AiteNovarica

AUGUST 2022

AITE MATRIX: LEADING BOT DETECTION AND MANAGEMENT PROVIDERS

JIM MORTENSEN
TARI SCHREIDER

This excerpt provided compliments of this Best-in-Class vendor:

HUMAN

IMPACT REPORT

IMPACT REPORT

AUGUST 2022

AITE MATRIX: LEADING BOT DETECTION AND MANAGEMENT PROVIDERS

JIM MORTENSEN
TARI SCHREIDER

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Bad actors, nation-states, and ransomware operators use bots to launch attacks that deny access to computer resources, take over accounts, and commit fraud and computer crimes. Bad bot traffic overwhelms fraud and security personnel; bots performing malicious tasks comprise as much as 40% of internet traffic. Bots have become increasingly sophisticated and automated, creating a growing cybercrime economy.

Bot solutions have been around for over 10 years, but criminal bot operators always find ways to keep one step ahead. Today's institutional bot strategy is no longer about preventing malicious bots; it's about making it uneconomical to pursue an organization as a target. If criminal bot operators find their overtures and attack strategies against an organization are too difficult, they will move on to another, more vulnerable target.

This Impact Report shows how organizations can protect themselves from bot attacks. It explores the key trends within the bot detection and management market and discusses how technology is evolving to address market needs and challenges. This report also introduces organizations to leading bot prevention and management vendors and compares them, highlighting their primary strengths and areas for enhancement.

Finally, this Impact Report is designed to help companies make informed decisions as they examine the market and evaluate adopting new functionality, outlining a roadmap of key considerations as they begin that process.

METHODOLOGY

This Impact Report examines the state of the bot prevention and management market and participating vendors using primary and secondary research. The primary research is from interviews, surveys, and demonstrations of the 10 vendor solutions. Aite-Novarica Group looked outside the key vendors presented within its Aite Matrix report to gain a broader perspective of market players and size. Solutions solely targeting gaming and advertising verticals were excluded, as this report focuses on the impact of bots on financial services.

The research performed for this report included a general analysis of 27 bot prevention and management vendors and 10 deep-dive investigations of vendors participating in Aite-Novarica Group's Aite Matrix process, including client reference interviews related to those vendors. The research for this report occurred from November 2021 through

June 2022. Given the size and structure of the research, the data in this report are considered a directional indication of conditions in the market and the profiled vendors.

Leveraging the Aite Matrix, a proprietary Aite-Novarica Group vendor assessment framework, this Impact Report evaluates the overall competitive position of each vendor, focusing on vendor stability, client strength, product features, and client services. The following criteria were applied to develop a list of vendors for participation:

- Each participating vendor must have bot detection and management software deployments in production in financial services. Eligible vendors include only software-based solutions and not those providing hardware-based appliances.
- Each participating vendor must have had more than US$10 million in annual revenue in one of the last two years.

Participating vendors were required to complete a detailed product request for information (RFI) composed of qualitative and quantitative questions, conduct a product briefing and demo, and provide active client references.

THE PLAYERS

This section presents comparative data and profiles for the individual vendors participating in the Aite Matrix evaluation. This comparison is by no means an exhaustive list of vendors. Firms looking to undergo a vendor selection process should conduct initial due diligence before assembling a list of vendors appropriate for their unique needs.

Table A presents basic vendor information for the participating solutions.

TABLE A: EVALUATED VENDORS

COMPANY	HEADQUARTERS	FOUNDED	TYPE	EMPLOYEES	FUNDING (US$ MILLIONS)
Akamai Technologies Inc.	Cambridge, Massachusetts	1998	Public	Over 9,000	N/A
Arkose Labs Inc.	San Mateo	2017	Private	186	US$114
BioCatch Inc.	Tel Aviv, Israel	2011	Private	Over 200	US$215
Cequence Security Inc.	Sunnyvale, California	2015	Private	Over 100	US$100
DataVisor Inc.	Mountain View, California	2013	Private	Over 120	Over US$70
F5 Inc.	Seattle	1996	Public	Over 6,000	US$183 (Shape Security)
HUMAN Security Inc. (Goldman Sachs)	New York	2012	Public	Over 250	US$142
Kasada Pty Ltd.	New York	2015	Private	78	US$39

COMPANY	HEADQUARTERS	FOUNDED	TYPE	EMPLOYEES	FUNDING (US$ MILLIONS)
Mastercard Technologies Canada	Vancouver, British Columbia	2008	Public	NuData: 88 (estimated) Mastercard: 24,000	NA
Radware Ltd.	Mahwah, New Jersey	1997	Public	Over 1,200	NA

Source: Vendor RFI responses

THE MARKET

Online attacks are a pernicious threat to companies of all types, but they can be particularly destructive to FIs and merchants. Fraudsters continue to leverage tools to make these attacks more effective and less costly to perpetrate. At the same time, fraud and cybersecurity professionals focus on defenses that deal with new and evolving attack vectors. The effect is similar to a game of multidimensional chess in which the number of dimensions continually change, and the participants add new chess pieces with different movement capabilities while the game is ongoing. These conditions make for a dynamic market with several trends (Table B) shaping the present and future of the market landscape for bot detection and management solutions. These trends are discussed in greater detail below.

