The Forrester Wave™: External Threat Intelligence Services, Q1 2021

The 12 Providers That Matter Most And How They Stack Up

by Brian Kime and Elsa Pikulik

March 23, 2021

Why Read This Report

In our 26-criterion evaluation of external threat intelligence services providers, we identified the 12 most significant ones — CrowdStrike, Digital Shadows, FireEye, Flashpoint, Group-IB, IBM, Intel 471, IntSights, Kaspersky, Recorded Future, RiskIQ, and ZeroFOX — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right ones for their needs.

The Forrester Wave™: External Threat Intelligence Services, Q1 2021

The 12 Providers That Matter Most And How They Stack Up

by Brian Kime and Elsa Pikulik
with Merritt Maxim, Shannon Fish, and Peggy Dostie
March 23, 2021

Effective Cyberdefense Requires External Threat Intelligence Services

S&R pros are realizing the benefits of threat intelligence and now require more than indicators of compromise (IOC) feeds and phishing alerts. Since the release of The Forrester New Wave™: External Threat Intelligence Services, Q3 2018, this market has continued to grow as S&R pros look to external threat intelligence services to enhance existing cyberdefenses. As the number and sophistication of cyberthreats increase and IT environments become more complex, S&R pros seek out threat intelligence providers that have just the right visibility into threats most relevant to their organization and industry. In fact, according to Forrester Analytics' Business Technographics® survey data, global security decision-makers now subscribe to an average of 7.5 commercial external threat intelligence services, which is up from an average of 4.2 vendors in 2018. As in 2018, this research is not intended to help S&R pros procure only one vendor. Based on your unique threat landscape, and after exhausting all of your internal security telemetry, use this Forrester Wave to select the vendors with the most advanced capabilities in each of the core capabilities to fill out your organization's intelligence collection strategy.

As a result of these trends, customers should look for external threat intelligence services providers that:

- **Have primary source intelligence.** It's impossible to thoroughly track cyberthreats and the campaigns they undertake without access to primary source intelligence — direct observations via incident response engagements and access to the sensors that observe threat activity (e.g., managed/monitored security controls). Every organization has its own primary source intelligence — its own security telemetry. Enrich your own primary source intelligence with that of vendors rich in their own primary source intelligence.
- **Specialize in protecting brand reputation.** Regardless of enterprise size, every organization has a brand and customers to protect. Seek out superior brand threat intelligence vendors with a managed service and an organic takedown service.

FORRESTER®

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

- **Excel in vulnerability intelligence.** It's no longer acceptable to simply pass along National Vulnerability Database information to customers. The Common Vulnerability Scoring System (CVSS) is not a risk metric. Business process owners are exhausted responding to every "critical" vulnerability. Superior vulnerability intelligence uses both primary and secondary source intelligence to focus solely on helping asset owners reduce the risk of vulnerability exploitation and application downtime.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our reports on threat intelligence.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: External Threat Intelligence Services, Q1 2021

