The Forrester New Wave™: Bot Management, Q1 2020

The 13 Providers That Matter Most And How They Stack Up

by Sandy Carielli and Amy DeMartine
January 29, 2020

Why Read This Report

In Forrester's evaluation of the emerging market for bot management, we identified the 13 most significant providers in the category — Akamai Technologies, Alibaba Cloud, AppsFlyer, Cloudflare, DataDome, Imperva, Instart, Netacea, PerimeterX, Radware, Reblaze, Shape Security, and White Ops — and evaluated them. This report details our findings about how well each vendor scored against 10 criteria and where they stand in relation to each other. Security pros can use this review to select the right partner for their bot management needs.

Key Takeaways

Netacea, PerimeterX, Akamai Technologies, And Imperva Lead The Pack

Forrester's research uncovered a market in which Netacea, PerimeterX, Akamai Technologies, and Imperva are Leaders; White Ops and DataDome are Strong Performers; Shape Security and Radware are Contenders; and Alibaba Cloud, Cloudflare, AppsFlyer, Instart, and Reblaze are Challengers.

Attack Detection, Attack Response, And Reporting Are Key Differentiators

The top bot management tools combine extensive signal collection with deep analysis to detect simple and sophisticated attacks. Attack responses range from basic blocking to methods that increase attacker costs to make the attack economically unviable. Reports and dashboards that address both security and business contexts will be attractive to buyers whose marketing, executive, eCommerce, and security stakeholders are all affected by bots.

The Forrester New Wave™: Bot Management, Q1 2020

The 13 Providers That Matter Most And How They Stack Up

by Sandy Carielli and Amy DeMartine
with Stephanie Balaouras, Kate Pesa, and Peggy Dostie

January 29, 2020

Table Of Contents

Related Research Documents

Forrester Infographic: Build A Better Bot Management Program

New Tech: Bot Management, Q4 2019

Top Cybersecurity Threats In 2020

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Evolving Bad Bot Attacks Require Sophisticated Solutions

The internet is flooded with automated traffic from sources such as search engines, virtual assistants, and chatbots. But running counter to this productive automated traffic are bad bots — software programs that malicious attackers use to automate their attacks.[1] Bot management tools must determine the intent of automated traffic in real time to distinguish between good bots and bad bots.[2] Meanwhile, attackers can easily create, buy, and modify bots, so bot behavior, objectives, and sophistication levels vary greatly:

- **Basic bots simply gather data.** Web scraping has existed for as long as websites have published data; search engine providers and sales-channel partners built bots to simply gather information. But just as quickly, malicious actors built bad bots to steal unprotected, sensitive information. Vulnerability scanning bots, for example, search for known application vulnerabilities to inform future attacks. As companies identify and block bots based on behavior such as quickly changing geographies of static IP addresses or downloading lots of data, attackers continually modify their bots to make them more difficult to detect.
- **More mature bots attack vulnerable applications.** Bots can attack applications to achieve various malicious goals, such as taking over accounts, stealing sensitive customer data, committing fraud, and disrupting commerce. Cyberattackers use bots, either individually or in coordinated botnets, to change source IP addresses or to originate from legitimate customers' devices. One way to detect these bots is to employ challenge scripts to determine whether the client browser is valid, what peripherals are attached, or what kind of battery a mobile phone contains. More advanced responses, such as misdirection, honeypots, sending misleading information to a bot, or leaving bot connections open with no response, increase attackers' costs and help to make bot attacks less economically rewarding.
- **Sophisticated bots can mimic human behavior.** When humans browse websites, they pause, use nonlinear mouse movements, and follow logical flow. Sophisticated bots can mimic these behaviors, evade basic captcha challenges, and even hijack a real customer's browser and tokens. To combat these most sophisticated bots, security pros need a bot management tool that can layer detection methods such as statistical analysis of user behavior, collect biometrics to detect anomalies, and continuously update reputational scoring. A bot management vendor's threat research team will keep abreast of new bot trends and feed that data to the development team and to the market.

Bot Management Evaluation Overview

The Forrester New Wave™ differs from our traditional Forrester Wave™. In the New Wave evaluation, we assess only emerging technologies, and we base our analysis on a 10-criterion survey and a 2-hour briefing with each evaluated vendor. We group the 10 criteria into current offering and strategy (see Figure 1). We also review market presence.

