The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021

The Seven Providers That Matter Most And How They Stack Up

by Paul McKay and Alla Valente
February 25, 2021

Why Read This Report

In Forrester's evaluation of the emerging market for cybersecurity risk ratings, we identified the seven most significant providers in the category — BitSight, Black Kite (previously Normshield), Panorays, Prevalent, RiskRecon, SecurityScorecard, and UpGuard — 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 and risk leaders can use this report to select the right partner for their cybersecurity risk ratings needs.

Key Takeaways

SecurityScorecard And BitSight Lead The Pack
Forrester's research uncovered a market in which SecurityScorecard and BitSight are Leaders; Panorays and RiskRecon are Strong Performers; and Prevalent, UpGuard, and Black Kite are Contenders.

Ratings Model Accuracy, Transparency, And Integrations Are Key Differentiators
The cybersecurity risk ratings market resembles the credit ratings market from which it is inspired. Establishing trust in the model accuracy (and not just accuracy of attribution) and open and transparent methodology are foundational elements on which everything else rests. To allow CISOs to use cybersecurity risk ratings solutions in the context of their own third-party and enterprise risk management process, good-quality integrations with a range of other risk and compliance management technologies are crucial to ubiquitous adoption. The world does not need another security portal or single pane of glass.

The Forrester New Wave™: Cybersecurity Risk Ratings Platforms, Q1 2021

The Seven Providers That Matter Most And How They Stack Up

by Paul McKay and Alla Valente
with Joseph Blankenship, Shannon Fish, and Peggy Dostie

February 25, 2021

Table Of Contents

Related Research Documents

Cybersecurity Risk Ratings Market Outlook, 2020 And Beyond

The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018

FORRESTER®

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

Cybersecurity Risk Ratings Are Not Yet Ready For Prime Time

The cybersecurity risk ratings (CSR) market takes its inspiration from the credit ratings market. Using externally observable data for an enterprise's external internet presence, solutions in this market give a single, aggregated rating of a firm's cybersecurity posture across several security risk factors. Data collected by the platforms provides value by allowing firms to validate claims made by third parties and internal stakeholders about their security posture versus what is observed. The most common use cases supported by these solutions include cybersecurity vetting and continuous monitoring within third-party risk management (TPRM), enterprise security risk management and benchmarking, M&A due diligence, executive or board-level communication, and cyberinsurance policy underwriting.

The market has come a long way since the last Forrester New Wave™ published in 2018, with many improvements in ratings accuracy, asset attribution, and workflow improvements made by many of the CSR platforms.[1] However, the market is still immature, with several improvements required before it's ready to be considered as a mature, enterprise-ready class of security solutions. Here are some of the things we observed in our research:

- **CSR platform accuracy measurements don't necessarily reflect a firm's cyber risk.** Many of the vendors in this research focus their accuracy measurements on asset attribution: Have they correctly associated an asset with the appropriate organization? Vendors are commissioning external work to review their models from that perspective. However, while accurate asset attribution is important, it's not the same thing as a statistical confidence level that the rating itself is an accurate representation of a firm's current security posture. Ratings vendors need to go further to validate that the security data points chosen for their models, the weightings of those variables, the type of analysis, and how the machine learning models are trained and tested are also most accurately representing the true risk. Ratings vendors also need to go beyond the internal review by having their models externally validated to further build confidence in what this market delivers.
- **Vendors have varying levels of transparency into their models and algorithms.** Transparency has improved since the last Forrester New Wave, but the CSR firms still need to do much more. Some firms provide less detail than others in the public domain, holding a lot of information back only for customers, while others provide detailed white papers and portals explaining their methodologies for all to review. The level of transparency offered around the dispute resolution process is a key area for improvement. This is handled mostly by the firms themselves, leading to accusations by some in the security industry that these firms are "playing God." CSR ratings firms need to improve the level of transparency they offer around their dispute resolution procedures and consider implementing an industrywide ombudsman to independently adjudicate on disputes between firms and publish publicly the outcome of these disputes.
- **Vendors need to better integrate with adjacent security solutions.** CSR solutions are used for two primary use cases — providing additional data and continuous monitoring capability to help with the assessment of both a firm's own security posture and the security posture of its third-

party ecosystem. There are differences in vendors' approach to integrations, with some building their own workflow engines and questionnaire modules. Others are building native integrations with leading GRC and TPRM platforms (and occasionally security analytics platforms such as Splunk). The quality of the integrations provided by some vendors is not good enough, with low-quality data dumps delivered and missing out on opportunities to bring additional context and insight from the data in the context of the wider business process for third-party security reviews or enterprise risk management.

