Market Guide for Online Fraud Detection

Published 12 December 2022 - ID G00755906 - 23 min read

By Analyst(s): Akif Khan, Dan Ayoub

Initiatives: Identity and Access Management and Fraud Detection

Detecting fraud in digital channels is a challenge, due to the competing requirements of dealing with emerging attack vectors and delivering a smooth user experience. Security and risk management leaders must orchestrate multiple capabilities to create dynamic user journeys, while minimizing risk.

Overview

Key Findings

- Vendors are increasingly offering solutions that combine multiple online fraud detection (OFD) capabilities. We see individual features such as device intelligence and behavioral biometrics becoming commoditized. Best-of-breed solutions may be the most appropriate choice for difficult use cases, but they can complicate the ability to employ orchestration to improve user journeys.
- Leading payment gateway vendors are offering digital commerce merchants increasingly credible native fraud detection solutions. These might not be as capable as dedicated fraud detection vendors' solutions, but they may be good enough for merchants with less complex requirements.
- The continued use of on-premises solutions, particularly by banks deploying transaction intelligence platforms, creates challenges in relation to platform upgrades, data retention and impaired fraud detection efficacy. It also delays the time to value for new features.
- Awareness of, and demand for, journey-time orchestration (JTO) capabilities that can reduce the complexity of managing multiple OFD tools continues to grow. Orchestrating adjacent capabilities, such as identity proofing, authentication and access management, is typically part of many OFD projects.

Recommendations

Security and risk management (SRM) leaders responsible for identity and access management and fraud detection should:

- Meet specific business needs by supplementing all-in-one OFD solutions with best-of-breed point solutions, taking care to ensure that they can be integrated or orchestrated for maximum effect.
- Reduce complexity by assessing whether the fraud detection capabilities of their payment gateway are sufficient for their needs.
- Maximize the efficacy of fraud detection by favoring vendors with SaaS deployment models that share threat intelligence across their entire ecosystem in as close to real time as possible.
- Meet JTO requirements cost-effectively and efficiently by taking advantage of orchestration capabilities that may be delivered by a customer identity access management (CIAM) solution or an OFD solution.

Market Definition

Gartner defines the OFD market as the market for solutions that detect and prevent fraudulent actions within digital channels (browsers and mobile apps). OFD solutions provide a spectrum of capabilities within digital channels to prevent direct and indirect financial losses and to mitigate risks. Their core capabilities:

- Mitigate the activity of malicious automated bots
- Detect account takeover (ATO) attacks and trigger remedial actions
- Detect fraudulent activity in high-risk events along the digital customer journey, such as when customers make payments, transfer funds, perform account management actions or access personally identifiable information (PII).

Market Description

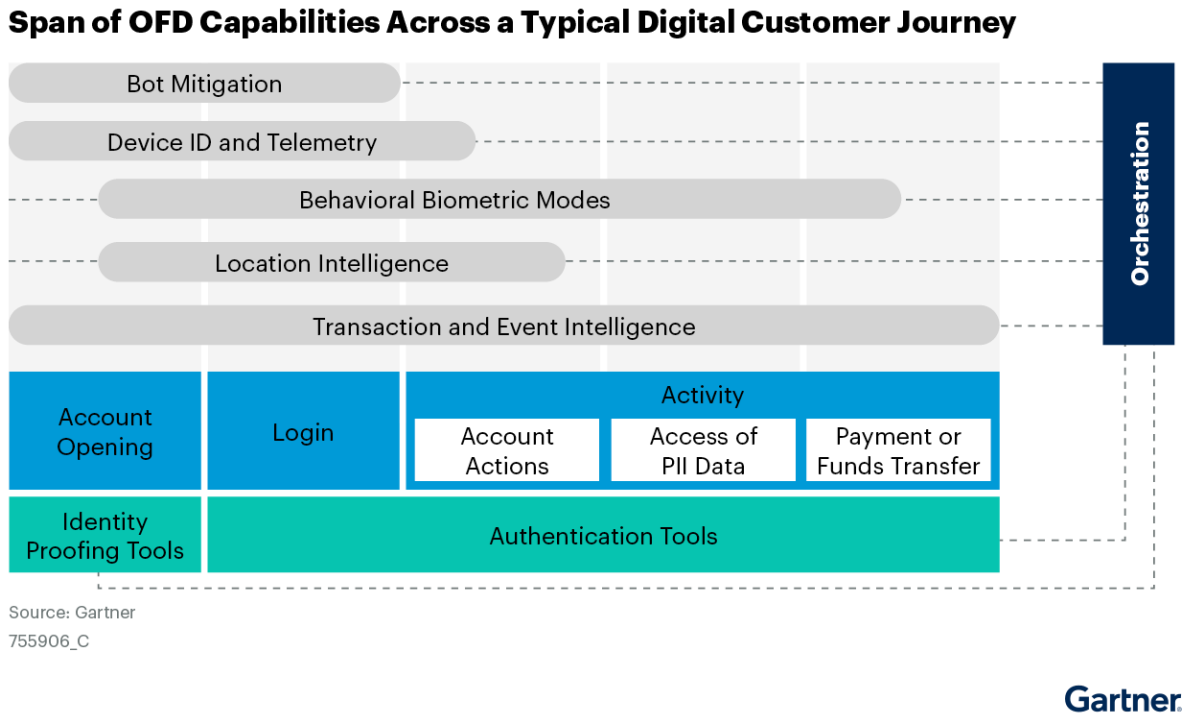
To meet the requirements of most organizations, an end-to-end fraud management strategy requires a broad range of capabilities, particularly when the focus is high-risk events such as logins and payments. Although some vendors offer multiple capabilities, no single vendor offers them all.