We included 13 vendors in this assessment: Akamai Technologies, Alibaba Cloud, AppsFlyer, Cloudflare, DataDome, Imperva, Instart, Netacea, PerimeterX, Radware, Reblaze, Shape Security, and White Ops (see Figure 2 and see Figure 3). Each of these vendors has:

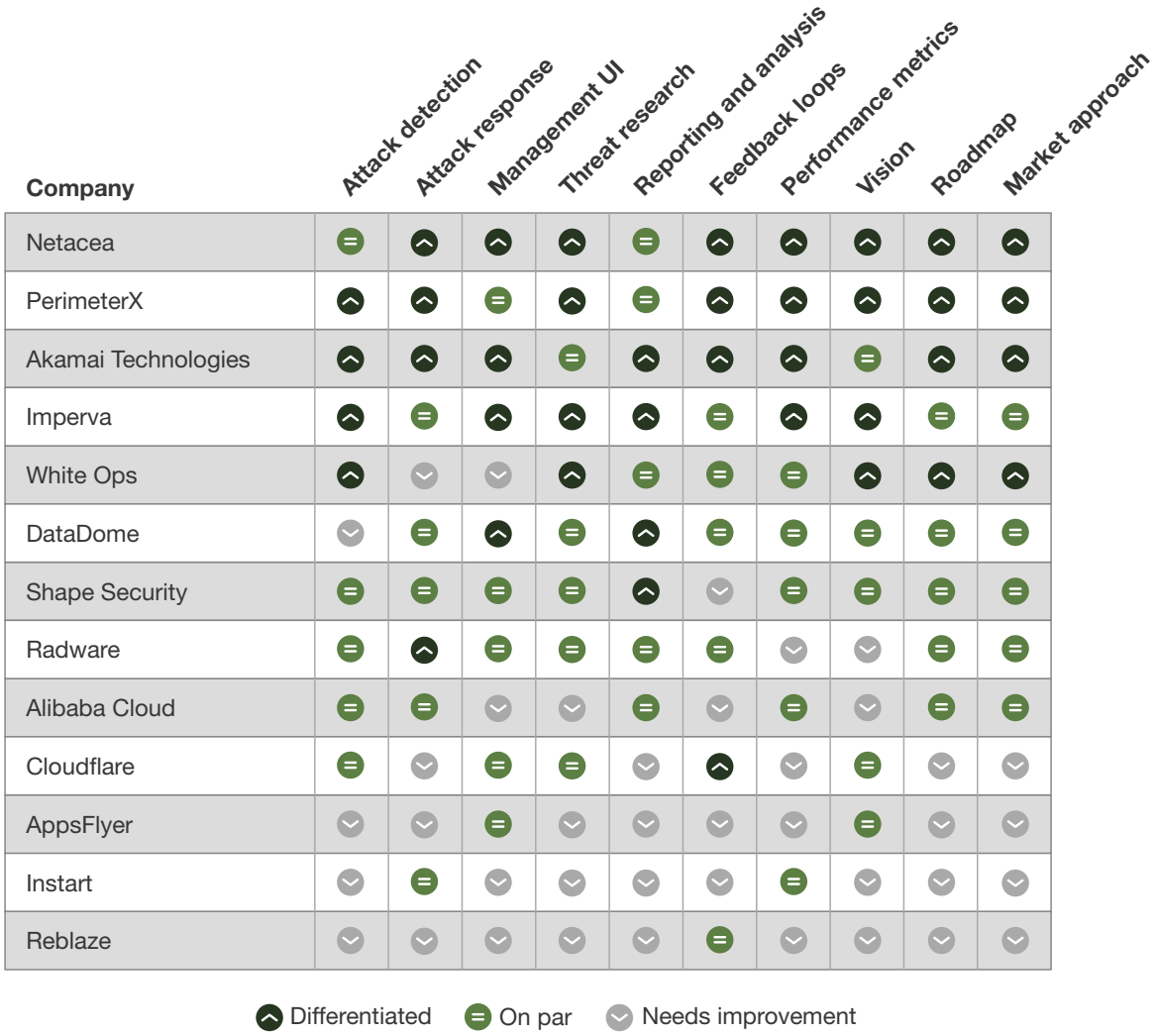
- **A comprehensive, enterprise-class bot management tool.** All vendors in this evaluation offer a range of bot management capabilities suitable for enterprise security pros. We required participating vendors to have products with most of the following capabilities out of the box: ability to analyze intent to identify bad bots, block attacks, incorporate research on new attack methods, and visually represent attack data.
- **Interest from and/or relevance to Forrester clients.** Forrester clients often discuss the participating vendors and products during inquiries and interviews. Alternatively, participating vendors may, in Forrester's judgment, have warranted inclusion because of their technical capabilities and market presence.