TABLE B: MARKET TRENDS AND IMPLICATIONS

MARKET TRENDS	MARKET IMPLICATIONS
Growth in e-commerce and online servicing	Consumers have been migrating to digital channels for shopping and servicing, increasing the attack surface through an explosion in the availability of compromised online credentials.
Higher fraud rates in digital channels	The broad availability of compromised personally identifiable information (PII) and login credentials means criminals prefer digital channels to afford a broad attack surface and provide a cloak of anonymity.
Pervasiveness of inventory hoarding bots	Bots that accumulate or hoard scarce items, such as limited-edition sneakers, are detrimental to a retailer's brand because they prevent legitimate and loyal customers from acquiring products at the retail price.
Increase in cyberattacks by nation-states	The rate of nation-state attacks continues to increase, challenging the ability of cybersecurity professionals to detect and mitigate these targeted threats adequately.

MARKET TRENDS	MARKET IMPLICATIONS
Pressures on customer experience improvement	Customer experience has always been important, but companies are looking to provide a consumer experience with minimal to no disruption for good customers and challenges that are easy for a human to solve but difficult, if not impossible, for bots to crack.
Deployment of ML technology	Advances in ML and the near-ubiquity of the technology have facilitated the creation of hard-to-detect bots and fueled the efficacy of bot detection tools. But it has also facilitated the creation of hard-to-detect malicious bots.
Availability of funding for new fintech startups	The availability of funding for innovative fintech startups has enabled them to get a foothold in the market and develop novel technologies and methods to detect bots and mitigate their impact.
Specialized bot and fraud platform solutions expanding the vendor landscape	Bots have become more sophisticated and harder to detect, and new bot detection and fraud providers have emerged with solution approaches that elevate detection and mitigation requirements.
Move toward bot management vs. bot elimination	An acceptance that bot attacks will never be eliminated as a threat has driven increased investments in bot threat intelligence, bot hunting, and the development of challenge techniques that are costlier for fraudsters to solve.

Source: Aite-Novarica Group

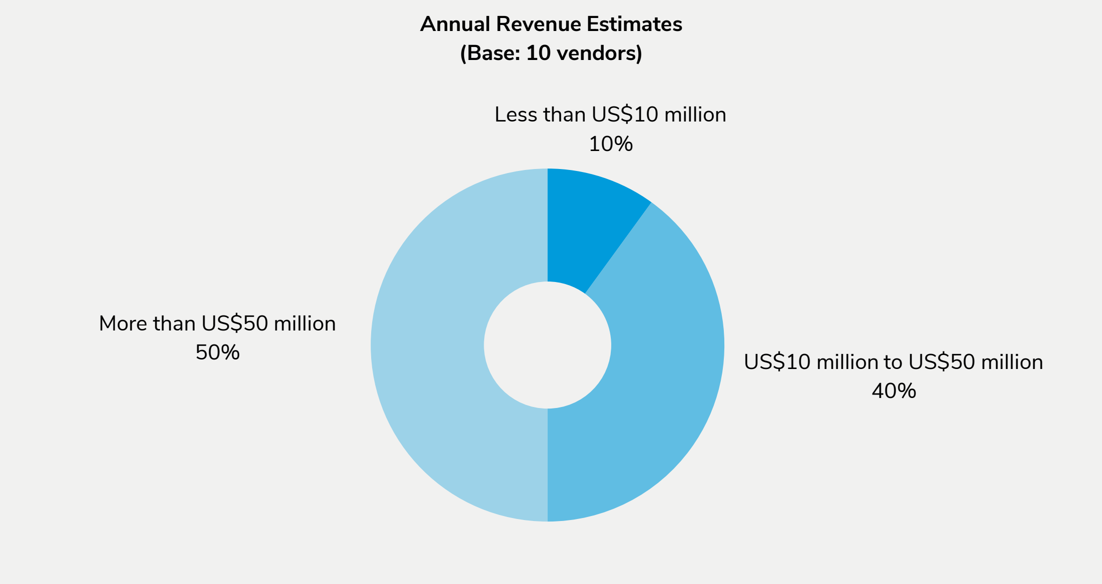
KEY STATISTICS

This section provides information and analysis on key market statistics related to the bot detection and management vendor market.

ANNUAL REVENUE ESTIMATES

The vendors that provide bot detection and management capabilities consist of established market participants and relatively new entrants. Well-established providers have strong client bases, diverse revenue streams, financial strength, and often an array of IT and security-related solutions. Some of these companies are publicly owned enterprises, generating a combined annual revenue of over US$80.6 billion. Newer entrants generate lower annual revenue than their established peers, but they are penetrating the market and are often innovators, given their narrow focus (Figure 1).

