2015 in Cyprus. They are a mid-stage fraud protection startup. Sumsub addresses the identity verification, device intelligence, user behavioral analysis, and behavioral biometrics portions of FRIP. The service is primarily SaaS-delivered, but customers can choose to host it in any of the major IaaS providers. The SaaS elements are hosted in datacenters in Europe, Middle East, and Africa (EMEA) and APAC. Client components include JavaScript and SDKs. Pricing models are transaction-based, with charges aligned to the volume of checks performed and discounts for high transaction volumes.

Sumsub offers a mobile app and SDKs for identity document validation, selfie-to-ID document photo matching, and liveness detection backed by many innovative mechanisms. NAF and synthetic identity fraud can be prevented with their deepfake detection during onboarding. Sumsub does not process compromised credential intelligence in its risk analyses, but it does offer phone and email verification.

The device intelligence capabilities (augmented with a partnership with Fingerprint) include checking IPs, VPN detection, geo-location, device fingerprinting, reputation, and malware presence detection.Its UBA module considers a wide assortment of transaction attributes such as login patterns, transaction types, amounts, payees, velocities, and relationships to high-risk accounts, multiple attempts by multiple users on a single device, and detection of account creation clusters. Data retention policies are not configurable per customer, but procedures exist to purge data according to region-specific regulations.

For behavioral biometrics, SDKs examine the basic modalities such as swipe and touchscreen analysis and can detect if the user is on a call at the time of transactions, which aids in determining if the user is being coerced. Device intel, UBA, and behavioral biometrics provide the basis for ATO detection. Their Fraud Network Tool looks for connections between users, devices, account creation events, sessions, and network info to detect bots. It can detect inventory hoarding/grinch and jingle bots, account creation and credential stuffing bots, gift card cracking, and headless browsers. Allow- and denylisting, challenging, throttling, and redirection comprise the bot management options currently. Sumsub protects clients against discount policy, guest checkout, and loyalty program abuse.

Sumsub can detect CNP fraud and malicious card testing attempts. Money mule accounts can be identified using device intelligence and behavioral intelligence. Sumsub can find evidence of crypto, romance, and travel scams with UBA.

Sumsub's risk engine features visualization and configuration of risk evaluation policies for admins, providing risk scores or decisions and text explanations. Clients can customize the weighting of risk factors within policies. Supported API protocols include REST, Webhooks, and OpenAPI, with multiple options for strong API authentication. Call center and ITSM integration are not currently supported. Reports and dashboards feature standard case management and fraud analysis processes, providing reports on case statuses and anomaly detections. GenAI is employed in the fraud analyst interface for interactive NL queries.

Sumsub is ISO 27001/27017/27018 and SOC 2 Type 2 certified. Sumsub employs CDN security services and custom WAF rules for DDoS protection, uses per-client endpoint rate limits, and detects protocol-specific attacks to protect the service from abuse and unauthorized access. Cloud-based elastic scaling is used to meet peak customer demand. Sumsub provides initial service setup assistance and handles incidents on a case-by-case basis. Support services are offered in English, Spanish, Chinese, Russian, and Portuguese, while documentation is available in English and Chinese. Customers are responsible for data and consent collection, and Sumsub uses most available privacy enhancing technologies to comply with relevant regulations.

Sumsub is missing some key features for compromised credential intelligence and bot detection, and its implementation of device intelligence and behavioral biometrics could be expanded to be more effective. Sumsub has good UBA capabilities that help protect clients against transaction fraud. Its credit card fraud prevention functions are useful for both issuers and merchants. Businesses in eCommerce in any region should consider Sumsub's offering in this space.

