Market Guide for Online Fraud Detection

Published 30 April 2019 - ID G00352548 - 17 min read

By Analysts Jonathan Care, Akif Khan

Online fraud detection continues to grow in complexity with many solutions measuring dynamic behavioral characteristics. Security and risk management leaders responsible for fraud prevention should focus on creating a trusted ecosystem, and seek orchestrated solutions to improve customer experience.

Overview

Key Findings

- The online fraud detection (OFD) market shows continued signs of M&A activity with the attention of many investment firms becoming focused on this space. As a result, many solution providers are the target of acquisition by financial services, payment providers or large software companies.
- Machine learning continues to drive innovation in the space. However, buyers responsible for the specification and purchase of OFD solutions report increasing weariness with the jargon deployed by many vendors, leading to confusion over technical features rather than a focus on business benefits.
- In many organizations, fraud teams are being challenged to grow beyond transaction governance and compliance, through the need to accommodate new channels such as social media, and to combat unreliable, unverified information found on those channels.

Recommendations

Security and risk management leaders responsible for identity and access management (IAM) and with a focus on fraud prevention should:

- Deliver solution roadmaps that keep pace with the changing nature of fraud threats by embracing new interaction channels such as social media.
- Build a solution architecture that integrates data from vertical silos into a customer-focused analytics hub. This analytics hub should be able to orchestrate activity with aligned components such as user authentication and identity proofing.
- Align with cross-organizational groups to map out the integration of contact center, digital and in-person use cases. Fraudsters are not afraid to use complex attacks moving across multiple interaction channels.

Strategic Planning Assumptions

By 2025, the primary role of 60% of fraud leaders will shift focus from simply adhering to governance, risk and compliance toward creating an environment of trust and safety where customers can transact, interact and communicate, up from less than 5% today.

By 2023, the fraud market will consolidate and 70% of fraud detection solutions will be part of a larger portfolio offered by larger software vendors or payment solution providers, up from 15% today.

Market Definition

This document was revised on 13 May 2019. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Security and risk management leaders focused on fraud prevention (“fraud leaders”) are concerned with bringing fraud losses within organizational risk tolerances and thus want to detect fraud as it happens. To that end, they have adopted techniques that focus on:

- Transaction monitoring
- Detection of consumer experience abuses
- Identification process by fraudsters

OFD tools detect online fraud as transactions and interactions occur, in real time or near real time. Vendors provide tools for web, mobile or telephony channels. As the sophistication of attacks continues to evolve, so too have the tools, technologies and strategies that detect and prevent fraudulent activity.

Market Description

The OFD market is composed of vendors that provide products or services that help an organization detect fraud that occurs over web, mobile or other telephony channels. These products and services perform one or both of these functions:

- Running background processes that are transparent to users. These use hundreds to thousands of contextual attributes and data points — for example, geolocation, device characteristics, user behavior, navigation and transaction activity — to determine the likelihood of fraudulent users or transactions (see "Take a New Approach to Establishing and Sustaining Trust in Digital Identities"). This is done by comparing collected contextual event information to expected behavior using advanced analytics, statistical algorithms, or rules that define "abnormal" behavior and activities.
- Corroborating a user's identity. This is done by comparing:
  - Incoming identity information
  - Contextual attributes (as described above), and reconciling them against available external or internal identity information

OFD systems typically return alerts and results (such as scores with supporting data) to fraud operations teams, and also into orchestrated systems in the enterprise architecture. This enables the enterprise to take appropriate follow-up action:

1. Suspending the transaction, if the actual behavior is out of the range of what's expected or if the user appears suspect. This can be fully automated.
2. Conducting further manual review and investigation of the transaction and user, as warranted.
3. Triggering automated identity proofing, authentication and/or transaction verification to further determine the legitimacy of the user or transaction. This can be fully automated.

OFD applies mainly to three kinds of attacks (see Table 1).