FIGURE 1 Assessment Criteria

Criteria	Platform evaluation details
Attack detection	How does the product identify bots for websites, mobile apps, and APIs? How does the product ensure that good customer traffic is not impacted? What different data sources are used in determining intent of a particular user? How does the product detect the most complex attacks?
Attack response	How does the product natively respond to attacks such as alerting, cutting off the user session, denying a specific request, requesting additional identification, slowing down traffic from partners, misdirection, and creating a honey pot?
Management UI	How does the UI enable centralized management for the application and modification of attack detection and response? Are rules customizable and, if so, how flexible is the product in creating rules and does the product make editing, testing, and applying rules easy?
Threat research	How does vendor discover/address new threats and new bot patterns? Are new rules suggested or created for all customers based on these new threats/patterns? What research is published by vendor's research team about evolving bot trends, and is this research published to customers and/or publicly?
Reporting and analysis	Does the product create native dynamic reports and visualizations that effectively communicate the value of the bot management solution to security pros and other concerned parties (including business stakeholders)?
Feedback loops	How does the product enable feedback loops to security operations, marketing professionals, and customer experience professionals? Are the feedback loops enabled via out-of-the-box integrations with applications that support those specific roles such as Marketo or a SIM?
Performance metrics	How does the vendor ensure that the bot management product effectively blocks bad bots, slows good partner traffic, and enables good performance for its clients? What are the vendor's measurements for performance impact? Does the vendor offer performance SLAs?
Vision	How well does the vendor's product vision align with the need for its clients to win, serve, and retain customers?
Roadmap	How strong is the company's execution roadmap?
Market approach	Does the company exhibit successful plans for its go-to-market approach? Can the company show tangible evidence of a successful approach to gaining customers?

FIGURE 2 Forrester New Wave™: Bot Management, Q1 2020

FIGURE 3 Vendor QuickCard Overview



Vendor QuickCards

Forrester evaluated 13 vendors and ranked them against 10 criteria. Here's our take on each.

Netacea: Forrester's Take

Our evaluation found that Netacea (see Figure 4):

- **Leads the pack with robust attack response and dashboarding capabilities.** Netacea offers a full set of responses, including a black hole — an open connection with no response — and a bot state indicator that injects user information into the HTTP header for developers to act upon. Netacea's interactive dashboard allows for easy filtering and drilldown and includes reports on bot intent and scrapers.
- **Still needs to address performance tradeoffs.** Because Netacea's solution is server-side only, its performance is among the slowest of the solutions we reviewed.
- **Is the best fit for companies that need to protect a wide range of traffic.** Netacea's server-side only model allows it to detect and respond to bot traffic coming from web applications, mobile devices, APIs, IoT devices, and any other web-based system.

Netacea Customer Reference Summary

Customers liked Netacea's range of attack responses and easy-to-use UI, but they wanted more options to export reports and more automated error management.

FIGURE 4 Netacea QuickCard

Netacea

Wave position
LEADER

- **Attack detection**
- **Attack response**
- **Management UI**
- **Threat research**
- **Reporting and analysis**
- **Feedback loops**
- **Performance metrics**
- **Vision**
- **Roadmap**
- **Market approach**

Differentiated | On par | Needs improvement

Products evaluated
Bot Management 3.51.9

REFERENCE QUOTES

"We like the various approaches to blocking bot traffic."

"I preferred the UI and level of interaction with Netacea."

"There is limited exportable reporting — we want to be able to export information from the reporting dashboard to CSV."