FIGURE 1: ANNUAL REVENUE ESTIMATES BREAKDOWN



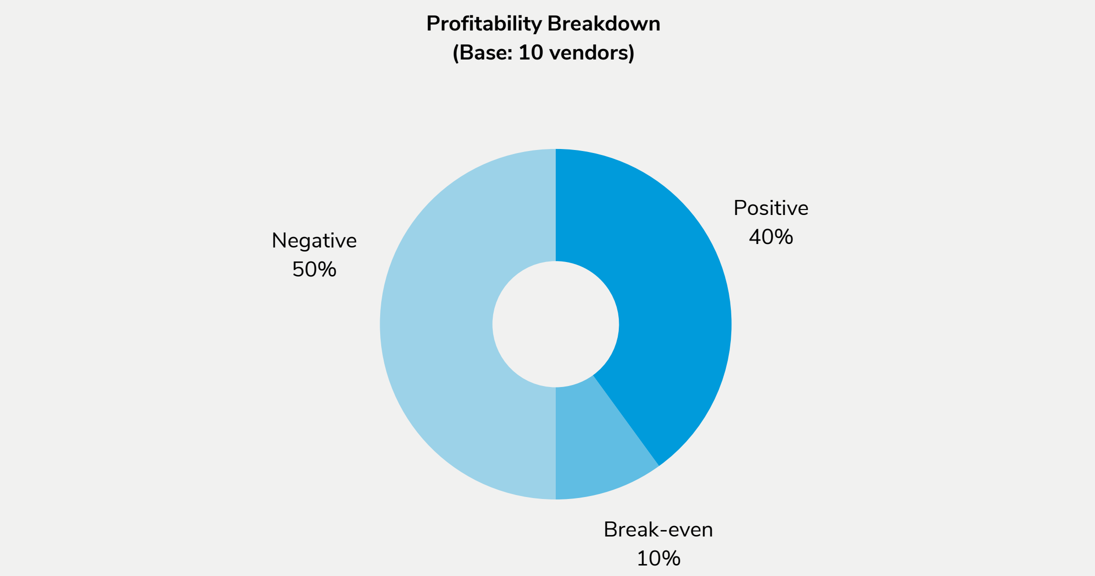
Source: Vendors

PROFITABILITY AND GROWTH RATE ANALYSIS

Only 40% of the vendors in this Aite-Novarica Group study are currently profitable, while 10% are breaking even (Figure 2).

The remaining half of the participating vendors (50%) currently operate at a loss. These companies are relatively new, i.e., established within the last six years; they continue to invest significantly in R&D and growth. As with any new company that has yet to achieve profitability, buyers should be aware and consider whether the company will survive or be acquired when they consider becoming a customer.

FIGURE 2: PROFITABILITY ANALYSIS



Source: Vendors

All vendors that participated in the study reported growth rates exceeding 15%. This result supports the market CAGR of approximately 13%, as there is a bit of churn across markets, and many customers leverage more than one bot solution for specialized purposes.

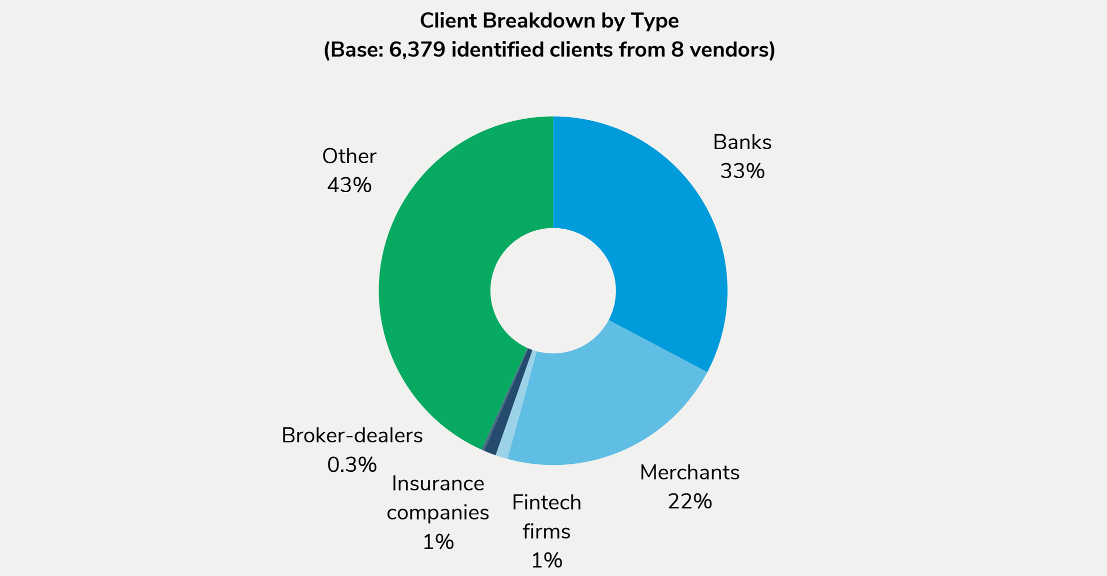
R&D INVESTMENT ANALYSIS

Given the continuing sophistication of bot attack techniques and capabilities, bot management providers must continue to invest in R&D to stay relevant. Clients are perpetually searching for new and innovative solutions to detect bot attacks and effectively mitigate those attacks in the least disruptive way possible. Bot management vendors invest heavily in their products to expand their capabilities, functionality, and features. Not investing at a high level would cause them to fall behind their competition and, as importantly, the fraudsters. As a result, all participating vendors invest more than 15% of their revenue in ongoing R&D.

BOT DETECTION AND MANAGEMENT CLIENT ANALYSIS

The bot detection and management production client breakdown among the participating vendors illustrates that bot detection and management solution adoption is most prevalent among banks, at 33%. Merchants follow with 22% of the clients and slightly over 2% combined across broker-dealers, insurance companies, and fintech firms. A large dispersion of other companies represents the majority of clients, at 43%. (Figure 3).