Table 1: Online Fraud Attacks

Attack Type	Description	Impact Examples
Account Takeover	User account credentials are stolen (e.g., via malware-based attacks or phishing).	Targeted account takeover using credential stuffing or credential recovery techniques
New Account Fraud	Fraudster sets up a new account with a stolen or fictitious ("synthetic") identity.	An automated script (or bot) engaged in a massive attack against hundreds, thousands or more accounts An individual human conducting a manual attack
Stolen Financial Account	A purchase is made or money is moved between accounts.	An individual human conducting a manual attack A combination of human and automated scripts executing targeted or mass attacks

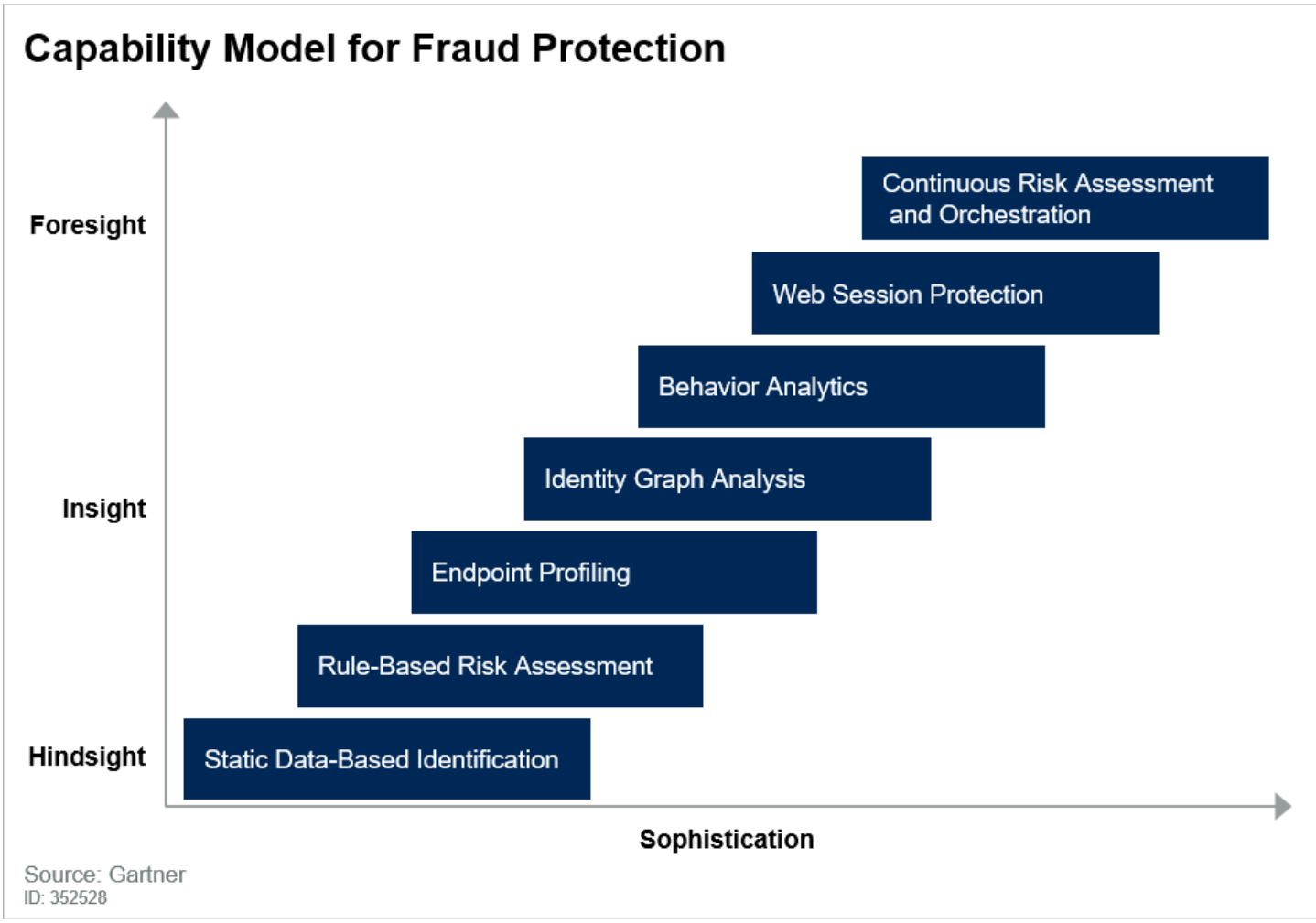
OFD products often integrate with identity proofing and corroboration tools as a means of increasing the trust assurance of a particular interaction, or to meet new account information gathering for underwriting or regulatory requirements.