PerimeterX: Forrester's Take

Our evaluation found that PerimeterX (see Figure 5):

- **Leads the pack with robust machine learning and attack response capabilities.** PerimeterX applies over 120 machine learning algorithms and 165 machine learning models to traffic processing. The company has developed a unique challenge to verify humans without the complexity of traditional captchas.
- **Still needs to improve reporting and out-of-the-box integrations.** PerimeterX has a limited number of OOTB integrations in support of feedback loops. The reporting needs to be more consumable for nontechnical personas like marketing and customer experience.
- **Is the best fit for companies that interact with users across multiple channels.** PerimeterX can track user fingerprints across web, mobile, and API channels, making it a good choice for organizations looking to understand behavior regardless of how the user accesses the site.

PerimeterX Customer Reference Summary

Customers would like continued reporting improvements but strongly praised PerimeterX's responsiveness and the 24x7 support over shared Slack channels.

FIGURE 5 PerimeterX QuickCard

PerimeterX

Wave position
LEADER

- **Attack detection** — Differentiated
- **Attack response** — Differentiated
- **Management UI** — On par
- **Threat research** — Differentiated
- **Reporting and analysis** — On par
- **Feedback loops** — Differentiated
- **Performance metrics** — Differentiated
- **Vision** — Differentiated
- **Roadmap** — Differentiated
- **Market approach** — Differentiated

Differentiated · On par · Needs improvement

Products evaluated
Bot Defender web, mobile, API, analytics

REFERENCE QUOTES

"PerimeterX is one of the most responsive vendors I've worked with. They provide 24x7 support via Slack."

"Was extremely easy to deploy in production and maintain."

"We would like better insight into what rules are being applied to what routes."

Akamai Technologies: Forrester's Take

Our evaluation found that Akamai Technologies (see Figure 6):

- **Leads the pack with robust attack response and reporting capabilities.** Akamai offers a wide range of predefined and configurable attack responses, including tarpit, honeypots, and custom deny. Their Bot Intelligence Console provides information on individual bots and benchmarks bots according to industry and against the entire Akamai customer base. Akamai maintains a directory of about 1,500 legitimate bots and business services.
- **Still needs to offer integrations with marketing and customer experience data sources.** To meet marketing and eCommerce leaders' needs, Akamai must extend its out-of-the-box integrations beyond security use cases.
- **Is the best fit for companies looking to thwart bots at the edge.** Akamai CDN and security customers will find bot management easy to deploy and integrated with their other capabilities.

Akamai Technologies Customer Reference Summary

Customers cautioned that they needed dedicated resources or professional services to use the product effectively, but they praised the new UI and Akamai's strong and improving reporting.

FIGURE 6 Akamai Technologies QuickCard

Akamai Technologies

Wave position
LEADER

- Attack detection
- Attack response
- Management UI
- Threat research
- Reporting and analysis
- Feedback loops
- Performance metrics
- Vision
- Roadmap
- Market approach

Differentiated · On par · Needs improvement

Products evaluated
Bot Manager Premier

REFERENCE QUOTES

"We like its ability to classify and categorize the bot type."

"The depth of analysis we can go into with the newest UI features is a plus."

"The product is highly complex. It requires quite a bit of domain knowledge to effectively manage."

Imperva: Forrester's Take

Our evaluation found that Imperva (see Figure 7):

- **Leads the pack with robust management UI and strong vertical focus.** Imperva allows customers to set machine learning thresholds, path-specific policies, and rule expiration dates. Imperva publishes vertical-specific threat reports that discuss bots' impact on eCommerce, airlines, and ticketing.
- **Still needs stronger feedback loops.** Imperva needs to improve feedback loops to strengthen integrations with SIM tools and tools for marketing and customer experience professionals.
- **Is the best fit for firms that need to protect apps across multiple technology stacks.** Imperva integrates with multiple technology vendors, including AWS, Cloudflare, F5, and NGINX, so customers can protect apps deployed on those platforms.

Imperva Customer Reference Summary

Customers liked the granularity of path rules and the easy-to-manage whitelists and blacklists. However, they would like better analytics about how threats are identified and mitigated and better API protection options.

