The Forrester Wave™: Vulnerability Risk Management, Q4 2019

The 13 Providers That Matter Most And How They Stack Up

by Josh Zelonis and Trevor Lyness

October 17, 2019

Why Read This Report

In our 14-criterion evaluation of vulnerability risk management providers, we identified the 13 most significant ones — Brinqa, Digital Defense, Expanse, Kenna Security, NopSec, Outpost24, Qualys, Rapid7, RedSeal, RiskIQ, RiskSense, Skybox Security, and Tenable — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Key Takeaways

Tenable, Rapid7, And Qualys Lead The Pack

Forrester's research uncovered a market in which Tenable, Rapid7, and Qualys are Leaders; Kenna Security, NopSec, RiskIQ, and Expanse are Strong Performers; Digital Defense, Brinqa, RiskSense, RedSeal, and Skybox Security are Contenders; and Outpost24 is a Challenger.

Prioritization And Reporting Are Key Differentiators

Many VRM solutions are limited and fail to provide meaningful prioritization and metrics on the health of your VRM program. Vendors with improved prioritization and reporting are pushing the market forward.

The Forrester Wave™: Vulnerability Risk Management, Q4 2019

The 13 Providers That Matter Most And How They Stack Up

by Josh Zelonis and Trevor Lyness
with Stephanie Balaouras, Madeline Cyr, and Peggy Dostie

October 17, 2019

Table Of Contents

Related Research Documents

Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model

The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2018

The Forrester Wave™: Vulnerability Risk Management, Q1 2018

FORRESTER®

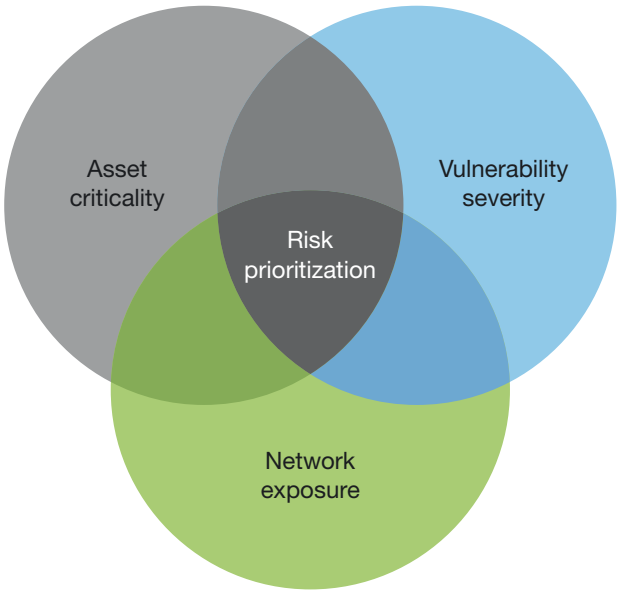
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Risk Prioritization Requires Complete Infrastructure Understanding

In the last vulnerability risk management (VRM) Forrester Wave™, Forrester focused on the four-stage process that is VRM: asset management, vulnerability enumeration, prioritization, and remediation.[1] Forrester clients regularly report a backlog on remediation, so in this Forrester Wave, we focused on prioritization to help reduce vulnerability risk. As VRM evolves to address customers' needs, this Forrester Wave seeks to highlight those solutions that help customers prioritize remediation efforts based on three critical elements (see Figure 1):

- **Asset criticality helps you understand what needs protected.** Organizations almost universally struggle with having good asset management capabilities, but knowing where your crown jewels are can help you prioritize remediation efforts to reduce the risk of loss. One of the new capabilities evaluated in this Forrester Wave was how well these products help you with digital footprinting to understand what internet-exposed assets you may not be aware of.[2]
- **Vulnerability severity informs the level of threat.** Vulnerabilities are nothing more than vectors for adversaries to control execution on a system. Sometimes the impact of a vulnerability is negligible, other times it can allow full system compromise. By understanding how an adversary can, or is, leveraging this vulnerability in the wild can help with prioritization.
- **Network exposure can be a compensating control to reduce risk.** Zero Trust is not just a buzzword; the better protected your assets are, the less exposed your organization is to loss.[3] If your crown jewels are sitting on the same network segment as your end users, an adversary is only a phishing email and one hop away from a devastating breach.