Market Direction

In 2018, the market has been subject to significant consolidation, with several interesting mergers and acquisitions (M&As). The acquisitions of Brighterion and NuData Security by Mastercard signaled that the OFD space interests all the card associations, while the LexisNexis acquisition of ThreatMetrix and TransUnion acquisition of iovation denote the importance of OFD in multiple industry sectors. PayPal's acquisition of Simility also shows the interest of larger players to move into the fraud vendor marketplace.

OFD products and services exhibit the capabilities listed in Figure 1, and, by doing so, provide fraud leaders with the capability to reduce the impact of fraud on their organization.

Figure 1. Online Fraud Capability Model



In the retail space, the longstanding model has been for OFD vendors to be used by retailers for fraud detection, but with the retailers still absorbing the costs of any fraudulent transactions that evaded detection. These costs were most obviously borne in the form of chargebacks. There has been increased investment in, and market activity by, a subset of OFD vendors that have introduced a new model whereby the vendor takes liability for any fraudulent chargebacks resulting from transactions that have been screened by them. [1]

The commercial model between the retailer and vendor is naturally different from the traditional fixed per-transaction fees in the retail space. Such vendors have gained traction in the small and midsize business space during 2018 due to the attraction of such retailers for effectively paying for chargeback insurance, given their limited, if any, human resources to focus on fraud management. Larger retailers have yet to demonstrably move toward adopting such a model, predominantly due to economic concerns.

In particular, the orchestration and analytics capabilities that have been a hallmark of OFD tools

are experiencing creative applications in new use cases, aside from those outlined previously. Many fraud hubs have integrated with identity proofing and corroboration tools, and it is common for a fraud hub to double as an “identity hub” for dynamic, risk-based identity proofing, substantiation and corroboration use cases.

Technology Innovations Make Their Way From Financial to Retail and Other Markets

There are clear signs in the market that technology that has previously been leveraged for fraud detection primarily by financial institutions is starting to be explored and adopted in the retail space. Good examples are behavioral analytics and behavioral biometrics (the former focusing on aggregate behavior and the latter focusing on measurable traits for use in authentication).

For a number of years, such technology has been used by financial institutions, particularly around account login. During 2018, partnerships were created in the market between vendors focused on such techniques and those associated with providing more general fraud detection platforms for retailers. [2]

Other examples include vendors more traditionally focused on mobile device fingerprinting in the banking space being added to retailer-centric fraud detection platforms. [3] This suggests an increasingly blurred line between categorization of OFD vendors as being focused on either retailers or financial institutions and advances in fraud detection being driven by the broader ecosystem, rather than being segment-specific.

Machine Learning Continues to Gain Ground

The use of machine learning by vendors has continued to be a focus, both with respect to actual solution capabilities and in its prominence in vendor marketing collateral. This latter point, in particular, serves to highlight the acceptance among retailers and financial institutions that machine learning has become a critical component in their OFD toolkit and is a sought-after capability from their vendors. This is driven by the need to make ever-faster decisions incorporating relentlessly growing sets of transactional, contextual and historical data attributes. Competition for customer acquisition and retention remains fierce in an increasingly digitized marketplace. Customers are placing a premium on frictionless journeys and, in many sectors, the barrier to using an alternative retailer or financial institution is low. As a result, OFD vendors are focusing on their ability to support retailers and financial institutions in making rapid and effective risk decisions to expedite frictionless transactions and avoid false positives. To this end, there is an ongoing transition underway from primarily rule-based

systems to those that primarily rely on machine learning. Vendors can be classified into three groupings in this respect:

1. Those that rely primarily on static rule-based detection, with machine learning as a separate solution component that is used to typically generate a score and information codes that can be leveraged by human users to create further rules

2. Those that tightly couple rule-based detection and machine learning to the extent that, in addition to providing outputs that can be leveraged in rules, machine learning is used to optimize rule sets and proactively suggest new, more effective rules

3. Those that rely exclusively on machine learning with no rules being created or managed by the end user

Market Analysis

The OFD market continues to grow in terms of investment and new entrants, with growth expected to continue beyond 2019. This growth is being driven by a number of factors:

- Global e-commerce growth rates remain at around 20%, continuing the long-term secular trend of increasing digital commerce. [4]. In such a market environment, constant or even slightly falling fraud rates would nonetheless result in an overall increase in fraudulent activity, keeping the demand for the services of OFD vendors strong.