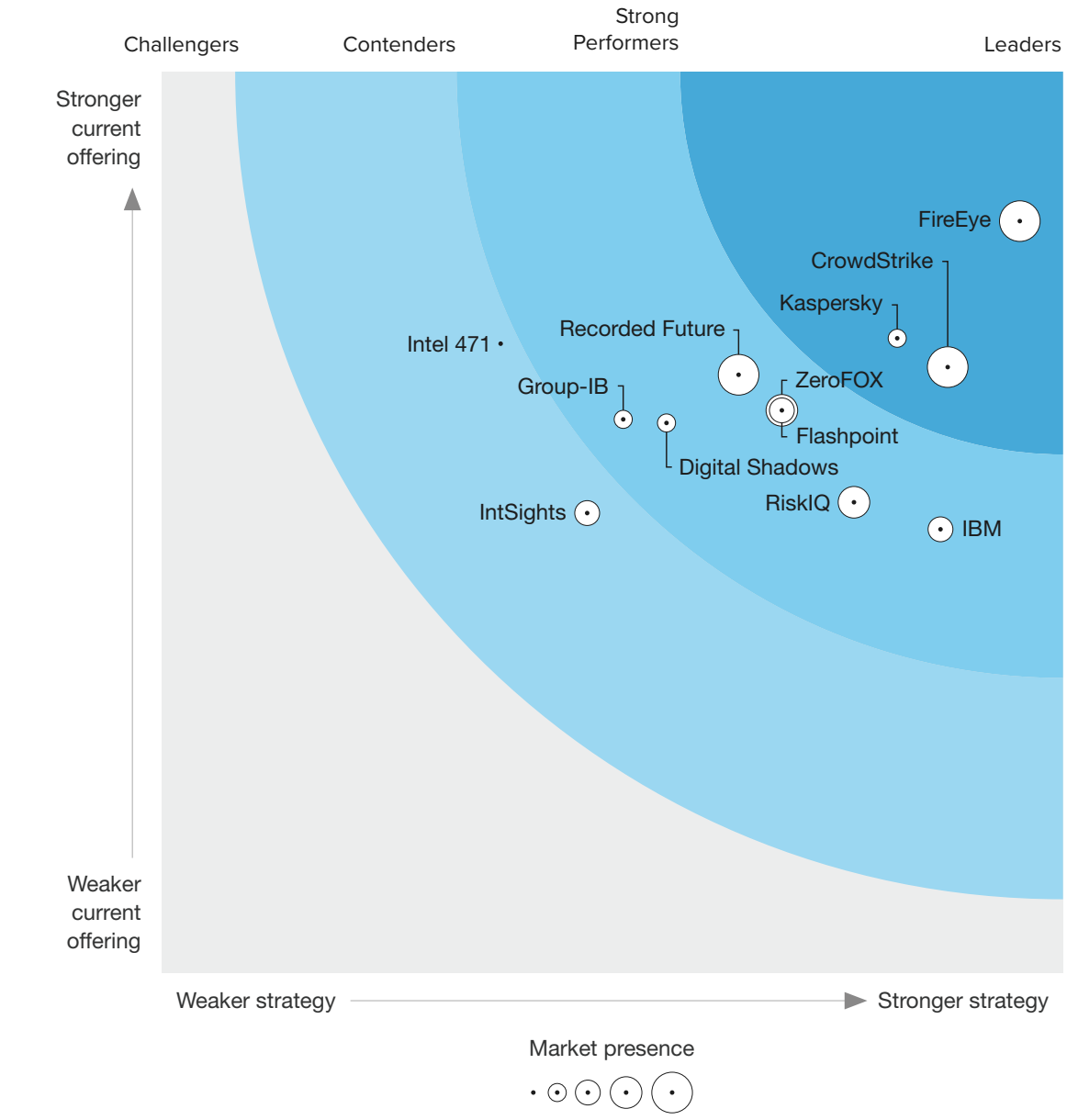

FIGURE 2 Forrester Wave™: External Threat Intelligence Services Scorecard, Q1 2021