FIGURE 1 Three Attributes That Enable Risk-Based Prioritization



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.

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 2 and see Figure 3). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 2 Forrester Wave™: Vulnerability Risk Management, Q4 2019

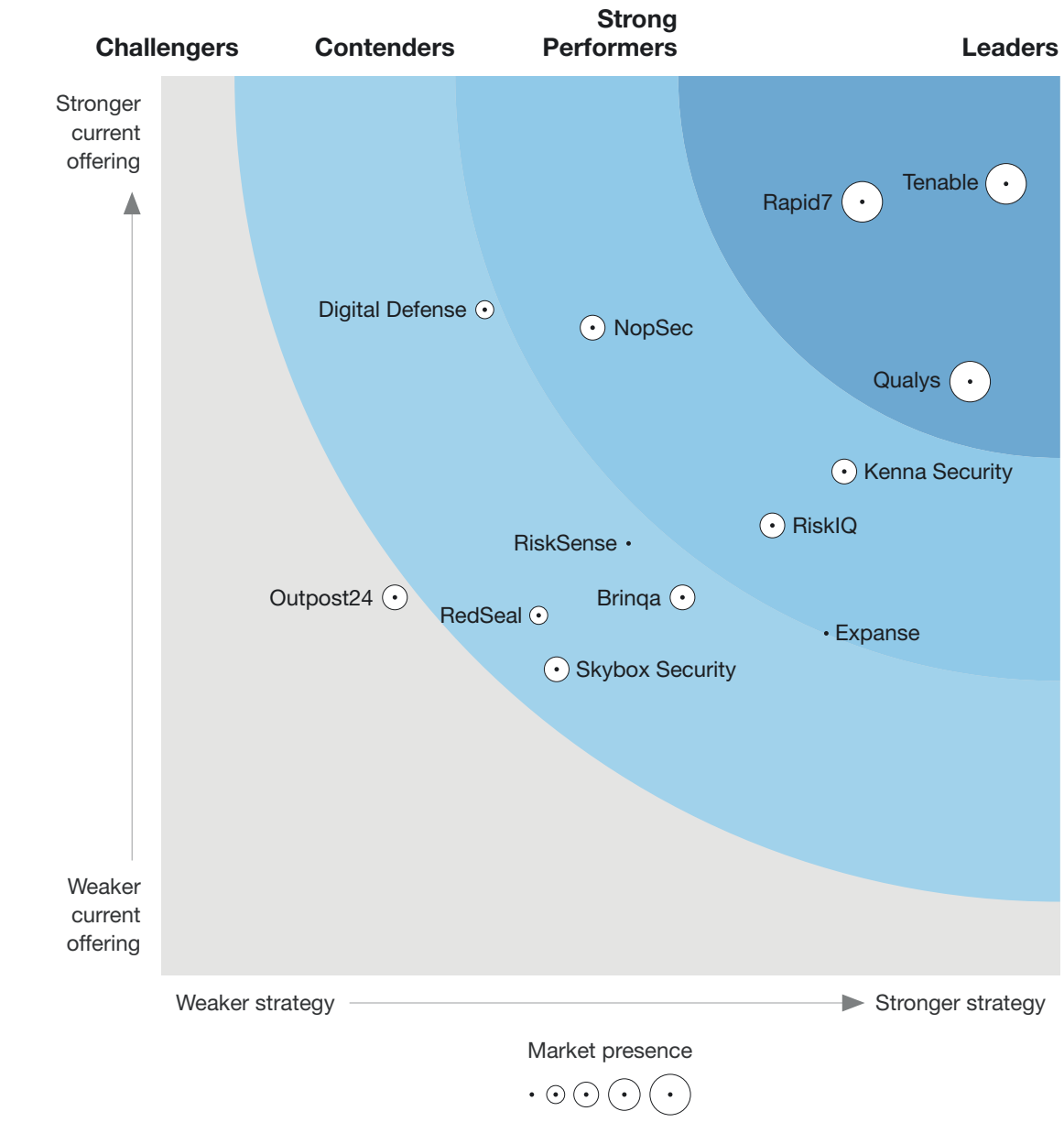


FIGURE 3 Forrester Wave™: Vulnerability Risk Management Scorecard, Q4 2019

	Forrester's weighting	Brinqa	Digital Defense	Expanse	Kenna Security	NopSec	Outpost24	Qualys	Rapid7	RedSeal	RiskIQ	RiskSense	Skybox Security	Tenable
Current offering	50%	2.10	3.70	1.90	2.80	3.60	2.10	3.30	4.30	2.00	2.50	2.40	1.70	4.40
Vulnerability enumeration	15%	3.00	3.00	3.00	1.00	3.00	3.00	5.00	5.00	1.00	3.00	1.00	1.00	5.00
Digital footprinting	10%	1.00	3.00	5.00	1.00	3.00	1.00	3.00	5.00	3.00	5.00	0.00	0.00	3.00
Asset criticality	15%	1.00	5.00	1.00	1.00	3.00	3.00	5.00	5.00	3.00	3.00	3.00	1.00	5.00
Network exposure	5%	3.00	1.00	3.00	1.00	1.00	1.00	3.00	1.00	5.00	3.00	1.00	5.00	1.00
Vulnerability severity	15%	3.00	3.00	1.00	3.00	3.00	1.00	3.00	5.00	1.00	1.00	3.00	3.00	5.00
Risk-based prioritization	15%	1.00	3.00	1.00	5.00	5.00	3.00	1.00	5.00	3.00	1.00	3.00	3.00	5.00