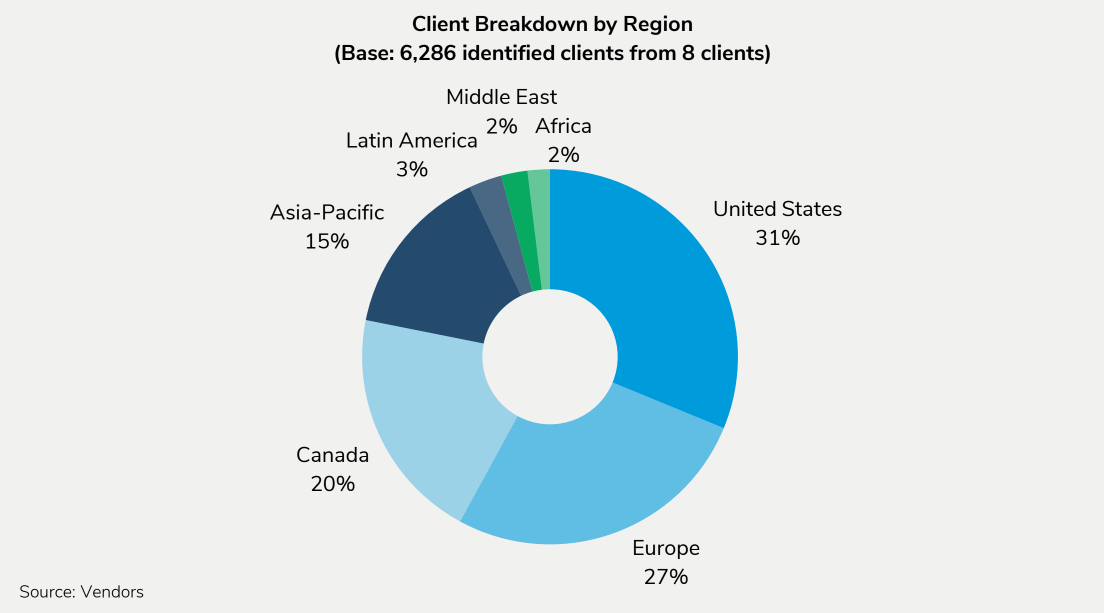
FIGURE 3: CLIENT INDUSTRY ANALYSIS



Source: Vendors

The U.S., Canada, and Europe account for 78% of the clients of eight of the participating vendors. Asia-Pacific accounts for 15% of the clients of the respective vendors, with the remainder (7%) comprising Latin America, the Middle East, and Africa (Figure 4).

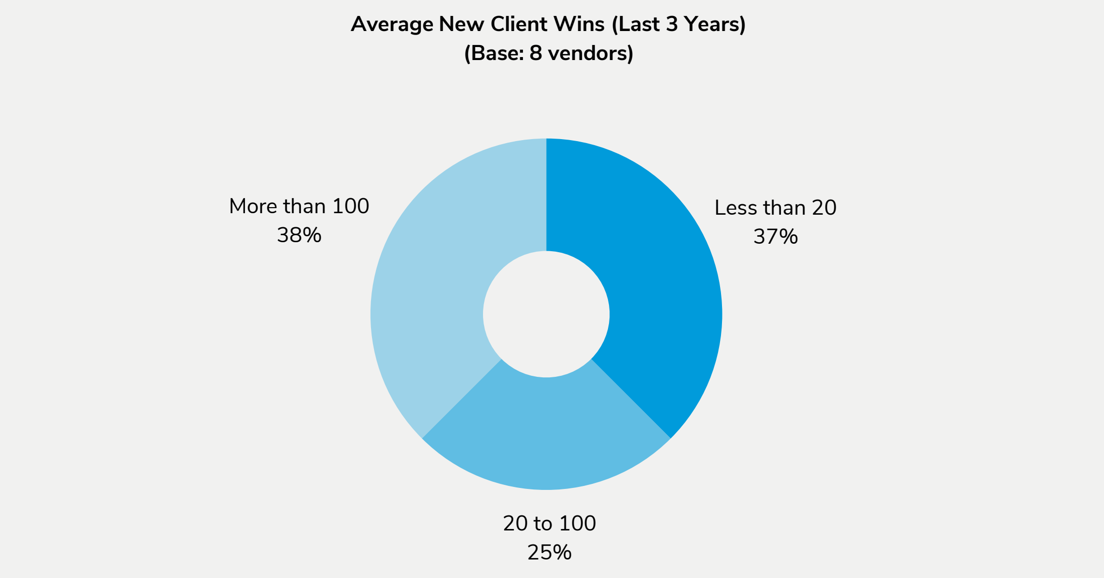
FIGURE 4: CLIENT GEOGRAPHIC ANALYSIS



Source: Vendors

Of the eight vendors providing the underlying data, a plurality (38%) of providers enjoyed greater than 100 average new client wins over the last three years. Twenty-five percent experienced between 20 and 100 new client wins, and 37% reported less than 20 wins (Figure 5).

