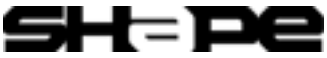


Bot Management Specialists Focus on the Outcome

FEATURING RESEARCH FROM FORRESTER

The Forrester Wave™: Midsize Digital Experience Agencies, Q4 2018

The Predominate Application Defense: Bot Management Specialists

Web scraping, account takeover, fraud, denial-of-service attacks and credential stuffing are all symptoms of the same underlying threat vector: malicious automation. A proper bot management solution must take these on, but also handle the attacker retooling that follows every mitigation.

SPECIALISTS VS. ADD-ONS

Shape Security is proud to be included in **Forrester's New Tech: Bot Management, Q3 2018** report. Report author Amy DeMartine's analysis of the bot management landscape is spot on, and we at Shape thought it would be good to highlight key points of her analysis and also emphasize to buyers what makes our anti-automation solution unique.

"**Bot Management Tools Come in Three Distinct categories**" —Amy DeMartine, Forrester New Tech Report: Bot Management, Q3 2018

DeMartine categorizes bot management vendors into three groups: advertising verification tools, web application firewalls, and bot management **specialists**. We believe that the last is superior with regard to efficacy and outcome.

"...a new breed of specialists focus only on bot management."

As a bot management specialist, Shape Security ticks six of the "high segment functionality" boxes in the *specialist* field of the New Tech criteria grid.

	Specialist Functionality
Detect threats	High
Thwart attacks	High
Improves security	High
Improves customer experience	High
Researches new threats	High
Reduces false positives	High

IN THIS DOCUMENT

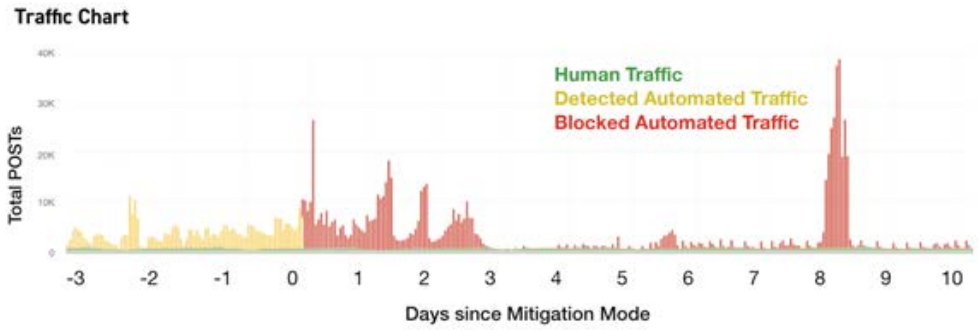
In the report, Shape is categorized as “late stage” maturity level —which is based on four equally weighted criteria:

- Number of dedicated employees
- Breadth of coverage against bots
- Revenue directly attributed to bot management
- Number of bot management customers

Those criteria correlate directly to Shape’s specialization in bot management for the Fortune 500 from 2014 to 2019.

AUTOMATION, ANTI-FRAUD AND RETOOLING

Why do companies choose Shape? Often, it’s the pain. A typical call to Shape comes from a customer dealing with intolerable fraud (3-5% of revenue) or a volume of automated traffic that they can no longer endure. When Shape goes online in front of the customer, within hours we will show that 65-90% of traffic coming at them is automation.



The sample graph above shows Shape flagging all the automated transactions, which for many customers, dwarfs their legitimate transactions (the green bars that are so small they look like a dotted line). In nearly every case, after viewing their graph, prospective customers simply say, “start blocking.” But the story doesn’t end there.

While many attackers get blocked and stay blocked, the sophisticated ones will “retool”—they will change their attack signals to get around detection and then reattach to the host. This retooling can happen within hours at least, or weeks at most; but retooling **always** happens. In the real-world graph above, the attacker took five days to retool, and launched the new campaign with twice the volume. Two days after that, they gave up. Shape’s ongoing value is in detecting the retooling and responding with dynamic countermeasures that target the attacker behind the retooling attempt, not naively playing whack-a-mole against the bots themselves. Other approaches, especially ones that do not include 24/7 teams, woefully fail.

One customer, a director at a Top 5 Canadian bank, put it succinctly: “A group of employees is spending 100% of their time [manually] tuning a solution. We need someone to fight the attackers for us.”