Metrics and reporting	20%	3.00	5.00	1.00	5.00	5.00	1.00	3.00	3.00	1.00	3.00	3.00	1.00	5.00
Role-based management	5%	1.00	5.00	3.00	3.00	3.00	5.00	3.00	3.00	1.00	1.00	5.00	1.00	1.00
Strategy	50%	2.90	1.80	3.70	3.80	2.40	1.30	4.50	3.90	2.10	3.40	2.60	2.20	4.70
Product vision	30%	3.00	1.00	5.00	3.00	1.00	1.00	5.00	5.00	1.00	3.00	3.00	3.00	5.00
Execution roadmap	30%	1.00	1.00	5.00	3.00	3.00	1.00	5.00	3.00	3.00	5.00	1.00	3.00	5.00
Commercial model	25%	5.00	3.00	1.00	5.00	3.00	1.00	3.00	3.00	3.00	1.00	5.00	1.00	5.00
Partner ecosystem	15%	3.00	3.00	3.00	5.00	3.00	3.00	5.00	5.00	1.00	5.00	1.00	1.00	3.00
Market presence	0%	3.00	2.00	1.00	3.00	3.00	3.00	5.00	5.00	2.00	3.00	1.00	3.00	5.00
Number of clients	50%	3.00	3.00	1.00	3.00	3.00	3.00	5.00	5.00	1.00	3.00	1.00	3.00	5.00
Product revenue	50%	3.00	1.00	1.00	3.00	3.00	3.00	5.00	5.00	3.00	3.00	1.00	3.00	5.00

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

Vendor Offerings

Forrester included 13 vendors in this assessment: Brinqa, Digital Defense, Expanse, Kenna Security, NopSec, Outpost24, Qualys, Rapid7, RedSeal, RiskIQ, RiskSense, Skybox Security, and Tenable (see Figure 4).