The products and services deployed by vendors typically offer real-time detection, and in some cases mitigation, at discrete points during a user journey, as opposed to continuously throughout a session. The outcome of such monitoring is typically a risk score, which may or may not be accompanied by metadata to give insight into why the score was assigned. Most vendors have decision engines that help turn this metadata into an action. The type of action depends on the fraud vectors being monitored, and at what point in the digital user journey the detection takes place. Decisions are typically along the lines of "accept/pass," "reject/block/decline," "challenge the user" or "manually review the transaction."

Organizations' buying centers for OFD tools vary greatly, depending on the use cases in question. Deployments are overwhelmingly SaaS-based, but less so in the banking sector, where on-premises deployments are still relatively common.

Keeping fraud rates within organizational tolerance levels is a baseline requirement for any vendor in this market. Consequently, the market has become more focused on how to achieve that while minimizing the number of false positives and without impairing the user experience (UX). Orchestration of multiple OFD solutions, often alongside identity proofing and authentication capabilities, has become increasingly important to reduce complexity and provide a more dynamic and adaptive UX (see Figure 1).

Figure 1: Span of OFD Capabilities Across a Typical Digital Customer Journey



Market Direction

Bot mitigation is arguably the foundation of any fraud detection strategy designed to protect digital channels, as it defends against bots at relatively low cost, thus enabling more expensive capabilities to be applied only to human users. Bot mitigation vendors are numerous and have traditionally focused on distinguishing between humans and malicious bots. However, some have broadened their focus to add value by distinguishing between good humans and bad humans, notably to protect core business logic within web- and mobile-based applications at various points on the user journey. Gartner has also noted a rise in the number of vendors improving their threat intelligence capabilities in order to monitor and track bot activity on the dark web, thereby strengthening their offerings and further differentiating themselves. This broadening of scope by bot mitigation vendors is expected to gather further momentum as it creates a strategic opportunity for customers to consolidate capabilities with fewer vendors.

Device intelligence remains a fundamental component of most OFD platforms. The intelligence and telemetry data collected from devices (see Note 1) is typically used as a trust factor for returning-user recognition and to ensure session integrity. Due to the wide variety of devices that must be supported by endpoint posture assessment systems, feature parity and cross-platform support can be complex and difficult to achieve. It typically requires integration and maintenance of multiple different SDKs (see Emerging Tech: Security — Streamlining Development to Improve Endpoint Posture Assessment). Notable enhancements to device intelligence innovation over the past 12 to 18 months have included the introduction of advanced hardware-bound proofs of work that use WebAssembly executables for advanced cryptography, integration of web-based profiling scripts within content delivery networks, and the advent of low-code/no-code frameworks that eliminate the need to maintain SDKs on mobile devices. The quality of device intelligence now varies greatly between vendors, but remains difficult to evaluate and compare meaningfully.