FIGURE 7 Imperva QuickCard

Imperva

Wave position
LEADER

▲ **Attack detection**	= **Feedback loops**
= **Attack response**	▲ **Performance metrics**
▲ **Management UI**	▲ **Vision**
▲ **Threat research**	= **Roadmap**
▲ **Reporting and analysis**	= **Market approach**

▲ Differentiated = On par ▼ Needs improvement

Products evaluated
Bot Management for web, for API, for mobile apps

REFERENCE QUOTES

"Path rules are granular and user-friendly to configure."

"The vendor relationship is fantastic, and they are very responsive to our requests."

"We'd like to have better API protection options."

White Ops: Forrester's Take

Our evaluation found that White Ops (see Figure 8):

- **Leads the pack with robust threat intelligence, attack detection, and vision.** White Ops helped detect and dismantle the 3ve online fraud operation, and the threat research team publishes new findings monthly. White Ops collects over 2,500 signals per execution, allowing multiple ways to detect malicious traffic.
- **Still needs to improve its attack response and the management UI.** White Ops needs to move its attack response capabilities to an inline versus out-of-band model. The management UI is limited and lacks features such as real-time dashboards.
- **Is the best fit for companies not willing to sacrifice on detection.** Security pros will need to work closely with developers to integrate White Ops into applications and then create integrations with other runtime protection tools to have complete bot management.

White Ops Customer Reference Summary

Customers commended White Ops' threat analysis team and published threat reports but criticized the UI and reporting features.

FIGURE 8 White Ops QuickCard

White Ops

Wave position
STRONG PERFORMER

- **Attack detection** — Differentiated
- **Attack response** — Needs improvement
- **Management UI** — Needs improvement
- **Threat research** — Differentiated
- **Reporting and analysis** — On par
- **Feedback loops** — On par
- **Performance metrics** — On par
- **Vision** — Differentiated
- **Roadmap** — Differentiated
- **Market approach** — Differentiated

Products evaluated
Application Integrity, FraudSensor, MediaGuard

REFERENCE QUOTES

"We like the threat analysis and published reports."

"Compared to other vendors, White Ops is more mature in signal collection in web."

"We'd like to see better visualization and real-time dashboards."

DataDome: Forrester's Take

Our evaluation found that DataDome (see Figure 9):

- **Leads the pack with robust UI and reporting capabilities.** DataDome reports and dashboards detail the type and intent of the attack, providing high-level business context to a variety of stakeholders. Within the management UI, administrators can create customized challenge pages to match the look and feel of their website.
- **Still needs to enhance detection.** DataDome's detection collects fewer signals than top competitors, and first-stage detection focuses primarily on fingerprinting. DataDome needs to extend its machine learning and add it to the first stage of detection.
- **Is the best fit for companies looking for self-service.** DataDome's intuitive UI, monthly customer success reviews, and dedicated Slack channel make it a good choice for those looking to self-manage.

DataDome Customer Reference Summary

DataDome's customers are looking for more detailed information about the source of attacks and detection algorithms but strongly praised the intuitive console and UI.

FIGURE 9 DataDome QuickCard

DataDome

Wave position
STRONG PERFORMER

Attack detection	Feedback loops
Attack response	Performance metrics
Management UI	Vision
Threat research	Roadmap
Reporting and analysis	Market approach

Differentiated · On par · Needs improvement

Products evaluated
Datadome 4.4.8

REFERENCE QUOTES

"The intuitive interface was an important factor to the easy adoption of all frequent and occasional users."

"The intuitive nature makes you feel like you lose control over the underlying actions."

"We'd like to know if an IP address is attacking others."

Shape Security: Forrester's Take

Our evaluation found that Shape Security (see Figure 10):

- **Leads the pack with robust reporting capabilities and vertical threat intelligence.** The management UI includes an interactive dashboard that administrators can click on to zoom in. Shape Security generates weekly executive reports and quarterly threat briefings; it also creates custom threat intelligence packages by industry and hones them further for each customer.
- **Still needs to add out-of-the-box feedback loops.** Shape Security does not offer any out-of-the-box integrations with security operations or other platforms.
- **Is the best fit for companies looking for close interaction with their vendor.** Shape Security provides a high-touch customer experience, with a SOC, technical account manager, strategic account manager, and the Shape Intelligence Center offering regular touchpoints.