FIGURE 4 Evaluated Vendors And Product Information

Vendor	Product evaluated	Product version evaluated
Brinqa	Brinqa Vulnerability Risk Service	5.9.0
Digital Defense	Frontline.Cloud	6.2
Expanse	Expanse Platform	SaaS
Kenna Security	Kenna Security Platform	M/A
NopSec	Unified VRM	5.0
Outpost24	Outpost24 Platform	Outpost24 Spring 2019
Qualys	Qualys Cloud Platform	8.20.0.0-2
Rapid7	InsightVM	
RedSeal	RedSeal	
RiskIQ	RiskIQ Illuminate	v5.0.0-9e387e8
RiskSense	RiskSense	8.11.0
Skybox Security	Skybox Security Suite: Vulnerability and Threat Management Solution	10.0.200
Tenable	Tenable.io with Tenable Lumin	SaaS

Vendor Profiles

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

Leaders

› **Tenable provides insights into how your org compares to peer performance.** Tenable executes on its vision to build the single-source-of-truth platform for VRM. Part of Tenable's strong strategy relies on translating data to provide business insight to provide prioritization. Its Vulnerability

Priority Rating (VPR) technology surpasses standard CVSS scores as a way to dynamically prioritize risk within an environment. Their reporting capabilities allow you to break out by line of business and trend over time, in addition to the ability to compare your security posture to your industry and population.

Customer references echo that Tenable's VPR technology and reporting capabilities are differentiable, but wish it had the ability to automatically classify assets. On its roadmap, Tenable has outlined plans to make improvements to its core VM product, its cyber exposure analytics product, Lumin, and its partner ecosystem. Tenable is a great choice for enterprises looking for a VRM vendor that provides strong prioritization and reporting across device types.

› **Rapid7 provides comprehensive visibility and a clear action plan.** Rapid7 is focused on helping clients understand the vulnerability risk their businesses face. It combines threat intelligence on active campaigns with its in-house research team's expertise to assign a Real Risk Score to vulnerabilities in the context of your business. Additionally, it offers Project Sonar, a free tool that gathers reverse DNS records for all public IPv4 addresses, enabling organizations to discover assets they didn't know they had.

While Rapid7's vulnerability enumeration and prioritization capabilities are impressive, its reporting capabilities lack flexibility, even though it has the data to back it up. Customer references agreed, noting that custom reporting on individual business units was cumbersome. On the positive side, references appreciated how easy it was to deploy scanning engines. Rapid7 is a strong choice for any company looking for a vulnerability management tool that can streamline their decision-making processes.

› **Qualys has a large breadth of sensors available for vulnerability enumeration.** Qualys is a global organization that is able to handle scanning large hybrid IT environments. It has strong capabilities supporting asset criticality including assigning asset groups dynamically. Its roadmap is pushing the market forward by extending vulnerability management to cover more areas, such as roaming systems, DevOps (CI/CD), containers, cloud, industrial control systems (ICS), and mobile devices.

Customer references indicate that Qualys is an excellent choice for scanning complex enterprise environments; however, they do note that it is a complicated product and that Qualys is playing catchup in terms of prioritization. Today, Qualys is a good fit for large enterprises that prefer to prioritize remediation via their own systems or processes

Strong Performers

› **Kenna Security makes itself the destination for all forms of vulnerability data.** Kenna Security does not provide a scanning solution; however, it ingests vulnerability data from a wide array of sources such as vulnerability scanners and endpoint agents. The Kenna Security solution is instead focused on providing risk scores to help security pros prioritize remediation. Unfortunately, Kenna Security itself does very little to facilitate asset management, relying on users to manually set asset priority within the Kenna platform or pull that data from a content management database (CMDB).

Customer references appreciate how easy it is import data from disparate sources but note that it can be difficult to understand the methodology behind a risk score change. Kenna Security is a strong choice for companies that already have asset management and vulnerability capabilities but need a solution to help them report on and prioritize vulnerability remediation.

› **NopSec's Unified VRM solution offers strong risk prioritization and reporting.** NopSec offers a vision of unified vulnerability management that integrates and automates manual workflows, risk prioritization, and remediation efforts. It has spent the past year rebuilding both the front and back end of its products to improve user experience. Its Unified VRM is scanner-agnostic and can ingest scans from third-party sources either via API or via upload.

NopSec differentiates by offering a complete end-to-end solution but fails to outshine competitors in any one area. Reference customers appreciate the new UI and strong reporting capabilities. They want to see more integrations with SIEMs and patching solutions. NopSec is a good option for customers who want a single VRM product that can both enumerate and prioritize vulnerabilities.