Solutions offering passive behavioral biometrics have attracted increased interest as organizations look beyond device identity as a means of passive authentication and aim to tackle emerging threat vectors. Adoption is largely within the digital banking domain. Behavioral biometric solutions can typically perform returning-user recognition, identify bots, and distinguish good users from fraudsters by monitoring timings and other signals related to how users interact with their devices. These include pointer movements, keyboard cadence, screen swipes and the handling motion of a device. Organizations are looking to maximize the benefits of these capabilities by deploying them across the user journey, not just to support risk assessment at login.

Adoption of location intelligence remains relatively nascent. It has been used for some time to aid compliance by, for example, enforcing geofencing for online gambling and streaming media content. But the use of multifaceted spoof-resistant location intelligence, based on a combination of GPS, IP address, Bluetooth sensor and Wi-Fi data, for fraud detection in the banking sector is still the preserve of early adopters. Nonetheless, vendor case studies show demonstrable efficacy in reducing ATOs, and interest in location intelligence will continue to grow. Concerns about privacy and user opt-in rates persist, but they vary greatly by country, with banks in emerging markets appearing more willing to take advantage of this capability.

Digital commerce organizations have continued to prompt vendors focused on payment fraud detection to broaden the uses to which their solutions can be put. As a result, many such vendors have developed or acquired chargeback management capabilities, which help clients to minimize the impact when fraudulent transactions slip through and to dispute first-party fraud ("friendly fraud") claims.

Addressing policy abuse, notably returns abuse, has become another key requirement in the field of digital commerce, with an increasing number of vendors introducing features to address this. Simply detecting payment fraud at the point of check-out is no longer enough for organizations seeking to reduce profit leakage at multiple points in the digital commerce journey.

Banks, of course, require fraud detection on payment transactions across a range of channels beyond just the digital. ATM, debit and credit card authorizations, deposits, withdrawals, wire transfers and contact center interactions are all screened alongside online transactions. Transaction intelligence solutions were traditionally deployed on-premises as banks sought to keep sensitive data on their own infrastructure, but also to minimize latency in fraud detection, particularly for real-time card authorizations. But as many banks embark on, or continue, migrations of applications to the cloud, there has been a strong shift toward deployment of transaction-monitoring platforms in vendor-hosted environments (see Buyer's Guide for Fraud Detection in Banking). This shift is likely to continue as banks realize the benefits of having vendors perform the task of updating and maintaining the solutions and the machine learning (ML) models that run on them.

Awareness of, and demand for, solutions that can orchestrate multiple layers of fraud detection capability, in addition to identity proofing and authentication capabilities, continues to grow. A persistent challenge mentioned by Gartner clients is the complex task of integrating multiple vendors, managing how and when they are used during the user journey, and interpreting and acting on the different signals they generate. Many fraud detection vendors are adding features that are on the JTO spectrum, such as the ability to ingest signals from other solutions. Many, however, lack the full suite of capabilities that define JTO according to Gartner's definition (see Innovation Insight: Journey-Time Orchestration Mitigates Fraud Risk and Delivers Better UX). Several JTO vendors have been acquired during the past 18 months, at the same time as the market saw new entrants. [1,2] The focus on JTO as a stand-alone capability or as one that is incorporated into a broader solution is likely to grow, with a particular focus on JTO delivered via the access management layer in order to mitigate ATOs.

Market Analysis

Bot Mitigation Is More Than Just Technology

Bot mitigation remains one of the most popular inquiry topics among Gartner clients. The focus of their inquiries is almost always detection and mitigation capabilities. Technical implementation of bot mitigation solutions typically involves a combination of embedding small pieces of obfuscated JavaScript or WebAssembly code within a webpage or mobile app session (to be executed on an endpoint) and network deployments that operate transparently to the end user. Visible challenges typically involve a simple puzzle or game presented to the end user (such as a CAPTCHA) to assess whether the user is human. By contrast, invisible challenges or covert UI tests involve some type of hardware-bound proof of work designed to assess the underlying hardware in order to discern if a session does originate from the type of device it claims to (a device may, for example, appear to be a smartphone but actually be a virtual machine).

There is, however, also growing interest in vendors that provide threat intelligence services to clients. Some vendors are taking a threat intelligence approach to combating bots by employing dedicated researchers who operate from environments rather like security operations centers. They monitor the activities of bot operators in order to augment defenses or to take down botnets that are attacking their clients. This reflects a move by large customers with more complex needs away from a purely defensive posture and toward tactical offensive techniques to mitigate bot threats. Provision of such services is becoming a key differentiator in a crowded market. It should be taken into account when selecting a bot mitigation solution to address targeted threats.