THE SHAPE OF THE FUTURE

Forrester's DeMartine concludes the New Tech report by predicting that bot management will become the predominant application defense, and we agree. If your site is experiencing significant account takeover, web scraping, or credential stuffing, you're really experiencing different symptoms of the same threat vector: automation. By partnering with a bot management specialist, you're treating the cause instead of the symptoms.

"Bot Management Will Become The Predominant Application Defense" —Amy DeMartine, Forrester New Tech Report: Bot Management, Q3 2018

We assert that Shape Security is the premier vendor among bot management specialists, and that our Fortune 100 customer list backs that up. Enjoy the following reprint of Forrester's New Wave report and join the Shape Network to fight automation.

FORRESTER®

The Forrester New Wave™: Bot Management, Q3 2018

The 12 Providers That Matter Most And How They Stack Up

by Amy DeMartine
September 20, 2018

Why Read This Report

In Forrester's evaluation of the emerging bot management market, we identified the 12 most significant providers — Akamai Technologies, Alibaba Cloud, Cloudflare, DataDome, Distil Networks, Oracle Dyn, PerimeterX, Reblaze, ShieldSquare, Stealth Security, Unbotify, 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

Distil Networks, Akamai Technologies, And ShieldSquare Lead The Pack

Forrester's research uncovered a market in which Distil Networks, Akamai Technologies, and ShieldSquare are Leaders; PerimeterX, DataDome, and White Ops are Strong Performers; Alibaba Cloud, Stealth Security, and Oracle Dyn are Contenders; and Reblaze, Cloudflare, and Unbotify are Challengers.

Attack Detection, Attack Response, And Threat Research Are The Biggest Differentiators

Bot management tools differ greatly in their detection methods; many have very limited — if any — automated response capabilities. For many buyers, threat research will be a key decision criterion, as it indicates whether the vendor continually updates its products for the next wave of bot attacks.

The Forrester New Wave™: Bot Management, Q3 2018

The 12 Providers That Matter Most And How They Stack Up

by Amy DeMartine
with Christopher McClean, Kate Pesa, and Peggy Dostie

September 20, 2018

Table Of Contents

Related Research Documents

New Tech: Bot Management, Q3 2018

The State Of Application Security, 2018

Stop Bad Bots From Killing Customer Experience

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 Technical Solutions

The internet is flooded with automated traffic from sources such as search engines, virtual assistants, and chatbots.[1] But running counter to this productive automated traffic are bad bots, software programs that malicious attackers use to automate their attacks.[2] Bot management tools must determine the intent of automated traffic in real time to distinguish between good bots and bad bots.[3] Meanwhile, attackers can easily create, buy, and modify bots, so their 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. As companies identify and block bots based on behavior such as that coming from 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 stealing sensitive customer data, committing fraud, and disrupting commerce. Cyber attackers 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, honey pots, or sending misleading information to a bot, avoid alerting attackers that they should modify their bots to skirt detection.
- **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 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 threat research team will keep abreast of new bot trends.

Bot Management Evaluation Overview

The Forrester New Wave™ differs from our traditional Forrester Wave™. In the New Wave evaluation, we evaluate 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 12 vendors in this assessment: Akamai Technologies, Alibaba Cloud, Cloudflare, DataDome, Distil Networks, Oracle Dyn, PerimeterX, Reblaze, ShieldSquare, Stealth Security, Unbotify, 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.