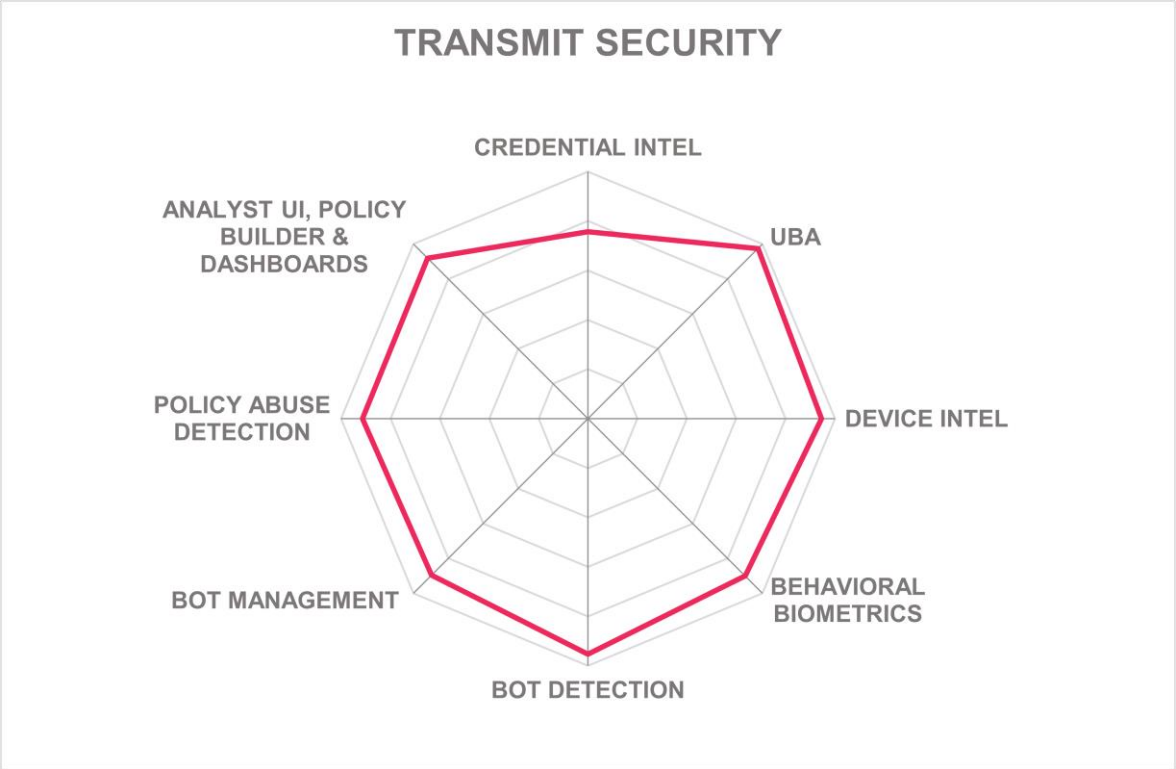
Strengths

- Mobile app and SDK for remote IDV includes many cutting-edge liveness detection methods.
- Deepfake detection.
- Detects CNP fraud and some types of scams.
- Natural language rule builder and query interface.
- Attack simulator can show what kinds of anomalies to look for per account.
- Granular UBA and transactional risk analysis.
- Good coverage for website/policy abuse.

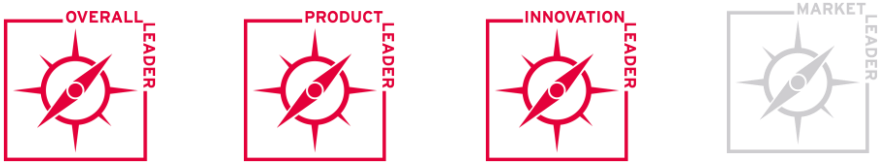
Challenges

- No compromised credential intelligence.
- Data retention policies are not configurable.
- Documentation is only available in English and Chinese.

Transmit Security – Mosaic Platform



Leader in



Transmit Security was founded in 2016 and is headquartered in Tel Aviv, Israel and Boston, Massachusetts, in the US. They are a well-funded late-stage VC-backed company. Their Mosaic Platform contains functionality in most of the FRIP functional areas defined above. Transmit also has leading products in the Passwordless Authentication and CIAM spaces. Transmit Mosaic Platform is a highly scalable SaaS that runs in public IaaS providers across globally distributed datacenters. On-prem and private cloud options are also available. The client portions are JavaScript and mobile SDKs. Pricing is on a per API call basis, with bundles available.

For IDV, Transmit has a mobile SDK that enables remote onboarding with selfie-to-official ID document matching and innovative liveness detection. Transmit uses in-network compromised credential intelligence and can be configured to call external sources by customers. Transmit's SDKs pull the full range of device attributes for evaluation. It conducts device posture checks and can detect jailbroken devices, malware, and SIM swaps. It can also be configured to call out to MNOs for updated, granular location information. Its UBA functions scrutinize a long list of login and transaction details, including transaction types/amounts/payees/items purchased, relationships to known high-risk accounts, multiple attempts from multiple users on a single device, and proximity to suspicious activities. The SDKs and JavaScript provide thorough behavioral biometrics, including the standard and some leading-edge modalities. These capabilities are used to prevent ATOs. Bot detection is driven by a combination of behavioral biometrics and activity signatures.