	Forrester's weighting	CrowdStrike	Digital Shadows	FireEye	Flashpoint	Group-IB	IBM
Current offering	50%	3.36	3.05	4.17	3.12	3.07	2.46
Intelligence requirements	12%	5.00	3.00	5.00	3.00	1.00	3.80
Raw intelligence collection	5%	4.24	3.00	4.20	3.44	2.56	4.20
Intelligence analysis	12%	5.00	3.00	5.00	3.00	3.00	3.00
Dissemination	5%	5.00	3.00	5.00	5.00	3.00	3.00
Client and stakeholder feedback	5%	4.00	4.00	4.00	3.00	3.00	3.00
Requests for information	10%	1.00	1.00	3.00	3.00	5.00	3.00
Cyber threat intelligence	17%	5.00	3.00	5.00	3.00	3.00	3.90
Brand threat intelligence	17%	2.20	4.20	1.80	3.00	3.80	0.00
Vulnerability intelligence	17%	1.00	3.00	5.00	3.00	3.00	1.00
Strategy	50%	4.36	2.80	4.76	3.44	2.56	4.32
Product vision	22%	5.00	3.00	5.00	3.00	3.00	3.00
Innovation roadmap	22%	3.00	3.00	5.00	5.00	1.00	5.00
Market approach	10%	3.00	3.00	5.00	5.00	3.00	5.00
Supporting products and services	24%	5.00	3.00	5.00	3.00	3.00	5.00
Commercial model	12%	5.00	3.00	3.00	3.00	3.00	3.00
Strategic partners	10%	5.00	1.00	5.00	1.00	3.00	5.00
Market presence	0%	5.00	2.00	4.50	2.50	2.00	3.00
Number of clients	50%	5.00	2.00	4.00	2.00	3.00	2.00
Overall service revenue	50%	5.00	2.00	5.00	3.00	1.00	4.00

All scores are based on a scale of 0 (weak) to 5 (strong).

FIGURE 2 Forrester Wave™: External Threat Intelligence Services Scorecard, Q1 2021 (Cont.)

	Forrester's weighting	Intel 471	IntSights	Kaspersky	Recorded Future	RiskIQ	ZeroFOX
Current offering	50%	3.49	2.55	3.52	3.32	2.61	3.12
Intelligence requirements	12%	5.00	1.80	3.00	3.80	3.00	3.00
Raw intelligence collection	5%	3.08	2.24	3.80	3.36	2.92	2.56
Intelligence analysis	12%	3.00	2.00	5.00	3.00	3.00	3.00
Dissemination	5%	3.00	3.00	5.00	5.00	3.00	3.00
Client and stakeholder feedback	5%	4.00	4.00	3.00	5.00	3.00	3.00
Requests for information	10%	1.00	1.00	1.00	1.00	1.00	1.00
Cyber threat intelligence	17%	4.10	3.00	5.00	3.00	1.90	3.00
Brand threat intelligence	17%	2.20	3.00	3.00	2.20	5.00	5.00
Vulnerability intelligence	17%	5.00	3.00	3.00	5.00	1.00	3.00
Strategy	50%	1.88	2.36	4.08	3.20	3.84	3.44
Product vision	22%	3.00	1.00	3.00	3.00	3.00	1.00
Innovation roadmap	22%	1.00	3.00	5.00	3.00	5.00	5.00
Market approach	10%	3.00	3.00	5.00	5.00	5.00	3.00
Supporting products and services	24%	1.00	3.00	3.00	3.00	3.00	3.00
Commercial model	12%	3.00	3.00	5.00	3.00	3.00	5.00
Strategic partners	10%	1.00	1.00	5.00	3.00	5.00	5.00
Market presence	0%	1.00	2.50	1.50	4.50	3.50	4.00
Number of clients	50%	1.00	3.00	1.00	4.00	3.00	4.00
Overall service revenue	50%	1.00	2.00	2.00	5.00	4.00	4.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Vendor Offerings

Forrester included 12 vendors in this assessment: CrowdStrike, Digital Shadows, FireEye, Flashpoint, Group-IB, IBM, Intel 471, IntSights, Kaspersky, Recorded Future, RiskIQ, and ZeroFOX (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated
CrowdStrike	Falcon X
Digital Shadows	Digital Shadows SearchLight 5.35
FireEye	FireEye Threat Intelligence & Mandiant Advantage Threat Intelligence Suite
Flashpoint	Flashpoint Intelligence Platform
Group-IB	Group-IB Threat Intelligence and Attribution
IBM	IBM Threat Intelligence Insights on Cloud Pak for Security
Intel 471	Cybercrime Intelligence
IntSights	IntSights External Threat Protection Suite
Kaspersky	Kaspersky Threat Intelligence
Recorded Future	Recorded Future Security Intelligence Platform
RiskIQ	RiskIQ Illuminate
ZeroFOX	ZeroFOX Digital Risk Protection Platform