› **RiskIQ helps companies manage vulnerabilities on assets they didn't know existed.** RiskIQ uses a sophisticated sensor network in combination with virtual web crawlers to identify assets and vulnerabilities on publicly addressable systems. It also fingerprints any services it finds and allows you to query this data to quickly identify vulnerabilities in your extended infrastructure. RiskIQ is purely an external solution and does not identify vulnerabilities inside your network.

RiskIQ is a strong tool to have in your vulnerability management toolbox, but the focus on attack infrastructure means it can only be just a piece of your VRM program. Reference customers state that RiskIQ has been invaluable in helping them discover infrastructure they didn't know existed. However, they felt there's a lot of manual processing necessary to sift through all the information discovered, especially during deployment. RiskIQ is a great fit for large enterprises that need help identifying unknown and vulnerable assets.

› **Expanse monitors the communications of assets, no installation required.** It enables asset discovery by continuously collecting information about all globally accessible systems on the internet. In addition, it leverages unique partnerships with internet service providers (ISPs) to monitor for risky communications involving customer assets without the need to install a sensor. It doesn't offer traditional vulnerability management capabilities, and instead looks to expand a vulnerability management team's visibility into assets the team is not aware of.

Expanse cannot be treated as a proper vulnerability management tool. Instead, it built an inventory of internet asset data to view within their UI or feed into something else. Unfortunately, Expanse's integration options are limited, and if you want to pull information you have to use its API or Splunk integration. Customers loved the visibility that Expanse gave them in seeing machines talk to each other but noted that the onboarding process takes time and effort to reduce the number of false positive that appear. Expanse is a good fit for companies that have additional VM budget and need additional asset discovery and visibility capabilities.

Contenders

› **Digital Defense simplifies vulnerability management and brings a red team mentality.** Its offering includes a vulnerability scanner that can scan most types of systems, though containers are still on its roadmap. It enriches vulnerability information with context from its in-house research team, and then incorporates that alongside business context into a risk score called the Frontline Security GPA. Digital Defense also offers penetration testing services, which are frequently bundled alongside its VRM solution.

Digital Defense's Security GPA risk scoring is pragmatic and approachable, making it easy for customers to know what problem they should be tackling next. However, Digital Defense has oversimplified its presentation of vulnerability severity and Security GPA calculations which makes it a challenge to understand why a particular severity has been chosen. Reference customers appreciated that they had a dedicated security specialist that maintained the customer relationship but want more integrations into VM products they use such as ticketing solutions. Organizations with a limited VRM team that need a straightforward vulnerability management tool should consider Digital Defense a good option.

› **RiskSense aims to be VRM's central dashboard.** RiskSense ingests vulnerability data from vulnerability scanners, databases, and CMDBs. It aggregates the data and assigns its credit-score-like risk score, the RiskSense Security Score (RS3). Bidirectional integrations with ticketing systems such as ServiceNow allow you to push remediation efforts to operation teams. The aim for RiskSense is to be the destination for all vulnerability data and a hub for risk prioritization and remediation.

However, RiskSense's product does not match its vision. While it adds severity context to vulnerabilities beyond a basic CVSS score, it is unclear how or why severity is changed. RiskSense can show you which of your assets are riskiest, but it didn't demonstrate the ability to provide you recommended actions that would reduce the most risk. Reference customers noted that the solution is rigid, with limited ability for customization. Companies looking for a dashboard to aggregate and report on vulnerability risk can consider RiskSense an option.

› **Brinqa wants to be your single pane of glass into vulnerability data.** Brinqa's vulnerability management solution has connections to 150-plus sources of vulnerability data, including digital footprinting and network exposure vendors. The platform is enormously customizable, allowing you to make the platform work however you'd like. Brinqa offers the ability to do risk prioritization but largely expects its customers to determine their own formula for prioritizing risk.