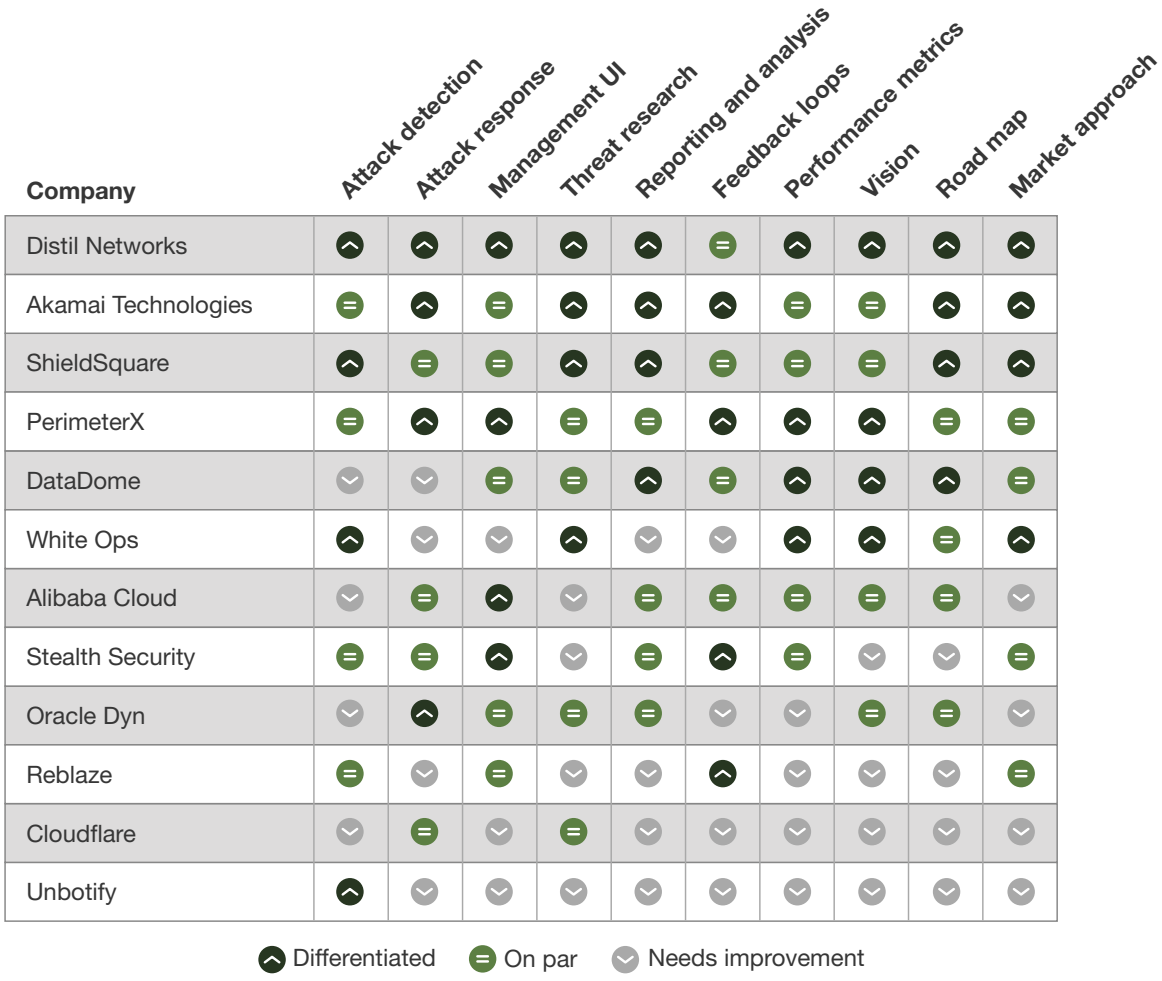
FIGURE 1 Assessment Criteria

Criteria	Platform evaluation details
Attack detection	How does the product identify bots? How is the attack detection differentiating? How does the product ensure that good customer traffic is not impacted? How does the product identify bots for websites and other types of applications such as mobile apps?
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? 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 the vendor discover and address new threats and new bot patterns? What research is published by the research team about evolving bot trends, and is this research published to customers and/or publicly? How many full-time threat research analysts does the company employ?
Reporting and analysis	Does the product create native dynamic reports and visualizations that effectively communicate the value of the bot management solution? Does the product provide out-of-the-box and customizable reports and dashboards on top mitigated attacks, attack response, and types of bots?
Feedback loops	How does the product enable feedback loops to security operations, marketing professionals, and customer experience professionals? Are the feedback loops enabled via integrations with applications that support those specific roles, role-based reporting, APIs, or command line?
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 information is produced for potential and current customers and/or publicly about best practices, trends, and performance impact?
Vision	How well does the vendor's product vision align with the needs of its clients to win, serve, and retain customers? How well does the vision align with current and future trends? Is the company identifying and addressing competitive threats? Does the vision have support and visibility from senior executives?
Road map	How strong is the company's ability to define specific milestones and benchmarks with corresponding resources and capabilities to deliver on its strategy? Does the company have plans to execute on its vision through product enhancements, commercial model enhancements, and partner ecosystem expansion?
Market approach	Can the company show tangible evidence of successfully gaining customers in terms of marketing message, vertical market strategy, geographic strategy, average deal size, number of current customers, and commercial model?