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **FireEye offers some of the best threat intelligence.** Founded in 2004, FireEye-Mandiant's intelligence team is based in northern Virginia. The vendor plans to: 1) increase intelligence collection via its controls-agnostic Managed Defense service; 2) invest to combine delivery of threat intelligence, security validation, and incident response; and 3) leverage data to help organizations quickly understand threats they face and take action.

  FireEye-Mandiant's strength in threat intelligence is in large part due to the reputation and visibility provided via the company's robust incident response consultancy, security controls business, and managed security services. The visibility gained from those supporting services is ahead of the pack. Customer references expressed high satisfaction with the new Mandiant Advantage portal. Their vulnerability intelligence subscription sets the bar for the category. The vendor also maintains

one of the few cyber/physical threat intelligence capabilities. Security buyers in North America, Europe, the Middle East, and Asia with operational technology environments and state-nexus threat concerns should strongly consider FireEye for their external threat intelligence service.

- **CrowdStrike began as a threat intelligence vendor and continues to stay out front.** Founded in 2011 as a cloud-native security company, the Falcon X cyber threat intelligence platform drives CrowdStrike's business. The vendor plans to: 1) expand cloud, mobile, and vulnerability intelligence practices; 2) deliver intel workbench serving tactical, operational, and strategic stakeholders; and 3) continue investment in digital reconnaissance.

  Reference customers using CrowdStrike's Falcon X Elite tier were extremely impressed with the level of service provided by the dedicated intelligence analysts. The quality of technical intelligence and expertise of the dedicated analysts were noted by multiple customer references. One customer specifically felt like CrowdStrike was a "true partner of their security organization" and "the [dedicated analyst] is an extension of our team." CrowdStrike is strong globally except for LATAM. Buyers should consider CrowdStrike even if they're not using the vendor's EDR tools, especially if state-nexus threats are in their landscape.

- **Kaspersky plans to integrate existing threat intel solutions into a unified platform.** Kaspersky is a global cybersecurity company headquartered in Moscow. The vendor plans to: 1) increase the number of third-party integrations and improve existing ones; 2) develop a master search to query for information throughout all Kaspersky threat intelligence services; and 3) integrate several existing Kaspersky threat intelligence products into a single, more powerful research platform.

  Kaspersky is a front-runner for intelligence quality and requests for information (RFIs). Kaspersky was behind other vendors in the evaluation for brand threat intelligence use cases. Reference customers were very satisfied with Kaspersky's information quality as well as its process to help clients measure efficiency and results. Kaspersky is relevant for vendors of any size, especially those based in EMEA or APAC.

Strong Performers

- **IBM offers unparalleled scale in threat intelligence.** The service reviewed is X-Force Threat Intelligence. The vendor plans to: 1) add a brand threat intelligence and takedown service; 2) enhance features such as "Am I Affected" and prioritized X-Force threat score; and 3) build out its third-party ecosystem, including embedding a threat intelligence platform (TIP).

  IBM's partnership with the Quad9 DNS service is differentiating and helps give IBM its exceptional visibility into cyberthreat activity. One customer reference told us that "IBM has the lowest false positive rate of any of their significant providers over the past three years." Another said, "IBM has a lot of strengths; those strengths have to do with the accuracy and specificity of their data." With its incredible global visibility and exceptional technical intelligence, IBM has superior capabilities

to track threat actors and detect their campaigns. Its brand threat intelligence and vulnerability intelligence capabilities are not as strong as other vendors. Any buyer in the world seeking a premier source of technical intelligence should consider IBM.