FIGURE 5: NEW CLIENT WINS

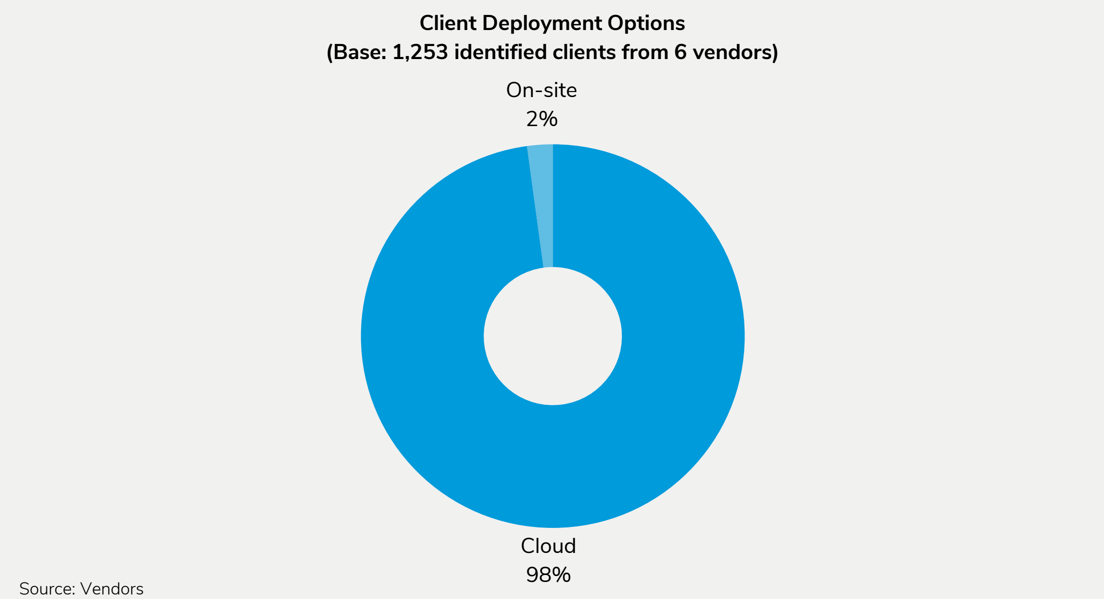


Source: Vendors

DEPLOYMENT OPTIONS

Like other software providers, bot detection and management vendors have embraced cloud deployments vs. on-site deployments. Of the reporting vendors, 98% of deployments were cloud deployments, with a mere 2% being on-site. Given the dynamic nature of attack vectors, the key benefit of cloud deployments is that vendors can quickly implement updates to threat detection capabilities and make them available to clients (Figure 6).

FIGURE 6: CLIENT DEPLOYMENT OPTIONS



Source: Vendors

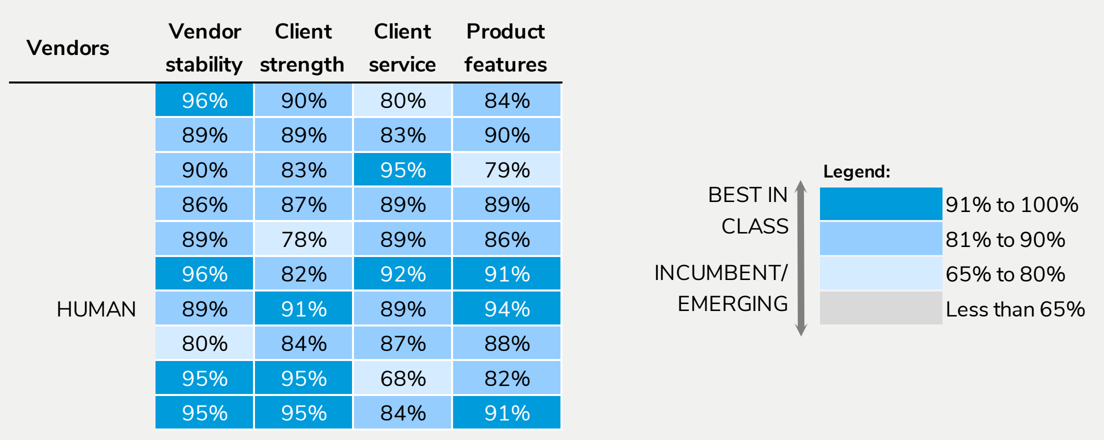
AITE MATRIX EVALUATION

This section breaks down the individual Aite Matrix components, drawing out the strongest bot detection and management vendors in each area and how they are differentiated in the market.

THE AITE MATRIX COMPONENTS ANALYSIS

Figure 7 provides an overview of how each vendor scored in the various areas of importance. Each vendor is rated, in part, based on its data provided when responding to the RFI that Aite-Novarica Group distributed and product demos and follow-up discussions as part of the Aite Matrix process. Ratings are also driven by the references provided by the customers of the examined vendors to support a multidimensional rating.

FIGURE 7: AITE MATRIX COMPONENT ANALYSIS HEAT MAP



Vendors	Vendor stability	Client strength	Client service	Product features
	96%	90%	80%	84%
	89%	89%	83%	90%
	90%	83%	95%	79%
	86%	87%	89%	89%
	89%	78%	89%	86%
	96%	82%	92%	91%
HUMAN	89%	91%	89%	94%
	80%	84%	87%	88%
	95%	95%	68%	82%
	95%	95%	84%	91%

BEST IN CLASS
INCUMBENT/ EMERGING
Legend:
91% to 100%
81% to 90%
65% to 80%
Less than 65%

Source: Aite-Novarica Group

Vendor Stability

Steadily growing and ultra-competitive, the bot detection and management market consist of long-established market incumbents with a few relatively new entrants. Well-established providers have strong client bases, robust revenue streams, and financial strength. Half the vendors participating are publicly owned, generating a combined annual revenue of over US$80.6 billion. Unsurprisingly, the public companies profiled in this report scored well for vendor stability as they have the resources to invest in expanding market share and research and development.

Several of the newer firms profiled were founded in the last six years and, as such, are still building their full product suite but catching up quickly. These firms are gaining market traction, with some growth coming from converting older bot detection and management products to their newer technology. As these companies grow and develop, they will become more stable, and their solutions will continue to be innovative, given their focus and agility.

Client Strength

Sustained growth requires the ability to maintain existing customers and attract new ones. This category evaluates provider strength based on important factors, such as the total number of bot management clients in production, the diversity of those clients, client retention rate, reference checks on the vendor's reputation in the market, and customer feedback regarding their likelihood to replace their solution.

Most of the providers in the bot detection and management solution space have been effective in retaining customers. However, further penetrating a highly competitive market can be challenging. Clients are continually looking for solutions with greater efficacy as fraudsters and bot operators continue to improve their capabilities. The never-ending search for the best solution places all vendors at risk of being replaced by the next great thing in bot detection and management. The move toward SaaS platforms creates a dual-edge sword. On one side of the sword, updates and support are easier; on the other, it is now easier to replace an incumbent solution. Changing to a new bot management provider can be done with a relatively short payback period. HUMAN scored highly in this area.