Preventing Authorized Push Payment Fraud Is An Unsolved Challenge

Judging from inquiries from Gartner's clients in the banking sector, authorized push payment (APP) fraud has become arguably their greatest fraud concern. APP fraud occurs when a good user is tricked or coerced into making a money transfer to a fraudster posing as a genuine payee (see Note 2). APP fraud is challenging to detect, given that the genuine account holder is logging in and can rightly pass authentication.

Effective transaction monitoring is imperative to detect transaction characteristics that can be indicative of risk, such as the amount, the time of day and the beneficiary's account details. Banks need to ensure the fullest set of transaction attributes are passed into and used by their transaction intelligence platforms. In some countries, such as the U.K., France and the Netherlands, "confirmation of payee" schemes have been introduced that check whether the stated beneficiary name sufficiently matches the actual name on the beneficiary account.

The focus on APP fraud has also driven increased client interest in behavioral biometrics. Some vendors have demonstrated efficacy at detecting whether a good user's behavior across the entire journey or session is suggestive of them being coached by a fraudster or being under stress. Examples of suspect behavior include more hesitation than is normal. This requires behavioral biometrics to be deployed across the entire journey, rather than just at login, which further increases the need for effective JTO to invoke mitigating actions if APP fraud is suspected. Clients looking to implement behavioral biometric solutions should understand the limitations and real-world conditions that can affect the efficacy of this technology (see Improve Customer Identity Corroboration With Passive Behavioral Biometrics).

Customer Identity Access Management Platforms Are Becoming Focal Points for Journey-Time Orchestration

CIAM platforms are fulfilling growing demand to manage user access to applications (see Solution Comparison for Customer Identity and Access Management Capabilities of 7 Vendors and 5 Essential Ingredients of a Successful Access Management Strategy). As these platforms govern the account creation and account access processes, they are also platforms on which fraudulent account opening and ATOs can take place. Many leading CIAM solutions have JTO capabilities that support adaptive access by obtaining contextual signals that inform policies governing authentication and authorization decisions. These signals — from device IDs and telemetry, analysis of IP addresses and behavioral biometrics, for example — can in some cases be delivered natively by the CIAM platform. However, many vendors have built a marketplace or library of integrations to vendors specializing in a range of different fraud detection capabilities. Using these, clients can choose "best of breed," if they wish, for a specific capability, or leverage an existing contract with a vendor.

As CIAM solutions mature and adoption grows, it is becoming more logical for organizations to assess whether their CIAM platform, in the first instance, should be the focal point of their efforts to prevent fraud in digital channels.

Leading Payment Gateway Vendors Are Investing in Native Digital Commerce Fraud Detection Tools

Digital commerce merchants typically face a choice when it comes to payment fraud detection capabilities — either use the native fraud detection capability of their payment gateway or use a dedicated fraud detection vendor. Historically, the fraud detection capabilities built into payment gateways have been relatively basic and "one size fits all" — suitable for smaller digital commerce merchants with less complex needs, but less suitable for larger merchants with more complex requirements and a greater desire for control. Some payment gateway vendors have partnered with dedicated fraud detection vendors to resell their services, with mixed results in terms of how well a fraud detection vendor can deliver services to merchants it has no relationship with.

However, some leading payment gateway vendors, such as Adyen, Checkout.com and Stripe, have invested in developing native fraud detection solutions to the extent that they are now credible alternatives to separate, dedicated solutions for an increasing number of merchants. But even as these native solutions become good enough for merchants of growing size and complexity, it is likely that the largest merchants will continue to use dedicated fraud detection solutions. A key reason for this is that many large merchants use multiple payment gateways for redundancy and authorization optimization. As such, they want to decouple fraud detection from payment gateways, and have a single fraud detection platform with visibility across all transactions, regardless of payment gateway.

On-Premises Deployments Reduce the Efficacy of Fraud Prevention Platforms

Although the number of OFD SaaS deployments has been growing in the financial sector, many financial institutions still rely on on-premises deployments (see Buyer's Guide for Fraud Detection in Banking). Vendors may be pressured into accommodating on-premises deployment in order to win in competitive situations, but they often fail to fully educate their customers about the pitfalls and drawbacks. Gartner generally advises against on-premises deployment of new OFD platforms, as it typically results in otherwise avoidable problems that impact overall system performance, such as poor data retention, lack of timely system upgrades and inability to share "truth data."