Shape Security Customer Reference Summary

Shape Security's customers praised the vendor relationship and the supplied SOC team's responsiveness but noted that the UI was challenging to learn.

FIGURE 10 Shape Security QuickCard

Shape Security

Wave position
CONTENDER

- **Attack detection**
- **Attack response**
- **Management UI**
- **Threat research**
- **Reporting and analysis**
- **Feedback loops**
- **Performance metrics**
- **Vision**
- **Roadmap**
- **Market approach**

Differentiated · On par · Needs improvement

Products evaluated
Enterprise Defense

REFERENCE QUOTES

"The supplied SOC team is highly responsive and able to resolve issues quickly."

"The WebUI is a bit challenging until you become skilled in using it."

"We need multiple parties to support the product."

Radware: Forrester's Take

Our evaluation found that Radware (see Figure 11):

- **Offers strong attack detection and response capabilities.** Radware operates a Global Deception Network, deploying honeypots worldwide and capturing 4,000 unique malicious IPs per hour. Radware users can set responses based on bot maturity — from basic to highly sophisticated — and configure captcha difficulty. Customers can also define custom responses tied to their site's business logic.
- **Still needs to add out-of-the-box feedback loops and published performance SLAs.** Radware offers a number of custom integrations, but they're not available out of the box. SLAs around metrics such as performance latency and false positives were not available.
- **Is the best fit for companies that need a full-stack, cloud-based solution.** Along with bot management, Radware offers cloud-based DDoS protection, WAF, workload protection, and malware protection.

Radware Customer Reference Summary

Customers were critical of Radware's reporting features but appreciated the strong vendor relationship and good customer support.

FIGURE 11 Radware QuickCard

Radware

Wave position
CONTENDER

Attack detection	Feedback loops
Attack response	Performance metrics
Management UI	Vision
Threat research	Roadmap
Reporting and analysis	Market approach

Differentiated · On par · Needs improvement

Products evaluated
Radware Bot Manager 2.2.1

REFERENCE QUOTES

"Strong vendor support that Radware provides has been a big winner for us."

"Dashboard is easy to adopt, no frills, straightforward."

"We'd like additional threat intel features, including analysis of which bots attack which page."

Alibaba Cloud: Forrester's Take

Our evaluation found that Alibaba Cloud (see Figure 12):

- **Offers robust challenge capabilities and published performance metrics.** Threat response options include "slide captcha" (asking the user to perform actions such as clicking or dragging), JavaScript challenges, and the ability to customize captcha and block pages. Alibaba Cloud provides SLAs for service availability and protection accuracy.
- **Still needs to improve threat intelligence and rule creation.** Alibaba Cloud's threat intelligence team is small and doesn't share its analysis in public-facing reports, blogs, or presentations. Creating rules in the management UI is a technical process requiring a lot of expertise.
- **Is the best fit for companies looking for human-assisted protection.** Alibaba Cloud integrates bot management with its SOC to collect and share data with customers.

Alibaba Cloud Customer Reference Summary

Alibaba Cloud's customers highlighted its leadership position in China and ability to serve local customers better than international competitors. Customers noted the challenges of rule creation and wished for more security reports.

FIGURE 12 Alibaba Cloud QuickCard

Alibaba Cloud

Wave position
CHALLENGER

- Attack detection
- Attack response
- Management UI
- Threat research
- Reporting and analysis
- Feedback loops
- Performance metrics
- Vision
- Roadmap
- Market approach

Differentiated | On par | Needs improvement

Products evaluated
Anti-Bot Service 3.0.0.0

REFERENCE QUOTES

"We are able to customize policies according to business characteristics."

"Product rule configuration is relatively difficult."

"We would like more custom policies and more abundant security reports."