Client Service

Strong client service has become a must to achieve customer satisfaction and demonstrate how committed a vendor is to ensure its customers receive the highest standard of products and services. Fraud and cybersecurity executives often expect vendors to become strategic partners, collaborating and guiding them on near-term and long-term technology adoption. Customers continue seeking greater visibility into and enhanced documentation on current product changes and future development. Customers expect quick resolution of defects and issues and continual advancements in design, usability, functionality, and performance.

Client ratings of the vendors' service and support, responsiveness, ability to deliver on promises, and cost-to-value ratios were the primary drivers of the ratings in this category, along with the vendor's position on key support items, such as providing 24/7 support, having a dedicated point of contact, facilitating customer advisory boards, and offering global/localized support.

The top-scoring vendors in this area include HUMAN. For many vendors, the overall scores indicate that client service remains a huge opportunity to achieve an advantage, especially as the competition among solutions continues to escalate.

Product Features

The ability to enable sophisticated rules and model development, testing, validation, and deployment is core to today's bot detection and management solutions. Bringing a more integrated AI approach, leading solutions enable an Agile orchestration of ML techniques and facilitate integration across disparate systems and data sources to produce superior bot detection capabilities. In addition, an essential component is the ability to successfully challenge suspected malicious bots with techniques that inject minimal to zero friction for true consumers and are highly effective in arresting malicious bot traffic.

In addition, an ability to understand bot attack volume and related mitigation is essential as a core product feature that most buyers require. A comprehensive and easy-to-use dashboard with the ability to customize metrics and reports is required by all clients to have confidence in their ability to manage their applications effectively. Many clients also require the ability to have ready access to all underlying data and the ability to merge that data with other proprietary data for a fuller analysis of their cybersecurity threats.

Although quality, performance, and service outweigh cost and pricing considerations for most organizations, the total cost cannot be ignored. Focused on organizations that simply want a bot detection and management solution that works out of the box with little custom configuration, some providers deliver simpler solutions requiring little active management.

This category considers feedback from clients regarding the robustness and breadth of bot detection capabilities, the approach to challenges in terms of injected friction, overall solution usability, and intuitiveness. The score also considered ease of deployment, integration, reporting, and the provider's ability to understand new threats and quickly deliver detection and mitigation techniques to counter those new threats. The top-scoring vendor is HUMAN.

THE AITE MATRIX RECOGNITION

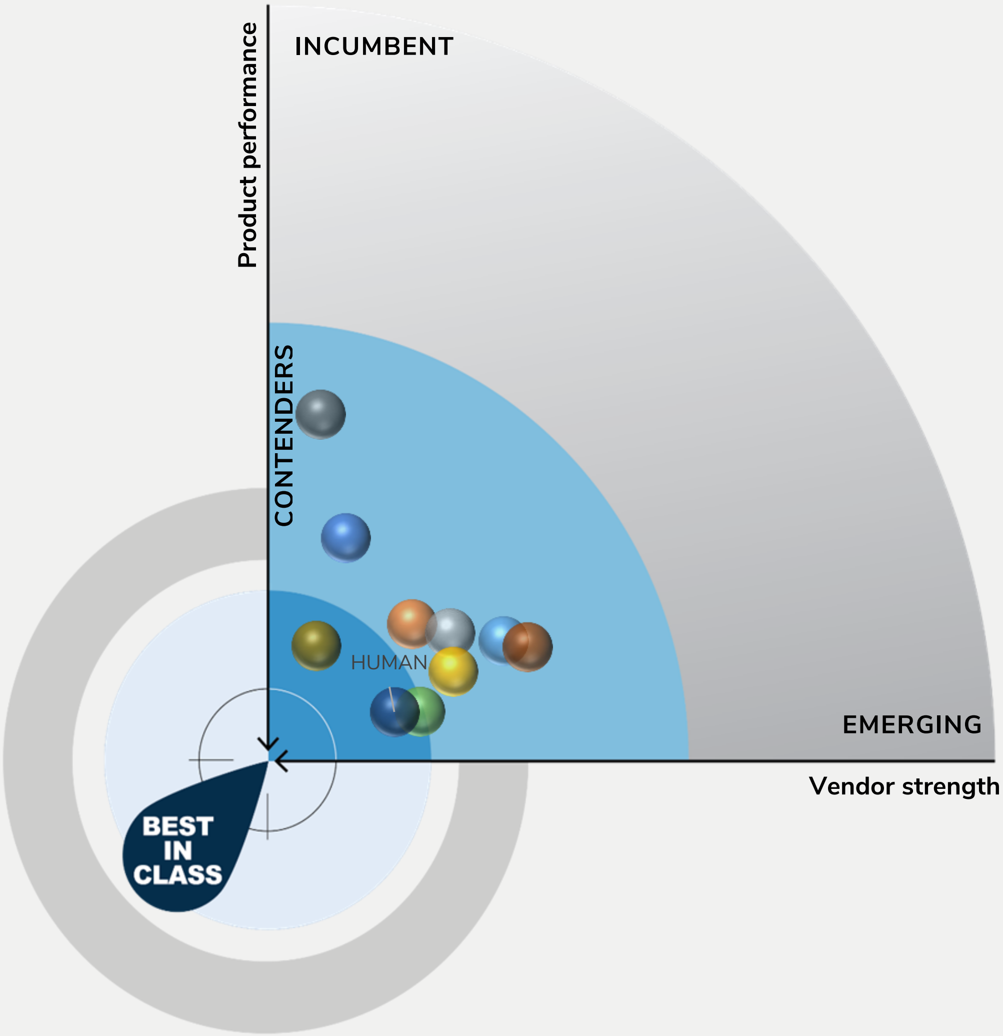
Three major factors drive the final results of the Aite Matrix recognition:

- Vendor-provided information based on Aite-Novarica Group's detailed Aite Matrix RFI document
- Participation in vendors' client reference feedback or feedback sourced independently by Aite-Novarica Group
- Analysis based on market knowledge and product demos provided by participating vendors

Figure 8 represents the final Aite Matrix evaluation, highlighting the leading bot detection and management solutions vendors.