Data retention is a critical aspect of all OFD platforms, as it is necessary to train ML models. In SaaS deployments, vendors typically keep a minimum of six to 18 months of data, so that algorithms can adapt and self-tune. However, where on-premises deployments are used, some customers attempt to cut costs by reducing the amount of storage to just 30, 60, or 90 days of data. This results in poor overall threat protection, as the models and algorithms deployed require substantially more data to operate optimally.

On-premises deployments are also very difficult to upgrade and maintain. Since these systems are typically integrated in-line within the core of a financial institution's transaction processing or online workflows, they are difficult to take offline. Also, the institution often lacks the time and resources to keep up with the vendor's latest codebase. Systems and algorithms therefore quickly become outdated against modern threats, which results in reduced customer value and decreased effectiveness against evolving threats. In these situations, it is not uncommon for customers to fall so far behind their vendor's release cycle that upgrading becomes impossible, and they are instead forced to migrate to entirely new codebases.

Additionally, the inability of fraud vendors to obtain any transaction information from on-premises deployments creates islands of fraud data that, individually, are of limited use for combating threats. Since on-premises deployments are typically run by financial institutions in tightly controlled environments, it is not uncommon to encounter reluctance about sharing confirmed fraud events in real time. Instead, these institutions may compromise by providing the occasional manual, ad hoc upload (perhaps monthly or quarterly) of small portions of data. This leaves OFD vendors unable to develop better intelligence — using ML algorithms, global policies, best practices and so on — with which to combat evolving threats. In turn, this reduces the effectiveness of vendors' OFD solutions.

Cross-Organization Threat Intelligence Is Essential for OFD

Fraudsters often operate within specific geographical regions and typically target organizations with the weakest countermeasures. Once an attack pattern has been stopped or is no longer relevant, fraudsters either change their tactics or switch targets. Thus, it is imperative that an OFD platform can learn and improve from confirmed loss events within specific geographies (ideally across borders and globally), not just within a single organization. This requires the platform to have the ability to share anonymized telemetry about users, devices, and event outcomes (particularly confirmed frauds) across an entire network and for all customers. Systems, policies and algorithms can then be updated in real time to defend against evolving threats.

However, many modern OFD platforms still silo data on a per-organization basis and do not possess the ability to share intelligence across the entire customer base of all the organizations they aim to protect. The ability to share threat intelligence about confirmed fraud cases across a vendor's entire ecosystem is something that all OFD platforms should have. Vendors unable to share threat intelligence across their entire network are at a significant disadvantage, compared with those that can. Organizations seeking OFD solutions should ensure that confirmed fraud events impacting their region and industry can be shared, learned and stopped in real time across a vendor's entire network. Although regional regulations may make this challenging in some geographies, OFD vendors that have privacy-preserving techniques capable of sharing telemetry about confirmed fraud events across their entire network are typically better positioned to mitigate risk and reduce losses due to fraud.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

The vendors listed in Table 1 range from well-established providers with significant presence in the OFD market, or that are often mentioned in clients' interactions with Gartner, to smaller, less frequently mentioned vendors, especially those with fresh approaches to meeting customers' requirements (see also Note 3).

Vendors were eligible for inclusion in Table 1 if they fell into one or more of the following categories:

- **Bot mitigation vendors:** These vendors focus on detecting and mitigating bots that are abusing business logic on web, mobile or API channels. Examples of such abuses include ATO, credential stuffing, credential cracking, carding and price scraping.
- **Device assessment, location intelligence and behavioral biometrics vendors:** This broad category includes vendors that focus on detecting risk in customer interactions on digital channels. Examples of these vendors' capabilities include creating unique device IDs, gathering browser and device telemetry, detecting client-side malware, assessing user location and creating profiles of customers based on behavior (pointer movements, swipe characteristics, typing patterns and so on). Vendors in this category may offer one or more of these capabilities.