Cloudflare: Forrester's Take

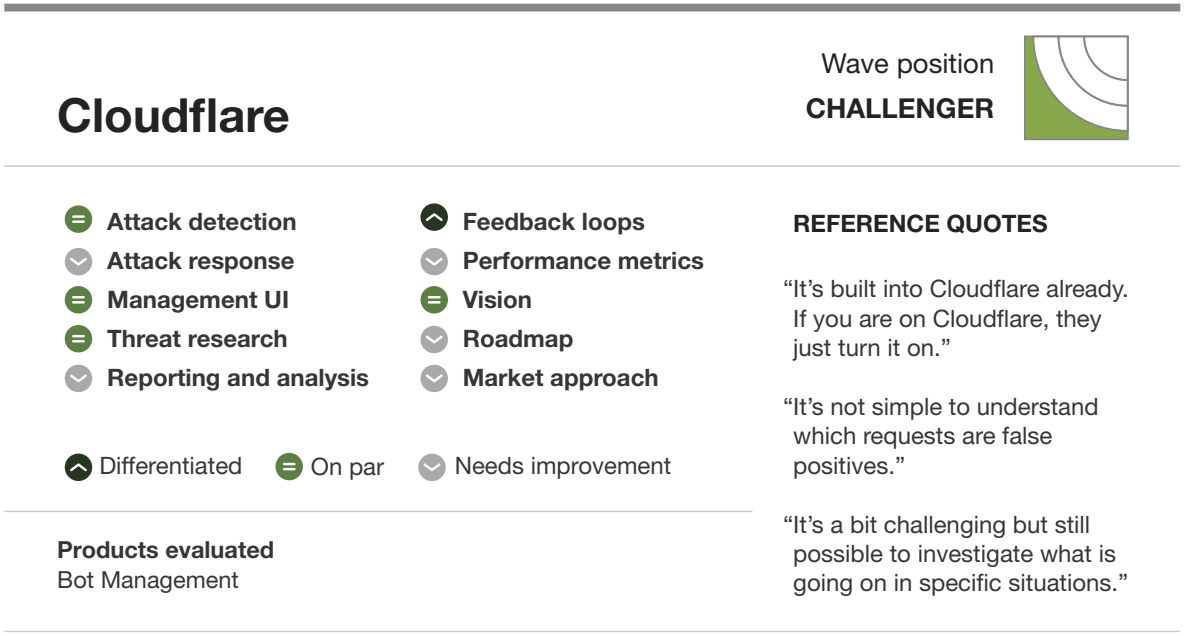
Our evaluation found that Cloudflare (see Figure 13):

- **Leads the pack with robust feedback loops.** Cloudflare leverages its existing security products platform to provide a large number of out-of-the-box integrations, allowing them to funnel data to a wide range of personas.
- **Still needs to extend reporting to other personas and fully support detection for APIs.** OOTB reports are limited to the security operations persona. Cloudflare must develop reports for marketing, eCommerce, and executive personas. Cloudflare's detection capabilities don't include direct API calls, such as machine interactions.
- **Is the best fit for companies that need easy integration with their Cloudflare WAF.** Cloudflare's bot management UI closely ties to its WAF UI. If you're a Cloudflare customer familiar with the WAF interface, adding bot management won't require much of a learning curve.

Cloudflare Customer Reference Summary

Customers found bot management easy to activate if they were already a Cloudflare customer, but they struggled to identify false positives and investigate incidents.

FIGURE 13 Cloudflare QuickCard



AppsFlyer: Forrester's Take

Our evaluation found that AppsFlyer (see Figure 14):

- **Provides robust post-attribution and estimated-savings capabilities.** AppsFlyer continues to analyze traffic and aggregate data after real-time decisions have been made in order to find new patterns and stop fraud that can't be identified in real time. The dashboard includes an estimate of how much money has been saved by blocking fraudulent activity.
- **Still needs to extend beyond mobile and marketing.** AppsFlyer needs to build a credible story for attacks such as credential stuffing and vulnerability scanning. It must also move beyond its mobile roots and provide solutions for web applications and APIs.
- **Is the best fit for companies looking to address mobile marketing fraud.** AppsFlyer remains focused on the mobile tech stack and on marketing fraud use cases, particularly attribution hijacking and fake installs.

AppsFlyer Customer Reference Summary

AppsFlyer gave limited customer references, but the feedback indicated that AppsFlyer would be an easy access point between the customers' data and their media partners. However, the feedback rated attack response poorly and struggled to understand the data the product presented.