FIGURE 2 Forrester New Wave™: Bot Management, Q3 2018

*Gray marker indicates incomplete vendor participation.

FIGURE 3 Vendor QuickCard Overview



Vendor QuickCards

Forrester evaluated 12 vendors and ranked them against 10 criteria. Here's our take on each.

DISTIL NETWORKS: FORRESTER'S TAKE

Our evaluation found that (see Figure 4):

- **Distil Networks excels with robust detection, response, user interface, and reporting.** Distil Networks boasts 15 different machine learning models to identify bots and over 10 different attack responses. The company is continuing with its data science roots, researching new detection methods.
- **Distil Networks should add feedback loops to security operations and marketing.** Distil could use formal integrations with security and marketing analytical tools to help keep business stakeholders informed about attacks and potential obstruction of good traffic.
- **Distil Networks is best for firms that want flexibility in bot management.** Customers of Distil Networks have granular control over how the tool detects and responds to attacks.

DISTIL NETWORKS CUSTOMER REFERENCE SUMMARY

Customers praised the overall functionality, support, and professional services, but they felt that new functionality could be released faster and that the product needs more-granular reporting.

FIGURE 4 Distil Networks QuickCard

Distil Networks

Wave position
LEADER

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

REFERENCE QUOTES

"Comprehensive bot mitigation solution."

"Customization capabilities and configuration options are amazing. Vendor relationship is extremely good."

Products evaluated
Bot Defense for Web, API, and Mobile Apps

AKAMAI TECHNOLOGIES: FORRESTER'S TAKE

Our evaluation found that (see Figure 5):

- **Akamai Technologies offers robust attack response, threat research, and visibility.** Standout capabilities include the ability to respond to attacks by serving alternative data and deprioritizing bad traffic as well as threat analysis that can tie to financial loss.
- **Akamai Technologies could use API protection and a flexible rule application.** Akamai customers cannot detect bot attacks on APIs. They can assign and modify rules independently across different business units, but all management and some reporting is done by botnet ID and not more granularly.
- **Akamai Technologies is best for companies wanting to thwart bots at the edge.** Companies that already use Akamai for performance or other security protection will find adding bot management easy.

AKAMAI TECHNOLOGIES CUSTOMER REFERENCE SUMMARY

Customers praise Akamai Technologies' ability to respond to bots and product support but would like to see more reports that prove the product's worth to internal teams.

FIGURE 5 Akamai Technologies QuickCard

Akamai Technologies

Wave position
LEADER

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

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"Watching fraud drop was one of the best features we could have seen."

"We can scale and stop attacks with any type of mitigation anywhere in the world."

Products evaluated
Bot Manager Premier 3

SHIELDSQUARE: FORRESTER'S TAKE

Our evaluation found that (see Figure 6):

- **ShieldSquare offers broad attack detection coverage and robust threat research.** ShieldSquare has the ability to protect websites, mobile apps, and APIs from bot attacks. ShieldSquare's threat research team publishes quarterly reports to customers and partners, with topics such as breakdown of attacks by vertical or an anatomy of a sophisticated bot.
- **ShieldSquare still needs to enhance its product's UI and attack response.** Customers can configure attack response, but the product's attack response is limited to blocking, inserting fake data, and captcha. Customized response can be crafted by support only.
- **ShieldSquare is best for firms that require broad application coverage.** ShieldSquare customers can choose API-based implementation or integration with the web server.

SHIELDSQUARE CUSTOMER REFERENCE SUMMARY

Customers credit ShieldSquare as a valuable product, but they claim that it took time after initial configuration to remove all the false positives and that they want attack detection to be faster.