- Increased awareness of account takeover fraud in retail, due to the relentless drive to reduce friction in the customer journey, and the concomitant increase in retailers offering customers the ability to create accounts with stored payment credentials to expedite future transactions. Transactions from accounts of known “good” customers are often fraud-screened with less rigor than those from new customers and, as such, takeover of existing accounts is increasingly seen as an easier path by fraudsters.

- Continued digitization of retail banking transforming the relationships between customers and their banks. Many banks are adopting mobile-centric customer journeys as their primary mode of customer engagement, and this is happening particularly in the Asia/Pacific region. [5] This is leading to continued demand from the banking sector to ensure that abuse of its burgeoning online channels does not hamper this digital transformation.

- Maturing of fraud strategies among retailers and financial institutions to not simply carry out risk assessment at the point of payment, but also to assess risk throughout the customer

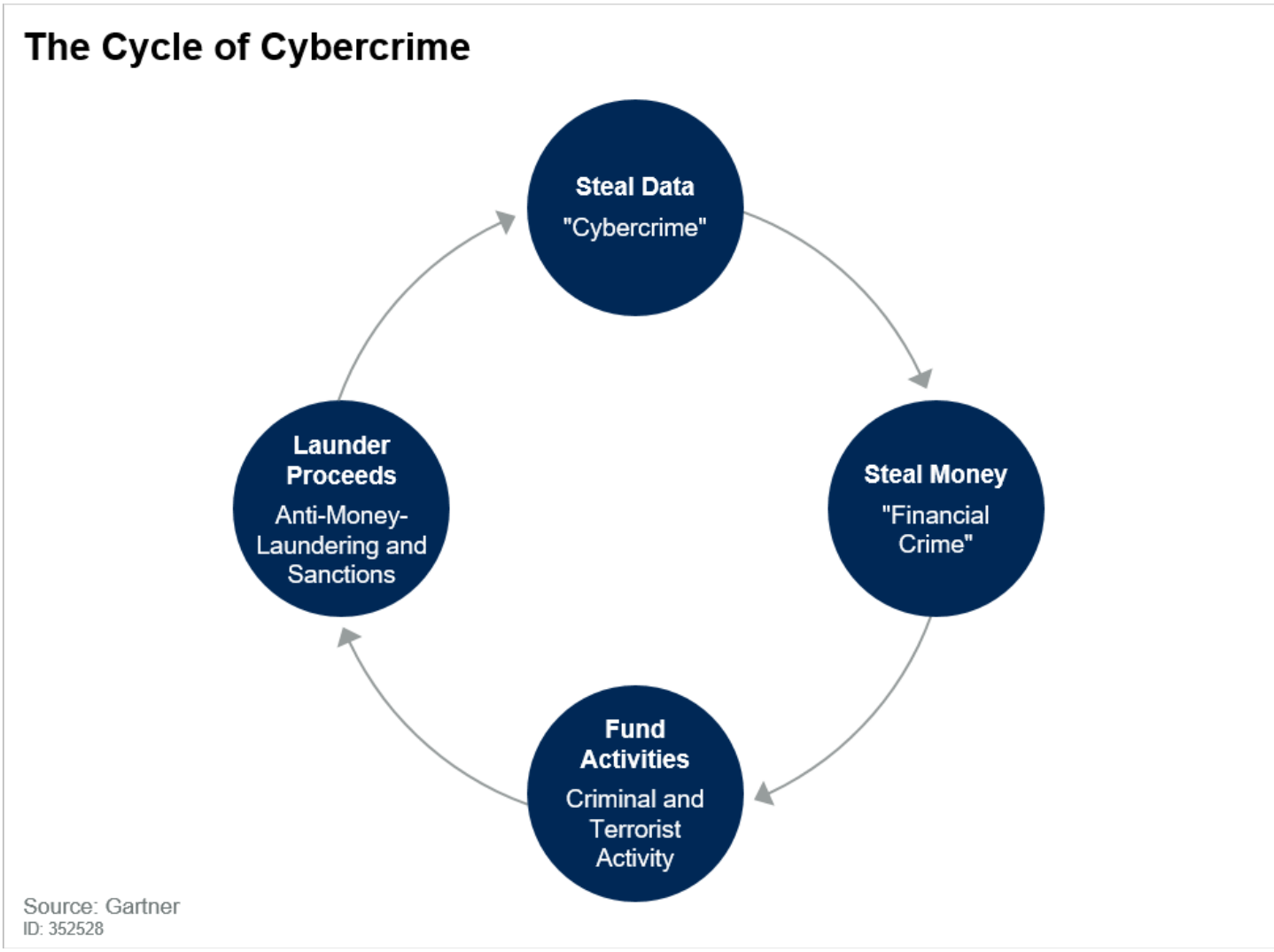
journey. While not all institutions have achieved this level of capability maturity in their fraud detection strategies, it is being actively explored and considered. It is also driving demand in the OFD space for vendors specializing in services that can be applied across the entire customer journey, such as behavioral analytics.