FIGURE 8: BOT DETECTION AND MANAGEMENT AITE MATRIX

Leading Bot Detection and Management Providers Aite Matrix



Source: Aite-Novarica Group

BEST-IN-CLASS VENDOR: HUMAN

HUMAN is among the three vendors that achieved best-in-class Aite Matrix status with a 90% or more composite score in all four categories. These vendors have invested in bot detection and management solutions for ten years, defending against bad bots for over 7,000 global customers. Their popularity is greatly owed to their deployment flexibility, ease of use, and robust product features. These vendors have more than 90% customer retention and extremely high customer satisfaction ratings. These vendors provide solutions that significantly reduce the incidence of bad bots. Organizations looking to solve their bad bot problem will find these best-in-class vendors exceptional performers.

HUMAN has an exclusive focus on bad bot prevention. It has the edge in vendor stability and makes significant investments in bad bot detection. HUMAN verifies 15 trillion digital interactions weekly and over three billion unique devices monthly. Customers of HUMAN love its products and admire the company and its founders. Human is poised to catapult in the bot detection and management market—in July 2022, it announced plans to merge with PerimeterX, a premier bot management platform.

BEST IN CLASS: HUMAN SECURITY INC.

HUMAN, acquired by Goldman Sachs, a US$54.5 billion public in 2020, was formerly known as White Ops, a New York-based cybersecurity company specializing in bot detection solutions. Founded in 2012 by Tamer Hassan, Michael Tiffany, Dan Kaminsky, and Ash Kalb, HUMAN employs over 250 people across the U.S.; Victoria, British Columbia, Canada; London; and Singapore. It recently raised US$100 million in a growth funding round led by WestCap and NightDragon, bringing its total investment funding to USD$142.1 million. Key clients include Yahoo, Adobe, MediaMath, and Xandr.

HUMAN employs ML, global threat intelligence, technical evidence, and continuous adaptation to thwart sophisticated bot attacks and fraud. Each week, HUMAN verifies the humanity of 15 trillion interactions. The HUMAN approach to modern defense emphasizes integrated, collective protection with more than 2,000 customers. The company has coordinated efforts among customers, partners, and law enforcement to spearhead major botnet disruptions and takedowns, including the botnet 3ve, which led to 10-year prison sentences for the cybercriminal ringleaders involved.

On July 27, 2022, HUMAN announced it would merge with PerimeterX, a leading bot management solution producer. The combined entity will comprise nearly 500 employees and eventually fall under the HUMAN Security name once the two platforms are integrated. Human received a $100 million debt facility from Blackstone Credit as part of the deal.

Aite-Novarica Group’s Take

HUMAN has protected customers’ digital experiences for a decade, giving them the hindsight of actionable intelligence built on combating cyber adversaries. HUMAN has grown from humble beginnings in the back of a sci-fi bookstore into one of the largest bot detection and management companies with over 2,000 customers. HUMAN’s reach into the bad bot and fraud underworld is vast, with 2,500 dynamic network, device, and behavioral signals across 350 algorithms (technical, statistical, and ML). Its bot battling philosophy, called modern defense, is based on raising the cost of every attack and lowering the cost of collective defense with takedowns, deception, and other innovations whereby bad actors give up or seek another target. Three billion unique devices—more than half of all internet devices—are verified monthly to sort the good from the bad.

HUMAN has taken a leading role in coordinating efforts with many of its customers, partners, and law enforcement to orchestrate major botnet disruptions and takedowns, including 3ve, Methbot, and PARETO. HUMAN's philosophy is collective protection, where an attack on any of its customers becomes a defense for all customers.

A key pillar in HUMAN's mission to defeat bot-driven cybercrime is the ability to find and disarm threats before they impact customers and partners. Its Satori threat intelligence and research team is the group tasked with shining a light into the dark corners of the internet to find cybercriminals' plans and develop strategies to defend against them.

HUMAN has over 95% customer retention, signaling strong acceptance of its modern defense approach to bot detection and management. Its technical observability of 2,500 bot signals and verification of over half the devices on the internet monthly affords it unparalleled insight into bot threats. The company is expanding from its origins in protecting against bots defrauding advertising companies to a broader customer base, including financial services and neo-fin, with the support from Goldman Sachs. Customers are now getting used to its new user interface with improved results. Its specialty is determining the difference between humans and bots based on their vast threat intelligence capability, especially emerging bots and fraud. The financial backing of Goldman Sachs, large customer base, high customer retention rate, and roadmap make HUMAN a long-term player in the bot detection and management market.

Table C provides basic firm and product information.

TABLE C: BASIC FIRM AND PRODUCT INFORMATION, HUMAN

CATEGORY	DESCRIPTION
Headquarters	New York
Founded	2012
Website	www.humansecurity.com
Number of employees	Over 250
Ownership	Public (NYSE: GS)—The Goldman Sachs Group, Inc.