FIGURE 6 ShieldSquare QuickCard

ShieldSquare

Wave position
LEADER

- **Attack detection** (Differentiated)
- **Attack response** (On par)
- **Management UI** (On par)
- **Threat research** (Differentiated)
- **Reporting and analysis** (Differentiated)
- **Feedback loops** (On par)
- **Performance metrics** (On par)
- **Vision** (On par)
- **Road map** (Differentiated)
- **Market approach** (Differentiated)

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"Feature rich, customizable, easy to integrate, cost effective, and very good support."

"The intelligence engine can get better; it works pretty well, and other times it is pretty naive."

Products evaluated
Bot Mitigation Engine 5.4.0 and Dashboard Portal 5.0.0

PERIMETERX: FORRESTER'S TAKE

Our evaluation found that (see Figure 7):

- **PerimeterX offers robust attack response and visibility.** PerimeterX can respond to attacks such as producing fake or stale content, blocking sessions, and creating a honey pot to divert attacks. PerimeterX offers out-of-the-box integrations with different analytics tools such as Big Query, Datadog, and Marketo.
- **PerimeterX still needs to improve its attack detection capabilities.** PerimeterX uses behavioral classification and fingerprinting, but customers complain about false positives.
- **PerimeterX is best for teams wanting to deceive attackers and communicate value.** Security pros can use PerimeterX's out-of-the-box honey pot and misdirection responses to keep attackers guessing. The product also helps users keep colleagues informed.

PERIMETERX CUSTOMER REFERENCE SUMMARY

Customers would like to see better detection capabilities and fewer false positives, but they credit PerimeterX with a flexible product and easy implementation, requiring no infrastructure change.

FIGURE 7 PerimeterX QuickCard

PerimeterX

Wave position
STRONG PERFORMER

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

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"We like the simple integration and SDK support for our mobile apps."

"The number of false positives is higher than we would have liked."

Products evaluated
Bot Defender Web, Mobile, API

DATADOME: FORRESTER'S TAKE

Our evaluation found that (see Figure 8):

› **DataDome offers robust visibility and performance tracking.** Best practices of DataDome's customers are published on its website. DataDome produces summary reports describing the attacking bots, with drill-down details and analysis of good, commercial, and bad traffic.

› **DataDome needs to improve its attack detection and response.** DataDome's attack detection capabilities use a combination of fingerprinting and validation challenges, and its primary attack response is blocking.

› **DataDome is the best fit for companies that require speedy detection and response.** DataDome optimizes using a combination of synchronous and asynchronous detection.

DATADOME CUSTOMER REFERENCE SUMMARY

Customers were excited about DataDome's ease of use and deployment; however, they wished it had better whitelisting and automatic blacklisting of known threats.

FIGURE 8 DataDome QuickCard

DataDome

Wave position
STRONG PERFORMER

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

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"Easy to deploy. No overhead."

"We have seen much-improved website availability and much more stable response time."

Products evaluated
DataDome 3.0

WHITE OPS: FORRESTER'S TAKE

Our evaluation found that (see Figure 9):

- **White Ops features robust attack detection, threat research, and vision.** White Ops discovered, disclosed, and helped dismantle the organization behind the MethBot, living up to the company's mission to root out the cause of bad bots. Attack detection capabilities include continuously tracking mathematical confidence scores to distinguish bad bots.
- **White Ops needs to improve its attack response and expand beyond ad fraud.** White Ops started by detecting ad fraud but must move past its roots to address a wider range of bad bots and include automated attack response.
- **White Ops works well 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

White Ops did not participate in this evaluation and did not provide customer references.

FIGURE 9 White Ops QuickCard

White Ops

Wave position
STRONG PERFORMER

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

REFERENCE QUOTES

White Ops did not participate in this evaluation and did not provide customer references.

Differentiated On par Needs improvement

Products evaluated
FraudSensor, MediaGuard

ALIBABA CLOUD: FORRESTER'S TAKE

Our evaluation found that (see Figure 10):

- **Alibaba Cloud has a robust management UI.** Alibaba Cloud has two bot management modules for its UI. Customers can modify detection and response rules and can set conditions that are specific to the business or process.
- **Alibaba Cloud should build better threat research and attack detection.** Alibaba Cloud has a relatively small team dedicated to researching and developing bot management. Attack detection capabilities are limited to blocking and identity challenges.
- **Alibaba Cloud is best for firms that want human-assisted protection.** Alibaba Cloud provides expert support and analysis of traffic in addition to its automatic detection and response capabilities.