- **Transaction and event intelligence vendors:**
  - **With a banking focus:** These vendors' offerings have traditionally been deployed on-premises or in private clouds that offer banks the ability to build and maintain custom-made ML models, although vendor-hosted and SaaS deployment models are gaining traction. Data is not usually co-mingled across clients. These vendors are traditionally used for transaction monitoring, but they have evolved to monitor additional events, such as logins and account management changes. Rule engines typically augment an ML capability, with case management tools to facilitate investigation. Not all these vendors offer their own capabilities, such as device assessment or behavioral biometric modes, to assess risk at the digital front end. Instead, some may ingest data from other vendors that a bank uses. Vendors in this category focus on banking and financial services, but not exclusively so.
  - **With a digital commerce focus:** These vendors' offerings are deployed as SaaS solutions that have a broad range of functionality, spanning ML, rule engines, device assessment, basic behavioral analytics and case management tools. Data from all clients is typically co-mingled to develop ML models that are used by all clients, and to facilitate link analysis across the vendor's entire universe of data. Vendors in this category focus on digital commerce and the payment event, but not exclusively so.

Vendors that focus on addressing fraud in contact centers by, for example, assessing call integrity or using speaker authentication, are not included in this Market Guide. Although this segment of the market remains within Gartner's coverage, it no longer meets the definition of digital fraud in this Market Guide. Nonetheless, risk and trust signals from such vendors' solutions are essential inputs for transaction and event intelligence platforms that are used for multichannel fraud detection.

Table 1: Representative Vendors in Online Fraud Detection

(Enlarged table in Appendix)

Vendor	Product, Service or Solution Name
ACI Worldwide	*Multiple applicable products*
Akamai	Bot Manager
Appgate	*No specific product name*
Arkose Labs	*No specific product name*
BioCatch	*No specific product name*
Bottomline	Cyber Fraud and Risk Management
Callsign	*Multiple applicable products*
Cequence Security	*No specific product name*
Cleafy	*No specific product name*
Cybersource, a Visa Solution	Decision Manager
Darwinium	*No specific product name*
DataDome	*No specific product name*
DataVisor	*Multiple applicable products*
F5	*Multiple applicable products*
Featurespace	ARIC Risk Hub
Feedzai	*No specific product name*
FICO	Falcon
Forter	*Multiple applicable products*
GeoComply	GeoComply Core
Google	reCAPTCHA Enterprise
Group-IB	*Multiple applicable products*
hCaptcha	*No specific product name*
HUMAN	*Multiple applicable products*
IBM	IBM Trusteer, IBM Safer Payments
Incognia	*No specific product name*
Kount, an Equifax Company	*Multiple applicable products*
LexisNexis Risk Solutions	*Multiple applicable products*
NuData Security, a Mastercard Company	*No specific product name*
Netacea	Bot Management
NICE Actimize	IFM-X
Outseer	Outseer Fraud Manager
Ravelin	Fraud solution suite
Riskified	*Multiple applicable products*
River Security	River Dynamic Security (Botgate)
SEON	*No specific product name*
Sift	*Multiple applicable products*
Signifyd	*No specific product name*
Spec	Trust Cloud
Tencent	TenDI
ThreatFabric	Fraud Risk Suite

Source: Gartner (December 2022)

Market Recommendations

Keeping fraud rates down is a baseline expectation for SRM leaders. They can achieve differentiation by also delivering a good UX for most users. This implicitly means reducing false positives when blocking user actions or increasing friction to elevate trust. Reducing operational complexity remains a constant imperative.

SRM leaders should:

- **Make considered choices about when to combine generalist and specialist solutions.**
  - Rationalize capabilities such as device intelligence, location intelligence and behavioral biometrics with generalist vendors that deliver them all, but accept that specialist vendors may be necessary for capabilities such as bot mitigation.

- **In digital commerce, explore opportunities to use the fraud detection capabilities of a payment gateway.**
  - Although the fraud detection provided by dedicated vendors will be more feature-rich, the increased investment by many leading payment gateway vendors in their own services means that they may be good enough for less complex requirements.

- **Avoid on-premises deployments, if possible.**
  - Use SaaS, where possible, not only to avoid the inevitable upgrade cycle, but also to enable vendors to dynamically manage and improve ML models using the maximum amount of data. Favor vendors that can demonstrate that intelligence and fraud events are shared in a privacy-preserving manner to improve detection rates across all clients that use their SaaS platform.

- **Seek cost-effective ways to orchestrate multiple OFD capabilities.**
  - As many CIAM solutions now offer strong JTO features, and an increasing number of OFD solutions are adding and evolving JTO features, explore whether these can meet your requirements before adding an additional vendor just for JTO.