- Increased focus and investment by a number of leading payment processing gateways for retailers on improving their native fraud detection capabilities. This opens up the possibility that, for part of the retail market, it may be sufficient or even advantageous to use fraud detection features available via existing relationships and integration with their payment processing gateway, rather than engaging an OFD vendor.

As noted in the 2018 Market Guide, data breaches are a significant driver of online fraudulent activity. The amount of data being accessed by bad actors has reached levels at which a degree of fatigue and acceptance has become the norm. This culminated in late 2018 with the loss of approximately 383 million customer records by the Marriott Hotels group. [6] Fraud leaders should adopt the mindset that the correct login and password being entered provide little to no assurance that the genuine user is accessing an account. Considerable evidence exists that serious and organized groups are utilizing increasingly sophisticated cyberattack techniques as a precursor to dishonestly obtaining goods and services (i.e., fraud).

Gartner's continuous adaptive risk and trust assessment (CARTA) model (see "Seven Imperatives to Adopt a CARTA Strategic Approach" and "Transform User Authentication With a CARTA Approach to Identity Corroboration") is directly applicable in the OFD market, as continuous assessment of transactional and nontransactional data is key to detecting, containing and eradicating organized fraud campaigns. As shown in Figure 2, there is a strong link between online fraud, money laundering, and criminal and terrorist activity. In addition there is evidence that fraud attacks comprise increasingly sophisticated cyberattacks, as well as the more mundane exploits of special offers and so forth.

Figure 2. The Cycle of Cybercrime



Who Buys Fraud?

One of the persistent questions asked of Gartner is who is commonly involved in the specification, authorization, implementation and operation of fraud detection and prevention solutions. Typically, a number of influencers are found in IT and in the line of business (LOB). Security and risk management leaders are taking an increasingly active role in leading organizational fraud detection and prevention activity, acting as technology advocates working in conjunction with the other stakeholders defined above.

Describing Capabilities/Categories

While noted above that some vendors appear to be working across both retail and banking environments, there remains a number of vendors that predominantly focus on one sector rather than the other. In 2020, Gartner will consider evolving this Market Guide to focus on both

sectors separately to provide greater clarity for clients in each respective sector.

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

Effective online fraud detection requires interpolation of many data types and signals. With the growth of e-business, online fraud detection systems are a necessary component in any security architecture and augment the basic application protection capabilities offered by a web application firewall. OFD systems are found in a variety of business sectors — predominantly financial institutions and retail, but also government, healthcare and others that offer services to the general public via the internet. Vendors listed in Table 2 have one or more of these capabilities and are representative of the evolution of the requirements of these use cases. This list is not meant to be exhaustive, and the presence or absence of a vendor is not indicative of the performance or abilities of a particular vendor's solution.

Table 2: Representative Vendors in Online Fraud Detection

Vendor	Product, Service or Solution Name	Primary Solution Type
Brighterion, a Mastercard Company	Smart Agent	Fraud Analytics
DataVisor	DataVisor Enterprise	Fraud Analytics
Feedzai	Agile Machine Learning	Fraud Analytics
Featurespace	ARIC	Fraud Analytics
Gurucul	Fraud Analytics	Fraud Analytics
SAS	Fraud Management	Fraud Analytics

ThetaRay	Fraud Detection	Fraud Analytics
Accertify, an American Express Company	Fraud Management	Fraud Hub
BAE Systems	NetReveal	Fraud Hub
Bottomline Technologies	Cyber Fraud and Risk Management (CFRM)	Fraud Hub
CyberSource, a Visa Company	Decision Manager	Fraud Hub
Experian	CrossCore	Fraud Hub
Fraud.net	Continuous Risk Monitoring	Fraud Hub
Kount	Kount Complete	Fraud Hub
XTN	SMASH	Fraud Hub
NICE	Actimize	Fraud Hub
Ravelin	Ravelin	Fraud Hub
Sift	Digital Trust & Safety Suite	Fraud Hub
Simility, a PayPal Service	Simility	Fraud Hub
CashShield	CashShield	Chargeback Guarantee
Forter	Decisioning	Chargeback Guarantee