- **ZeroFOX shines in the brand protection space.** Based in Baltimore, ZeroFOX is one of the largest vendors in this evaluation, in number of external threat intelligence services customers and in annual revenue. ZeroFOX's October 2020 acquisition of Cyveillance gives its customers access to a larger pool of threat data and intelligence. The vendor plans to: 1) focus on AI-driven intelligence; 2) improve unified data architecture; and 3) develop automated remediation and disruption.

  ZeroFOX is best in class for brand threat intelligence use cases and takedown service. Reference customers report extremely high satisfaction with brand threat intelligence. A reference customer did note difficulties with content not in English. Additionally, technical intelligence has not been a particular focus for ZeroFOX, but the recent acquisition of Cyveillance adds significant talent and data to address these weaknesses. Reference customers also noted the vendor's emphasis on being data driven and on being proactive in asking for feedback. ZeroFOX is relevant for clients of any size looking for brand protection use cases.

- **Recorded Future offers unparalleled open source intel in a usable platform.** Based in Somerville, Mass., Recorded Future offers clients proactive and predictive intelligence. The vendor plans to: 1) add modules focused on new intelligence use cases; 2) optimize data for use case workflows; and 3) add data sources and improve analytics.

  Recorded Future is best in class for open source intelligence and has good technical and human intelligence, making these a threat intelligence "multitool." Risk rules power intelligence cards on IOCs and help customers make smarter decisions. Reference customers told us they desired more-robust reporting for Recorded Future's vulnerability intelligence. Customers were universally impressed with the breadth and depth of the intelligence provided by Recorded Future as well as the customer support. Recorded Future is ideal for organizations looking to get comprehensive intelligence from an intuitive platform.

- **RiskIQ offers extensive tracking of both threat and friendly infrastructure.** RiskIQ is based in San Francisco. The vendor plans to: 1) launch telemetry for network traffic; 2) automate analyst insights; and 3) improve third-party integrations.

  Reference customers reported being satisfied with RiskIQ's open source technical intelligence capabilities. The vendor excels in uncovering infrastructure masquerading as a brand and, via its managed service, has a robust takedown service, relieving clients of adding headcount. Its PassiveTotal product is exceptional at tracking threat infrastructure. A weak area for RiskIQ is its analytical tradecraft capability. Customers also told us that RiskIQ was not proactive in eliciting feedback from customers. RiskIQ is best for customers that prioritize open source technical intelligence, especially those based in North America.

- **Flashpoint excels in uncovering fraud/stolen data in underground criminal communities.** Flashpoint was founded in 2010 and is based in New York City. The vendor plans to: 1) expand development of analytics and automation; 2) launch and expand third-party integrations and OEM relationships; and 3) build on its account takeover and card fraud offerings.

  Flashpoint continues to excel at cyber-enabled human intelligence. Its infrastructure and training to support intelligence collection of underground criminal forums allows the vendor to perform additional services for clients that differentiates it from other vendors. Flashpoint's Compromised Credential Monitoring solution is one of the premier capabilities for quickly reducing the risk of stolen credential reusage. The Wiki-style threat profiles in its portal are differentiating. Reference customers highlighted the vendor's lack of coverage of state-nexus threats. Buyers seeking to combat fraud or gain visibility into underground criminal forums should consider Flashpoint.

- **Digital Shadows helps smaller security teams achieve success with threat intelligence**. Digital Shadows has headquarters in both London and San Francisco, with additional presence in Singapore. The vendor plans to: 1) grow via current and new partners in the next few years; 2) automate mundane tasks to support large and small security operations teams; and 3) expand capabilities in the SearchLight platform into third-party threat intelligence.

  Digital Shadows is one of the premier services in brand threat intelligence. A reference customer told us, "Digital Shadows excels in highlighting things we should be looking for externally." Comparing Digital Shadows to a similar vendor, another customer reference told us, "For the cost and breadth of threat intelligence, Digital Shadows was the clear winner for us." Digital Shadows is a very talented intelligence service that is a strong fit for any resource-strained security teams in North America, Europe, and Asia.