ALIBABA CLOUD CUSTOMER REFERENCE SUMMARY

Customers noted the accuracy of Alibaba Cloud's bot detection as well as the quality of customer support; however, they wished the product had broader detection, response, and user training.

FIGURE 10 Alibaba Cloud QuickCard

Alibaba Cloud

Wave position
CONTENDER

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

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"We chose Alibaba Cloud because of accuracy in tracking malicious traffic and immediate response."

"There is no proper training or instruction."

Products evaluated
Web Application Firewall, Anti-Bot Service 3.6

STEALTH SECURITY: FORRESTER'S TAKE

Our evaluation found that (see Figure 11):

- **Stealth Security offers a robust management UI and feedback loops.** Stealth Security customers can set response options per application. The product offers integrations with Splunk and ArcSight to help keep security operations teams informed of bot attacks.
- **Stealth Security should improve its threat research.** Stealth Security has limited threat research capabilities, focusing just on following current attack patterns.
- **Stealth Security is best for firms that want granular response control.** Stealth Security customers can create custom rules, such as monitoring the behavior of a high-profile customer and tracking whether someone uses their login, but the changes require a high degree of expertise.

STEALTH SECURITY CUSTOMER REFERENCE SUMMARY

Customers like the ability to customize rules with Stealth Security, but they note that there is a learning curve on rule setup that can easily lead to mistakes that adversely affect customers.

FIGURE 11 Stealth Security QuickCard

Stealth Security

Wave position
CONTENDER

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

Differentiated On par Needs improvement

REFERENCE QUOTES

"We were able to demonstrate success in detection and analytics of bad traffic in our environment."

"Easy to make mistakes that affect legitimate traffic."

Products evaluated
Stealth Detector 2.4 and Mitigator 1.6

ORACLE DYN: FORRESTER'S TAKE

Our evaluation found that (see Figure 12):

- **Oracle Dyn has robust attack response.** Oracle Dyn can block bot attacks with a configurable error code, mitigate attacks by slowing down certain traffic for specific periods of time, and replace a website page with another. The product can respond to attacks based on IP address or session.
- **Oracle Dyn should improve performance metrics and feedback loops.** Oracle Dyn only allows customers to provide feedback to support with methods such as slack, and it does not publicly publish best practices or product performance metrics.
- **Oracle Dyn is best for firms looking to single source with Oracle.** Oracle Dyn will be especially appealing to Oracle Cloud Infrastructure (OCI) customers.

ORACLE DYN CUSTOMER REFERENCE SUMMARY

Customers confirmed they are satisfied with Oracle Dyn's detection, response, and integration with Oracle Dyn WAF, but they're looking for enhanced visibility.

FIGURE 12 Oracle Dyn QuickCard

Oracle Dyn

Wave position
CONTENDER

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

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"We like the product features and the detection and response capabilities."

"We'd like to see improved logging, reporting, and integrations."

Products evaluated
Bot Manager

REBLAZE: FORRESTER'S TAKE

Our evaluation found that (see Figure 13):

- **Reblaze's bot management is part of an integrated security solution.** Reblaze offers each customer strong privacy controls with a single-tenant CDN. Every minute, Reblaze re-analyzes web traffic, looking at fingerprints and using validation challenges to identify bots.
- **Reblaze needs to improve its attack response and threat research.** Blocking bots is the product's only attack response. Because Reblaze is a SaaS bot management solution, active threats against one customer will generate a rule that protects all.
- **Reblaze is best for teams looking for broad security protection.** Bot management is one of the security solutions Reblaze sells in addition to WAF and DDoS. Reblaze offers out-of-the-box SIM integration to keep security operations pros informed about bot attacks.

REBLAZE CUSTOMER REFERENCE SUMMARY

Customers like Reblaze's all-in-one solution but noted that product documentation lagged behind development, that it took time to learn the product, and that customized reporting is a weakness.

FIGURE 13 Reblaze QuickCard

Reblaze

Wave position
CHALLENGER

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

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"Our team can easily and quickly navigate around millions of daily events."

"It takes some time to become fully proficient with the various capabilities."