Riskified	Riskified	Chargeback Guarantee
Signifyd	Signifyd	Chargeback Guarantee
Emailage	RapidRisk Score	Data Consortium
Perseuss	Fraud Intelligence	Data Consortium
Nuance	Security Suite	Voice Solutions
Pindrop	Protect	Voice Solutions
Next Caller	VeriCall	Voice Solutions
Auraya	ArmorVox	Voice Solutions
Intelligent Voice	Intelligent Voice	Voice Solutions
BehavioSec	BehavioSec	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
BioCatch	BioCatch	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
iovation, a TransUnion Company	FraudForce	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
NuData Security, a Mastercard Company	NuDetect	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
ThreatMetrix, a LexisNexis Risk Solutions Company	ThreatMetix ID	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
Cleafy	Cleafy	Device Assessment, Endpoint Malware Detection and Behavioral Analysis

Jscrambler	Code Integrity/Webpage Integrity	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
IBM (Trusteer)	Pinpoint	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
SecuredTouch	U-manobot	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
Group-IB	Secure Bank/Secure Portal.	Device Assessment, Endpoint Malware Detection and Behavioral Analysis
Distil Networks	Bot Defense	Bot Mitigation
PerimeterX	Bot Defender	Bot Mitigation
Shape Security	Shape Enterprise Defense	Bot Mitigation
Akamai	Bot Manager	Bot Mitigation
Cloudflare	Bot Management	Bot Mitigation

Source: Gartner (April 2019)

Market Recommendations

As Fraud Threats Change and Evolve, Ensure That the Solution Can Flex and Accommodate New Modes of Customer Interaction

As new attacks develop on both existing channels and new channels (such as social media), fraud leaders much orchestrate detection and analytical capabilities to ensure use of this new data, and that the customer-centric risk model remains holistic. New challenges will arise as new threats occur, and it is therefore imperative that the solution be extensible and agile with respect to accommodating new channels.

Make Decisions From All Vendor Data Sources on a Single Platform

With the ever growing market of OFD vendors, it is tempting for retailers and financial institutions to continually add new specific vendors to bring additional capabilities to their fraud detection toolkit (for example, by adding behavioral analytics or endpoint profiling). Security and risk management leaders must ensure that data from all of these vendor sources is aggregated onto a single platform for decision making and analysis. This will avoid the creation of both data and decision silos, the formation of which creates opportunities for fraudsters.

Take an Omnichannel View of Fraud Detection

Security and risk management leaders must include all digital channels (web, mobile, telephony) in their fraud detection strategy, providing an omnichannel view of how fraudsters are attacking the business. This will minimize the risk of a fraudster simply migrating to one channel after being blocked on another. In line with the previous recommendation, this also involves leveraging a single centralized decision platform to ensure that data attributes and patterns of behavior can be correlated across all channels.

Evaluate Risk Across the Entire Customer Journey

Decision making about the risk level associated with a transaction needs to be pushed upstream to begin prior to the point of payment. Security and risk management leaders must create a fraud detection regimen that begins to assess risk from when the customer arrives on their digital premises. This includes assessing behavior, evaluating the likelihood of bots or scripts being used, monitoring account login or creation, and defining the risk of the action being carried out. Also required is implementing appropriate challenges along that journey commensurate to the judged risk.

Evidence

[1] "Signifyd Secures $100 Million Series D Funding," Signifyd; "Forter Proudly Announces $50 Million in Series D Funding," Forter.

[2] "Kount Bolsters Authentication With Latest Version of Passive Behavioral Biometrics," Kount.

[3] Accertify's InAuth partners.

[4] "Annual Retail E-commerce Sales Growth Worldwide From 2014 to 2021," Statista.

[5] "2019 Banking Industry Outlook: Optimism for Banking and Capital Markets," Deloitte.

[6] "World's Biggest Data Breaches and Hacks," Information is Beautiful.

Note 1
Representative Vendor Selection

Representative vendors were selected on the basis of one or both of the following:

- Frequent inquiry by Gartner clients about that vendor for online fraud use cases
- Vendors that are offering capabilities supporting online fraud detection in a way that is unique, innovative and/or that demonstrates a forward-looking product strategy

Note 2
Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.