CATEGORY	DESCRIPTION
Global business footprint	Offices in New York; Washington DC; Victoria, British Columbia, Canada; London; and Singapore
Key product names	BotGuard for Applications, BotGuard for Growth Marketing, MediaGuard, and Bot Insights
Product version and release	2012
Target customer base	Merchants, enterprises, and publishers
Number of bot management clients	Over 2,115
Global client footprint	Clients are located globally
Implementation options	On-site, hosted, and cloud with API, CDN, edge, reverse proxy, mobile, and SDK options
Key implementation partners	Google Cloud Services, AWS, Optiv, Fastly, and Accenture
Product version frequency schedule	Continual updates (weekly, biweekly, monthly)
Pricing structure	Fixed price per 1,000 transactions, then based on level of volume
Percentage of revenue invested in R&D	Over 15%

Source: HUMAN (as of June 30, 2022)

Key Features and Functionality Based on a Product Demo

- **Deployment:** Multiple integrations (including Fastly, Cloudflare, CloudFront, and NGINX) and Android and iOS SDKs to allow BotGuard to install into a range of architectures. Responses can also be configured using a dynamic policy engine (via API) within the dashboard, allowing customers to manage the bot mitigation logic inside the HUMAN dashboard without making additional adjustments to their codebase.

- **Bot detection:** The solution observes 2,500 user devices and interaction indicators. It uses several signal sources, including technical indicators, device-configuration signals, behavior-based signals, network signals, and customer email addresses. The polymorphic signal collection includes multilayered detection techniques, separation of detection and enforcement indicators, and delayed feedback loops to prevent evasion. Bot traffic is categorized based on collected signals, behaviors, and fingerprints.
- **Bot mitigation:** Customers can create a playbook to mitigate attacks using challenges, terminations, selective request denial, traffic throttling, or customer-defined techniques.
- **Outcome tagging:** Feedback is automatically fed to the platform and disseminated to customers.
- **New threat identification and management:** Actionable threat intelligence and insights are built on over 10 years of combating adversary attack vectors, tools, and methodologies derived from the threat hunting and intelligence teams.
- **Dashboard/Reporting:** Out-of-the-box and custom reporting are available in the dashboard and via a specialized reporting API. Through this same interface, alerts can be configured based on configurable thresholds. The dashboard allows for managing all HUMAN products across web, advertising, and mobile properties in a centralized manner.
- **Performance management:** Component-level consoles are used to monitor platform performance. Twenty milliseconds of latency is the average per-user experience. The platform is designed to support over 10 million transactions per second.

Top Three Strategic Product Initiatives Completed Over the Past Three Years

- BotGuard for Marketing helps marketers keep fake leads and referrals generated by bots from contaminating customer acquisition funnels (October 2019).
- BotGuard for Applications helps security and fraud teams keep cybercriminals out of their online applications and services (Feb 2020).

- BotThreat Insights are provided by bot mitigation specialists acting as an extension of the client's fraud and cybersecurity teams to help identify and respond to sophisticated bots (November 2021).

Top Three Strategic Product Initiatives in the Next 12 to 18 Months

- Expand Device ID to fraud use cases
- Provide client-side security
- Offer integrated application security stack as a service

Client Feedback

HUMAN's customers are a near cult-like following, loving the company as much as the product. Customers wanted to extoll the company's virtues over the product. The customer's love for HUMAN as a company equals their uniform agreement that service and support are superior to other vendor experiences. As one customer stated, "they're willing to help whenever always going above and beyond expectations." All customers stated there would be no chance of them changing vendors.

Customers pointed out some room for improvement as well. One area is that although the new user interface adds functionality, it is not as easy to use. Customers would like an improved ability to add inventory types and develop inventory on audit detection methodologies. While several customers acknowledge other products are inferior in this area, they would still like to see some improvements. Another area called out for improvement is on the impression detection side, where an improvement in click fraud post impressions metrics was needed.

Table D summarizes HUMAN's product strengths and improvement opportunities based on client feedback.

TABLE D: STRENGTHS AND IMPROVEMENT OPPORTUNITIES, HUMAN

STRENGTHS	IMPROVEMENT OPPORTUNITIES
Customer service, product support, and management approachability	Product documentation and revision communication
Cost value equation of the product	Click fraud post impressions metrics
Product technology stack and performance	Expanded malware detection capabilities

Source: Aite-Novarica Group

CONCLUSION

Aite-Novarica Group has concluded advice for buyers and sellers of bot detection and management solutions.

Solution buyers:

- Bring all relevant stakeholders to the table early to define requirements, functionality, roles, and responsibilities. Ensure the solution addresses the bad bot risk problem and the ability for the solution to grow with the institution's needs.
- Understand the current control framework and its strengths, weaknesses, and gaps to identify whether a new solution is necessary or the current solution requires augmentation. Also, ensure easy integration with an existing fraud framework.
- Understand your threat landscape, related defense needs, and constituent group requirements before entering into discussions with solution providers, as this will help create the list of potential vendors.
- Pursue products that address the 21 OWASP automated threats as that should be a key selection criterion for those in the market for bot detection and management solutions.
- Determine if the bot detection and management solution can be configured to protect the domain, URL, or page level addressing user requirements. Configuration decisions may affect the price of solutions.
- Consider using rate limiting based on client, device, etc., to respond to IP address spoofing and rotating attacks to increase detection efficacy.
- Understand budget parameters and perform a TCO before making a purchasing decision, as usage costs over time can be more expensive than a larger initial purchase price.
- The more sophisticated bot detection and management products are, the greater the potential for higher latency rates to increase. Products that recognize the mimicking of human behavior require more performance cycles than products focused more on rules. Ensure use cases exercising the whole product are tested to evaluate latency.
- Consider solutions that offer service level guarantees, especially those with an insurance-backed warranty.

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Jim Mortensen
+1.480.937.0445
jmortensen@aite-novarica.com

Tari Schreider
+1.470.524.2670
tschreider@aite-novarica.com

Contributing author:
Gabrielle Inhofe
+1.539.215.9118
ginhofe@aite-novarica.com