Brinqa's downside is its UX. Any major form of customization, such as changing your risk prioritization calculation or generating a specific view, requires you to write custom code within the Brinqa platform. This may work fine for teams that set up a system once and never change anything, but it will not work well for organizations with dynamic environments. Customer references appreciated the degree of flexibility, but noted you need to have an extremely clear vision of what you want, or you may design something that doesn't actually work. Brinqa is suited for companies that want to build a custom VRM dashboard.

› **RedSeal uses cyber risk modeling to help you understand your network exposure.** RedSeal's strategic vision is driving resilience into the infrastructure. Its goal is to help you understand the highest risk vulnerabilities in your infrastructure based on where they are and what they expose. RedSeal does not provide the core scanning functionality that clients look for in a VRM product; instead, it ingests configuration, vulnerability, and other information from existing devices within the customer's infrastructure.

References confirm the product adds value to their VRM strategy by helping them understand risk of a vulnerability based on the context of where it sits in the network particular. RedSeal is best for companies that is already happy with their current vulnerability enumeration capabilities but need more context into exposures within their network.

› **Skybox Security highlights exploitable vulnerabilities exposed in the environment.** To determine if a vulnerability is exploitable, Skybox does a combination of modeling and attack path simulation. This is determined by evaluating an organization's security controls from all potential threat origins. Its visualization of "reachability" demonstrates to users how network segmentation affects the risk of vulnerability exploitation in their environment. Skybox's vision is that a successful vulnerability risk management program takes into account the unique context of an organization for discovery, risk analysis, and remediation.

Reference customers mention that Skybox's "holistic" approach to vulnerability end-to-end is a differentiator. They like the ability to visualize their network and the firewall management capabilities Skybox provides them. Skybox is less feature rich than comparable vendors in this Forrester Wave for many of the evaluated features. Skybox is best for companies that want visibility into their network exposure.

Challengers

› **Outpost24 offers a supportive relationship for its reference customers.** Rooted in ethical hacking, Outpost24 has a strategy of full stack assessment, motivated by the need to provide value through more context of different attack paths. It has also invested heavily in its API strategy to help reference customers integrate with security and operational technology.

Customer references note that the product is flexible and easy to use. References were consistently happy with the support they received and the management of the product. Some did note that the interface could use some work and the reporting needs to be more competitive. In spite of offering a lot of the core functionality that clients look for in a VRM product, this product is more focused on vulnerability data collection than on risk-based prioritization than its competitors. Overall, we would recommend Outpost24 to those who are looking for a vulnerability assessment vendor who will be an engaged and responsive partner.

Evaluation Overview

We evaluated vendors against 14 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 vulnerability enumeration, digital footprinting, asset criticality, network exposure, vulnerability severity, risk-based prioritization, metrics and reporting, and role-based management.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, execution roadmap, commercial model, and partner ecosystem.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's number of clients, and product revenue.

Vendor Inclusion Criteria

Forrester included 13 vendors in the assessment: Brinqa, Digital Defense, Expanse, Kenna Security, NopSec, Outpost24, Qualys, Rapid7, RedSeal, RiskIQ, RiskSense, Skybox Security, and Tenable. Each of these vendors has:

- **Product revenue and growth.** Vendors needed annual product revenue greater than $10 million and show double digit growth for their VRM solution in the most recent fiscal year.
- **Product significance to the business.** Vendors needed to show they are actively invested in building a competitive product as reflected in product improvements over the last two years, as well as showing the VRM product was responsible for over 50% of their total revenue.
- **Enterprise client base.** Vendors needed to show the ability to sell to and support enterprise clients as demonstrated by at least 100 enterprise customers.
- **Forrester mindshare.** Forrester considered the level of interest from our clients based on our various interactions, including, but not limited to, inquiries, advisories, and consulting engagements.

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

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 July 31, 2019, 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™ 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.

Endnotes

[1] See the Forrester report "The Forrester Wave™: Vulnerability Risk Management, Q1 2018."

[2] See the Forrester report "New Tech: Digital Risk Protection, Q2 2018."

[3] See the Forrester report "The Eight Business And Security Benefits Of Zero Trust."

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.

152075