Products evaluated
Reblaze 2.10.2

CLOUDFLARE: FORRESTER'S TAKE

Our evaluation found that (see Figure 14):

- **Cloudflare offers security protection for all its customers.** Cloudflare includes its bot management capabilities as a standard offering. The company has a relatively large threat intelligence team, but none are specifically dedicated to bot research.
- **Cloudflare must differentiate bot management functionality.** Cloudflare's attack response is limited to blocking, identity challenge with captcha, and JavaScript challenge. Attack detection is performed by fingerprinting and validation challenges. Cloudflare cannot delay search engines from over-crawling websites and cannot protect mobile apps.
- **Cloudflare is best for firms that don't mind tinkering.** Cloudflare offers a configuration environment called Workers, which enables other advanced response techniques.

CLOUDFLARE CUSTOMER REFERENCE SUMMARY

Customers like Cloudflare's ease of implementation and combination of CDN and security features, but they noted that they had to implement some features sitewide, which made them difficult to test.

FIGURE 14 Cloudflare QuickCard

Cloudflare

Wave position
CHALLENGER

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

Differentiated · On par · Needs improvement

REFERENCE QUOTES

"Cloudflare is an all-in-one CDN and security protection solution that can prevent any bad traffic from hitting our servers."

"Cloudflare is constantly adding new features."

Products evaluated
WAF, Rate Limiting, Workers, Access, Threat Intelligence

UNBOTIFY: FORRESTER'S TAKE

Our evaluation found that (see Figure 15):

- **Unbotify offers differentiating attack detection.** Unbotify performs biometric tracing and machine learning to distinguish humans from bots. The company offers detection tools for desktop, web, and mobile apps.
- **Unbotify should improve its attack response and user interface.** Unbotify offers a simple dashboard, but to keep up with the market, it needs to include built-in attack response options and a UI that can create and modify responses based on detection.
- **Unbotify is the best fit for companies that can integrate other attack response tools.** Security pros will need to work closely with developers to integrate Unbotify into applications and then integration with other runtime protection tools for comprehensive bot management.

UNBOTIFY CUSTOMER REFERENCE SUMMARY

Forrester was unable to contact customer references for Unbotify during the research period for this report.

FIGURE 15 Unbotify QuickCard

Unbotify

Wave position
CHALLENGER

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

REFERENCE QUOTES

Forrester was unable to contact customer references for Unbotify during the research period for this report.

Differentiated | On par | Needs improvement

Products evaluated
Desktop and Website, Mobile Native Bot Management

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

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 is now over 50% of internet traffic and includes automated traffic with both good and bad intent. Source: "Bot traffic is taking over the Web," Image & Data Manager, December 15, 2017 (https://idm.net.au/article/0011797-bot-traffic-taking-over-web).

[2] A recent study found that all public websites with a login are actively attacked by bad bots. Source: Alison DeNisco Rayome, "Bad bots detected on 100% of web login pages, here's how to protect your business," TechRepublic, May 1, 2018 (https://www.techrepublic.com/article/bad-bots-detected-on-100-of-web-login-pages-heres-how-to-protect-your-business/).

[3] For more information on how bots — both good and bad — are adversely affecting your customers, see the Forrester report "Stop Bad Bots From Killing Customer Experience."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

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

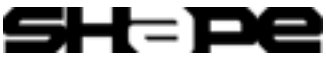
Technology Industry Professionals

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.

143516



ABOUT SHAPE, AND WHAT CUSTOMERS SAY

Shape protects the online accounts of five of the top ten US banks, including **Wells Fargo, Inc.** Rohan Amin, the CISO of JPMC, awarded Shape **JPMC's Hall of Innovation Award** and said, *"We were impressed by Shape's innovative approach to help enable a high-security, low-friction user experience… and we appreciate our partnership."*

Shape protects the loyalty programs of three of the top five hotels, and the miles of four of the top five airlines. **JetBlue's** CTO, Eash Sundaram, said, *"The safety and security of our customers, in all aspects, is JetBlue's top priority. Shape has proven to be a very impactful partner for us as we protect our customers online."*

At **Starbucks**, Mike Hughes, the director of Information Security, says "At its core, Shape is solving is a sophisticated, data problem that couldn't be addressed by legacy approaches." And **Loblaw**, a top Canadian seller, is one of many retailers who choose Shape to protect over 100 million e-commerce accounts.