Transmit looks for inventory hoarding/grinch/jingle bots, price checker bots, ad click and ad insertion bots, account creation and credential stuffing bots, ticket scalping bots, gift card cracking bots, and email address harvesting bots. Transmit has advanced bot management features including allow- and deny-listing, challenges, throttling, and redirection. The Mosaic platform also protects against loyalty program, discount, and guest checkout policy abuse, and helps prevent posting of fake reviews/comments/jobs/goods for sale.

Transmit can detect all forms of credit card fraud, including CNP, CNR, counterfeit cards, malicious card testing, and protect against transactions from skimmers and chargeback abuse. The risk analysis and authentication services can inform 3DS2 ACS and EU PSD2 SCA and TRA processes. Their IDV services can flag likely NAF and synthetic identities. Transmit can detect government benefits fraud by identifying synthetic identities or excessive claims through historical analysis. Its UBA implementation addresses crypto/dating/travel scams by analyzing unusual transaction patterns and looking for signs from behavioral biometric analysis that the user is being manipulated.

Transmit makes rule and policy building comparatively easy with a flow-chart style interface and movable sliders for adjusting risk factor weights. It can yield decisions or risk scores with customizable reason codes, and it can package results as JWT claims, SAML assertions, OAuth2 grants, OIDC flows, or HTTP headers. The API types supported are REST, Webhooks, and WebAuthn. Dashboards provide the essential information, and analysts can drill down from there to start investigations. The fraud analyst interface allows administrators to define multiple investigative workflows as templates. Queries can be turned into repeatable reports. Case management features are built-in, and generic connectors facilitate connectivity with ITSMs. 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. GenAI is used to create case and event descriptions, executive reports, and to support NL queries.

Transmit has obtained SOC 2 Type 2 certification. They leverage IaaS auto-scaling and have active/active deployments for the highest availability. Customers can choose between different SLA options. Transmit Security employs third-party security services for detecting request anomalies, uses a layered security model with WAF protection at the edge to detect and mitigate threats, and provides application security controls for monitoring and preventing

protocol-specific attacks. The APIs are protected by strong authentication mechanisms. Transmit offers several levels of training and certification for administration and product use, and provides 24/7 global support services, available both on-site and remotely. English, Spanish, and Japanese are supported. As an integrated CIAM vendor, Transmit can collect consent for PII usage, and it protects customer data using de-identification, pseudonymization, redaction, and encryption to adhere to privacy regulations.

Transmit Security has CIAM and FRIP capabilities, and the company is approaching the market with a combined offering. This is advantageous for organizations that are looking to upgrade. Transmit is focused on large organizations in the financial sector, but their solution is equally well suited for protecting eCommerce and merchants. Transmit has good capabilities for IDV, device intel, UBA, and behavioral biometrics. Their strong orchestration features allow it to work with other IAM and FRIP components. Organizations in any industry should have Transmit Security Mosaic near the top of their shortlist for FRIP RFPs.