Evidence

[1] Ping Identity Acquires Singular Key to Accelerate No-Code Identity Security Integration and Orchestration, Ping Identity.

[2] LexisNexis Risk Solutions Acquires TruNarrative, LexisNexis Risk Solutions.

Note 1: Intelligence and Telemetry Typically Gathered From Devices

Supported capabilities typically include the harvesting or creation of device-specific attributes from operating system or browser APIs (such as hardware configurations, cryptographic tokens, font lists and user settings), and assessment of device posture (such as OS tampering, supported language, configured time zone, installed software and system uptime). This information is also used to create a proprietary device ID, sometimes referred to as a device fingerprint.

Note 2: Example of APP Fraud

A common and insidious example of APP fraud is when fraudsters prey on elderly or otherwise vulnerable users by posing as bank employees or the police. They tell victims that their money is at risk of theft unless they transfer it immediately to a “safe account.”

Note 3: Representative Vendor Selection

The vendors listed in this Market Guide represent, in Gartner’s view, what is central to the OFD market, what extends it and what will transform it.

One or more of the following statements applies to each of the listed vendors:

- The vendor offers capabilities that support digital fraud detection in a way that is unique, innovative and/or that demonstrates a forward-looking product strategy.
- The vendor is frequently the subject of inquiries from Gartner clients with regard to digital fraud use cases.
- The vendor is representative of a particular market segment or geographic region, and thus helps to illustrate the OFD market’s breadth.
- The vendor had also met the requirements for inclusion in a previous edition of this Market Guide but been omitted simply due to space restrictions.

The list of vendors in this Market Guide is not exhaustive. It can include a maximum of 40 vendors out of hundreds. Necessarily, therefore, many worthy vendors are omitted, with no implied criticism. Equally, a vendor’s inclusion should not be considered an endorsement.

Document Revision History

Market Guide for Online Fraud Detection - 12 July 2021

Market Guide for Online Fraud Detection - 13 May 2020

Market Guide for Online Fraud Detection - 30 April 2019

Market Guide for Online Fraud Detection - 31 January 2018

Market Guide for Online Fraud Detection - 10 October 2016

Market Guide for Online Fraud Detection - 27 April 2015

Market Guide for Online Fraud Detection - 2 June 2014

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Security and Risk Management Leaders' Guide to Online Fraud Detection and Identity Proofing

Innovation Insight: Journey-Time Orchestration Mitigates Fraud Risk and Delivers Better UX

Buyer's Guide for Fraud Detection in Banking

Emerging Tech: Security — Streamlining Development to Improve Endpoint Posture Assessment

Table 1: Representative Vendors in Online Fraud Detection

Vendor	*Product, Service or Solution Name*
ACI Worldwide	*Multiple applicable products*
Akamai	Bot Manager
Appgate	*No specific product name*
Arkose Labs	*No specific product name*
BioCatch	*No specific product name*
Bottomline	Cyber Fraud and Risk Management
Callsign	*Multiple applicable products*
Cequence Security	*No specific product name*
Cleafy	*No specific product name*
Cybersource, a Visa Solution	Decision Manager
Darwinium	*No specific product name*
DataDome	*No specific product name*
DataVisor	*Multiple applicable products*
F5	*Multiple applicable products*
Featurespace	ARIC Risk Hub

Vendor	*Product, Service or Solution Name*
Feedzai	*No specific product name*
FICO	Falcon
Forter	*Multiple applicable products*
GeoComply	GeoComply Core
Google	reCAPTCHA Enterprise
Group-IB	*Multiple applicable products*
hCaptcha	*No specific product name*
HUMAN	*Multiple applicable products*
IBM	IBM Trusteer, IBM Safer Payments
Incognia	*No specific product name*
Kount, an Equifax Company	*Multiple applicable products*
LexisNexis Risk Solutions	*Multiple applicable products*
NuData Security, a Mastercard Company	*No specific product name*
Netacea	Bot Management
NICE Actimize	IFM-X
Outseer	Outseer Fraud Manager
Ravelin	Fraud solution suite

Vendor	*Product, Service or Solution Name*
Riskified	*Multiple applicable products*
River Security	River Dynamic Security (Botgate)
SEON	*No specific product name*
Sift	*Multiple applicable products*
Signifyd	*No specific product name*
Spec	Trust Cloud
Tencent	TenDI
ThreatFabric	Fraud Risk Suite

Source: Gartner (December 2022)