FIGURE 14 AppsFlyer QuickCard

AppsFlyer

Wave position
CHALLENGER

- Attack detection
- Attack response
- Management UI
- Threat research
- Reporting and analysis
- Feedback loops
- Performance metrics
- Vision
- Roadmap
- Market approach

Differentiated | On par | Needs improvement

Products evaluated
Protect360 2.0

REFERENCE QUOTES

"We can drill down on the data all the way to the publisher/campaign level."

"They need to reduce false positives in fraud detection."

"Understanding the data can be a bit difficult if you don't know what you're looking for."

Instart: Forrester's Take

Our evaluation found that Instart (see Figure 15):

- **Engages closely with its customers and supports threat intelligence.** Instart conducts regular threat protection check-ins with its customers, communicating best practices and reviewing the latest threats. Instart has globally deployed honeypots to assist with threat intelligence.
- **Still needs to invest in attack response and threat research.** Instart's attack response options are limited to warn or block. The threat research team is small and largely reactive; the team adds new rules when attacked but does not seek out current attacks proactively.
- **Is the best fit for firms seeking an integrated approach to bot protection and Magecart.** Instart's browser attack protection offering is available through the same interface as its bot management offering. Organizations looking to expand beyond bot management and into client-side protections might find Instart's offering convenient.

Instart Customer Reference Summary

While customers were pleased that Instart was easy to integrate with their content delivery network (CDN), they called out feature gaps around the UI, rule creation, and reporting.

FIGURE 15 Instart QuickCard

Instart

Wave position
CHALLENGER

Attack detection	Feedback loops
Attack response	Performance metrics
Management UI	Vision
Threat research	Roadmap
Reporting and analysis	Market approach

Differentiated · On par · Needs improvement

Products evaluated
Bot Management 07.2019

REFERENCE QUOTES

"Integration with our CDN provides a single point of entry and management."

"We've seen heavy false positive identification blocking actual customers."

"The product features are somewhat limited."

Reblaze: Forrester's Take

Our evaluation found that Reblaze (see Figure 16):

- **Offers robust policy definition capabilities.** Reblaze allows administrators to set specific policies per path. Administrators can define policies once and apply them to multiple paths or across multiple applications as needed.
- **Still needs to add attack response.** The only options available to respond to an attack are block, rate limit, and allow. Reblaze does not include common responses such as verification (captcha) and honeypots.
- **Is the best fit for companies that need a tailored solution with minimal training.** Reblaze offers a 4-hour training session to help customers run and maintain the product on their own.

Reblaze Customer Reference Summary

Reblaze customers would like to see more out-of-the-box integrations but appreciated Reblaze's ability to provide custom integrations as needed.

FIGURE 16 Reblaze QuickCard

Reblaze

Wave position
CHALLENGER

- **Attack detection**
- **Attack response**
- **Management UI**
- **Threat research**
- **Reporting and analysis**
- **Feedback loops**
- **Performance metrics**
- **Vision**
- **Roadmap**
- **Market approach**

Differentiated | On par | Needs improvement

Products evaluated
Reblaze 2.12.10

REFERENCE QUOTES

"The product offers detailed data visibility at near real time."

"A more human-friendly interface for custom signatures would have been nicer."

"We'd love to see external integration capabilities integrated into the product's UI, so we can set it up on our own."

Supplemental Material

The Forrester New Wave Methodology

We conducted primary research to develop a list of vendors that met our criteria for the evaluation and definition of this emerging market. We evaluated vendors against 10 criteria, seven of which we based on product functionality and three of which we based on strategy. We also reviewed market presence. We invited the top emerging vendors in this space to participate in an RFP-style demonstration and interviewed customer references. We then ranked the vendors along each of the criteria. We used a summation of the strategy scores to determine placement on the x-axis, a summation of the current offering scores to determine placement on the y-axis, and the market presence score to determine marker size. We designated the top-scoring vendors as Leaders.

Integrity Policy

We conduct all our research, including Forrester New Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] Automated traffic makes up 37.9% of all internet traffic, and bad bots account for over half of that, so security pros need to eliminate the bad traffic while keeping the good. See the Forrester report "New Tech: Bot Management, Q4 2019."

[2] For more information, see the Forrester report "Stop Bad Bots From Killing Customer Experience."

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.