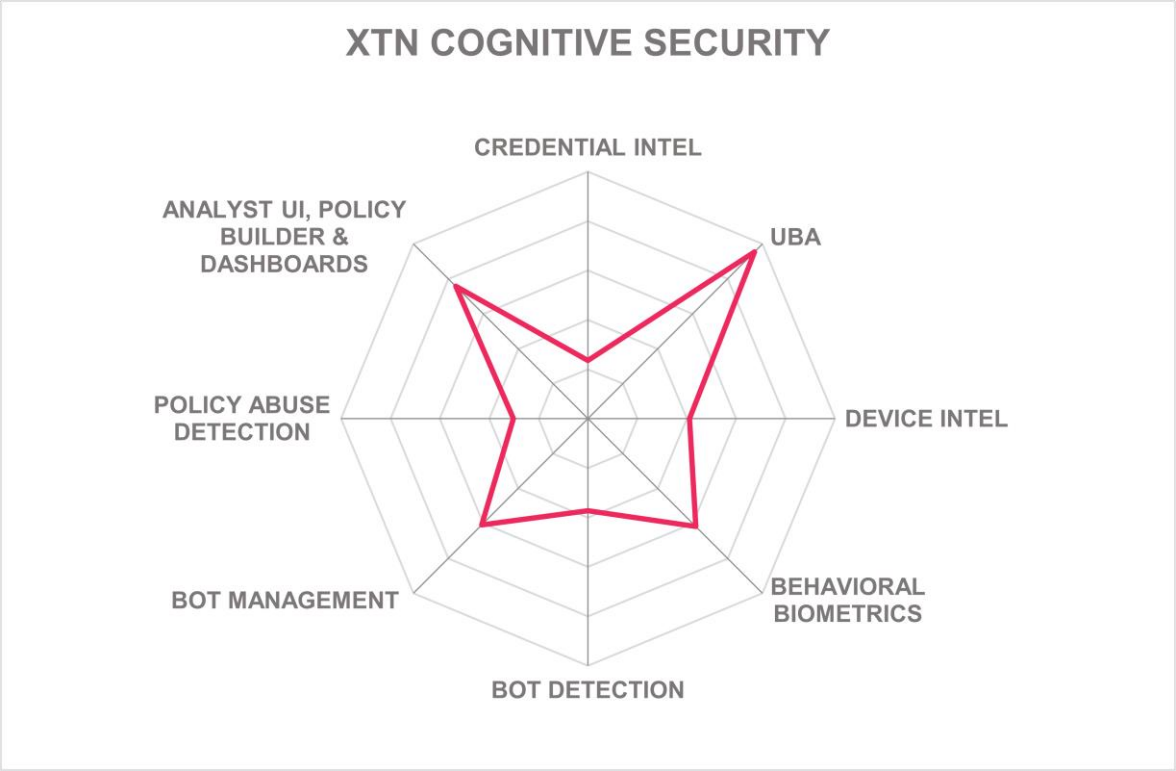
Strengths

- Easy to use journey builder facilitates complex orchestration if needed.
- Excellent coverage of credit card fraud detection methods.
- Detects NAF/synthetic identity fraud, APP and BNPL fraud, and scams.
- Device intelligence looks at all available parameters.
- Excellent behavioral biometrics for user profiling and bot detection.
- GenAI for case descriptions, executive reports, and natural language queries.
- Good coverage for bot-perpetrated attacks.
- Policy abuse protection is present.

Challenges

- Credit card detection requires partner integrations.
- Language support could be expanded.

XTN Cognitive Security® – Cognitive Security Platform®



XTN Cognitive Security®, founded in 2014 in Italy, is a privately held company backed by the majority shareholder CY4GATE SPA, listed on the Milan Stock Exchange. Their primary product, the XTN Cognitive Security Platform, is a cybersecurity and fraud prevention tool. XTN covers the device intelligence, UBA, behavioral biometrics, and bot detection parts of FRIP. It is primarily SaaS-delivered, leveraging two IaaS providers and datacenters in Europe. Customers can also choose to run it on premises or in private clouds. The client-side components are JavaScript and SDKs. The majority of XTN's clients are based in the EMEA region, with a focus on Southern Europe, and are primarily in the finance sector. They offer licensing models that charge per user or per analyzed transaction, tailored to specific use cases.

XTN does not use compromised credential intelligence. XTN’s JavaScript and SDKs (Android, iOS, Flutter, ReactNative, and Apache Cordova) pick up all the relevant device attributes and perform device posture checks, known user on new device checks, and can discover if devices are jailbroken or contain malware. XTN’s UBA functions examine an

extensive list of login and transaction details including transaction types/amounts/payees/item analysis/location, proximity to suspicious activities, multiple attempts from multiples users on the same device, relationships to known high-risk accounts, and income-to-spending analysis. XTN's SDKs pick up behavioral biometric signals including most of the basic and a few innovative modalities. The combination of device intel, UBA, and behavioral biometrics enables ATO detection. XTN looks for social media, ad click, account creation and credential stuffing, file downloading, and ticket scalping bots. Bot management options include allow- and deny-listing and challenging suspected bots. It can detect loyalty program policy abuse but does not address other types of policy abuse.

It can look for CNP and counterfeit credit card usage, chargeback abuse, and malicious card testing. To detect mule accounts, it watches account openings and transaction flows. XTN can detect when users are being manipulated over the phone in APP schemes and look for Remote Access Trojans (RATs) or legitimate remote-control software that might be used for nefarious purposes. To deter BNPL fraud, XTN scrutinizes applicant behavior during credit application processes. XTN's behavioral biometrics enables it to detect new account NAF and synthetic identity fraud. For EU PSD2 compliance, XTN centrally manages SCA exemptions, and performs risk analysis for Third-Party Providers (TPPs). Due to XTN's dual focus on the insurance as well as finance industries, it can discover fake brokers and insurance claim fraud.