- **Group-IB differentiates with unlimited RFIs and takedowns of abusive content.** Group-IB was founded in 2003 in Moscow as an incident response and cyberinvestigation company and has since built a robust threat intelligence service. It's now headquartered in Singapore, with a European headquarters in Amsterdam. The vendor plans to: 1) build more analytical and hunting tools into its system; 2) involve clients in research activity via gamification and collaboration; and 3) expand its business via MSSP partnerships.

  The firm offers clients unlimited takedowns of phishing sites regardless of who detected the brand abuse. Another differentiator is the vendor's policy of unlimited RFIs. Customer references cited difficulty working with the vendor's API and too many false positives. Buyers at financial service firms in Europe, the Middle East, and Asia should consider Group-IB for their specialization in payment card fraud and relationships with international law enforcement groups.

Contenders

- **Intel 471 is focused on cybercrime intel and excels at cyber-enabled human intelligence.** Intel 471 was founded in 2014; its external threat intelligence service, Cybercrime Intelligence, is its primary product. The vendor plans to: 1) expand to SMBs by offering a more-affordable service tailored to their needs; 2) increase the number of third-party integrations; and 3) pursue mergers and acquisitions to boost data and intelligence capabilities.

  Intel 471 excels at eliciting customer intelligence requirements via a thorough survey and ranking process. It also comes through with a detailed collection plan that focuses on clients' top priorities and is easy to understand. Open source intelligence is not a focus of Intel 471; therefore, this criterion is lacking compared to other vendors in the evaluation. Additionally, Intel 471 does not offer its own takedown service. Customers appreciated the focus on cybercriminals and malware and stated that the vendor was "top tier in terms of satisfaction and delivery." Intel 471 is ideal for customers that are looking for intelligence on financially motivated threat actors and appreciate having a vendor guide them on defining and prioritizing their intelligence requirements.

- **IntSights invests in cloud intelligence for the masses.** IntSights was founded in 2015 and is based in New York, with seven local offices on three continents. The vendor plans to: 1) build out its cloud security intelligence capabilities; 2) build out its botnet intelligence capabilities; and 3) develop its strategic insights dashboard.

  IntSights can cater to different stakeholders within the organization — including compliance officers — by generating reports with multiple levels of detail, from raw data to an executive summary. IntSights' capabilities to elicit clients' intelligence requirements and create a collection plan are lacking. Reference customers noted the competitive pricing, excellent customer service, and continued partnership with the vendor. Smaller enterprises looking for access to valuable threat data should consider IntSights.

Evaluation Overview

We evaluated vendors against 26 criteria, which we grouped into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include: intelligence requirements, intelligence analysis, cyber threat intelligence, brand threat intelligence, and vulnerability intelligence.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, innovation roadmap, and supporting products and services.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's number of clients and overall service revenue.

Vendor Inclusion Criteria

Forrester included 12 vendors in the assessment CrowdStrike, Digital Shadows, FireEye, Flashpoint, Group-IB, IBM, Intel 471, IntSights, Kaspersky, Recorded Future, RiskIQ, and ZeroFOX. Each of these vendors has:

- **A comprehensive external threat intelligence services offering.** All vendors in this evaluation have a large, globally available business offering a combination of vulnerability intelligence, brand threat intelligence, and cyber threat intelligence.
- **At least $10M in annual threat intelligence services revenue and over 100 threat intelligence services clients.** Each participant provides threat intelligence to clients in more than one geographic region (e.g., North America, EMEA, APAC).
- **A diverse and extensive threat intelligence team.** Each participant's threat intelligence team has a diverse skill set and cultural background.
- **Mindshare with Forrester clients.** Forrester clients often discuss the participating vendors during inquiries and interviews. Alternatively, the participating vendor may, in Forrester's judgment, have warranted inclusion because of technical capabilities and market presence.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by December 22, 2020 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ and New Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

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