The granular risk engine returns scores with configurable explanations. Decisions are not provided as customers determine how their applications process the scores. Packaging evaluation results into claims or assertions is not yet supported. XTN includes GenAI in the interface to help configure risk factor weighting. REST, SOAP, and Webhooks are supported. It can integrate with and orchestrate workflows in call center software.

Dashboards are adequate but customization is limited, and they could be redesigned to improve usability. Custom reports can be constructed. The analyst interface has map and timeline views and a link analysis tab that shows how transaction elements are related to other events. Case management is provided in the analyst interface, and there are integrations with JIRA and ServiceNow ITSMs.

XTN is ISO 27001 certified. XTN enforces API rate limiting, has strong authentication options for its API, relies on anti-DDoS protection from cloud services, incorporates input validation and security patch management to prevent protocol-specific attacks, and utilizes API firewall features through their cloud provider to identify and respond to potential abuse. Their SaaS uses standard IaaS auto-scaling to ramp up and down as needed. Setup and incident handling support are provided. Documentation and support are available in English, French, and Italian. Consumer data consent is handled by their customers, but their platform uses privacy preserving technologies like de-identification, pseudonymization, and encryption.

XTN targets the financial sector but also serves other industries with their device intelligence, UBA, and behavioral biometrics. It addresses several common bot attack types including competitive price checking bots, jingle bots, and headless browsers. It can also detect loyalty program abuse. Having the ability to detect more types of bot attacks and

prevent additional types of policy abuse would increase its appeal in the eCommerce and merchant industries.

Strengths

- UBA and transaction analysis functions encompass a wide range of risk factors, including some which are unique to this solution
- Some coverage of credit card fraud types
- Addresses several forms of insurance fraud
- Good implementation of behavioral biometrics
- Case management and ITSM integrations available

Challenges

- Lacks compromised credential intelligence
- Dashboards need to be reorganized for optimal reporting and investigations
- Additional bot detection and policy abuse prevention features would be useful

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless offer a significant contribution to the market space.

Amazon

Amazon was founded in 1994 in Seattle, Washington in the US. Amazon Fraud Detector is a service available in AWS for customers that has features for detecting online payments fraud, NAF, 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.

Brandefense

Brandefense was founded in 2018 in Turkey. Brandefense monitors cybercrime activities to continually update their understanding of attackers' tactics, techniques, and procedures (TTPs). Brandefense has an emphasis in stolen credit card monitoring, which helps issuers and merchants. Their other solutions include brand protection, external attack surface management, and third-party risk management.

Why worth watching: They look for compromised credentials and identity theft on the dark and deep web.

Deduce

Deduce was established in 2019 in New York, US Deduce supports the FRIP market by offering real-time behavioral intelligence derived from a large-scale identity network that spans hundreds of millions of profiles. It enhances CIAM and FRIP systems by detecting anomalies in login behavior, new device usage, or impossible travel patterns, without requiring PII exchange or browser fingerprinting. Deduce's risk signal enrichment helps inform risk-based authentication flows and fraud analytics platforms, enabling dynamic, step-up challenges or session termination based on inferred trust levels.

Why worth watching: Deduce has an innovative identity graph that expedites investigations. They were just acquired by Cheq in early 2025.

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. They are headquartered in Atlanta, Georgia, US.

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.

F5

F5 was founded in 1996 and 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. Their Distribute Cloud Data Intelligence product is their FRIP offering. Their products cover credential and device intelligence, UBA, and bot detection & management.

Why worth watching: F5 has a broad customer base covering many financial and ecommerce solutions. They were leaders in the last edition of this report, and we hope to include them in the next edition.

Feedzai

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

Why worth watching: Feedzai recently introduced new GenAI features to help fraud fighters including scam alert descriptions, case summarization, an LLM-based tool for creating SARs, and a natural language rules editor interface.

FICO

FICO is a long-established analytics and risk management company, founded in 1956 in California, US. The FICO Falcon Global Intelligence Network gathers risk signals from more than9,000 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.

Forter

Forter, founded in 2013 and headquartered in New York City in the US, 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.

Why worth watching: Forter Trust Platform is integrated into some major ecommerce and payment service provider platforms in the US. Their Trust Platform addresses many fraud reduction use cases specific to the ecommerce and payments industries and provides sophisticated remediation capabilities for policy abuse. They appeared in the last edition of this report, and we hope to include them in the next edition.

GBG

GBG, founded in 1989 in the UK, provides fraud protection through advanced identity proofing services that verify individuals using biometric matching, document authentication, and access to authoritative data sources, helping detect and prevent identity-based fraud such as account takeovers and synthetic identity creation. Integrated into CIAM and fraud reduction platforms, GBG's solutions support regulatory compliance and enable high-assurance identity verification for onboarding or high-risk transactions. Their offerings can be embedded via SDKs and APIs into web and mobile applications, making them adaptable across sectors including finance, healthcare, and digital commerce.

Why worth watching: GBG/Acuant has a full AML/KYC/watchlist screening solution. They appeared in the last edition of this report, and we hope to include them in the next edition.

LynxTech

LynxTech was launched in 2023 in Spain. They are still in the early stages but report that they are profitable already. Most customers are in Europe and South America. LynxTech is primarily an orchestration and risk engine. LynxTech has advanced UBA features.

Why worth watching: The founders have 30 years' experience in designing ML models for fraud detection. One of their USPs is that knowledgeable customers can design and import their own ML detection models. This is advantageous for banks that have created and tuned their own detection models for their particular business requirements.

Microblink

Microblink was founded in 2012, and they are headquartered in London, UK. They also have offices in Croatia and the US. They provide IDV services with document capture and liveness and deepfake detection. Microblink aids with AML and KYC with sanctions, PEP, and adverse media screening. The solution helps prevent NAF and synthetic ID fraud. They also cover CNP fraud detection and chargeback abuse prevention.

Why worth watching: They target not only FIs and fintechs, but also the travel and hospitality, iGaming, automotive, and ecommerce merchants. Their solutions are also OEM'd into other IDV and FRIP solutions.

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, was founded in 1984 and is headquartered in Chicago, Illinois in the 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.

Ravelin

Ravelin was founded in 2014 and is headquartered in London, UK. Their emphasis is on defending against online payments fraud. They also protect against policy abuse, such as refund and sales promotion 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.

Reality Defender

Reality Defender was founded in 2021. They are headquartered in New York City in the US. They provide call center integration (to detect calls with deepfake audio), deepfake image detection, disinformation detection, and LLM-generated text detection. Real-time video deepfake detection is currently in beta.

Why worth watching: with deepfakes proliferating, the ability to detect them is already imperative. It is likely that full service FRIPs will partner with organizations like Reality Defender to add on deepfake detection capabilities.

Seon

SEON was established in 2017 in Hungary. SEON analyzes users' digital footprints, device characteristics, behavioral patterns, and signals from email, phone, and social media data. It uses data enrichment and risk scoring to support transaction evaluation and policy-based

responses, including optional step-up authentication. It is an API-delivered solution and does not require full PII, which aids with privacy regulatory compliance.

Why worth watching: Seon is used in sectors such as fintech and e-commerce, often integrated into CIAM and FRIP workflows to support adaptive risk-based decisions.

Telesign

Telesign was established in 2005 and is based in Los Angeles, California in the US. 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.

Thales

Thales, headquartered in Paris, France, is a global defense and security company. They have extensive offerings in digital identity and cybersecurity, including the offering of high assurance identity credentials. Thales acquired OneWelcome, a leading CIAM vendor, and Imperva, a leading WAF, in the past few years. Imperva brings ATO protection, bot detection and management, and client-side protection features in the FRIP space.

Why worth watching: Thales provides high assurance identity and bot protection for banks and other industries.

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.

Related Research

Leadership Compass: Fraud Reduction Intelligence Platforms - Finance 2025

Leadership Compass: Fraud Reduction Intelligence Platforms 2023

Buyer's Compass: Fraud Reduction Intelligence Platforms

Copyright

© 2025 KuppingerCole Analysts AG. All rights reserved. Reproducing or distributing this publication in any form is prohibited without prior written permission. The conclusions, recommendations, and predictions in this document reflect KuppingerCole's initial views. As we gather more information and conduct deeper analysis, the positions presented here may undergo refinements or significant changes. KuppingerCole disclaims all warranties regarding the completeness, accuracy, and adequacy of this information. Although KuppingerCole research documents may discuss legal issues related to information security and technology, we do not provide legal services or advice, and our publications should not be used as such. KuppingerCole assumes no liability for errors or inadequacies in the information contained in this document. Any expressed opinion may change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Their use does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole 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 technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

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