- **Limited capabilities to contextualize risk limits ability to operationalize the ratings.** Vendors in this market are overwhelming customers with the volume of alerts, notifications, and data points collected on their third parties, and it's impeding customers' ability to act on the information. The "more is more" approach also extends to vendors' messaging that incorrectly suggests the more data points that are collected and input into the model, the more accurate the ratings. Instead of bombarding users with more data, CSR vendors need to focus on improving the risk context of their ratings to help security and risk pros prioritize efforts, support risk-based decisions, and act on the information. Additionally, for those with data-driven initiatives and inclinations, customers in this space should have complete choice over whether to use the CSR platforms or consume the solution entirely via their security platform of choice to run their own scenarios and algorithms.

Cybersecurity Risk Ratings Evaluation Overview

The Forrester New Wave differs from our traditional Forrester Wave™. In the Forrester 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 seven vendors in this assessment: BitSight, Black Kite (previously Normshield), Panorays, Prevalent, RiskRecon, SecurityScorecard, and UpGuard (see Figure 2 and see Figure 3).[2] At the time of this research commencing, the cybersecurity risk ratings business of FICO was acquired by ISS. As this business is still in transition between the two firms, we did not include them in this research at this time. Each of these vendors has:

- **$1 million of revenue from cybersecurity risk ratings products.** We did not include any firms that reported less than $1 million of revenue from their cybersecurity risk ratings products.
- **Mindshare and market presence.** We only included vendors that have at least 75 active customers for their CSR offering as measured by individual logos, not number of deployments, and receive interest from Forrester clients.

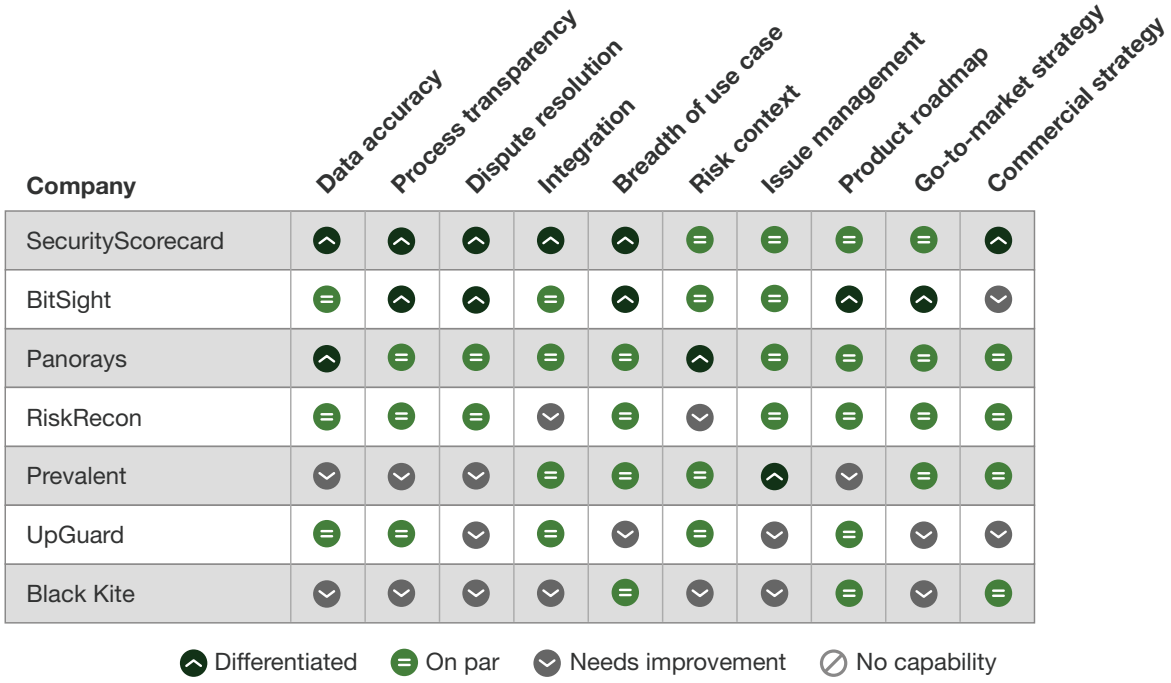
FIGURE 1 Assessment Criteria: Cybersecurity Risk Ratings, Q1 2021

Criteria	Platform evaluation details
Data accuracy	What types of data does the vendor collect to inform its cybersecurity ratings, and what is the collection method? How does the vendor ensure that data is correctly attributed to companies being rated? What calibration methods does the vendor use to update its ratings model, and how often is it updated?
Ratings process transparency	How does the vendor provide transparency to rated companies about how their rating was derived? What information is publicly available to rated companies (noncustomers) about the methodology and process for how their rating was derived?
Dispute resolution management	What is the vendor's process for dealing with disputes about a company's rating? How does the vendor make its dispute process publicly available and easily accessible? Upon accepting a ratings correction, how is the correction represented in both the current rating and historical rating?
Integration and interoperability	What is the vendor's approach to technology integration with other risk management platforms (such as GRC and third-party risk management)? How do these integrations help customers operationalize the ratings within other enterprise technologies? What languages does the vendor support?
Breadth of use case	What are the vendor's dashboard and reporting capabilities to view and interact with their security rating? How does the vendor's platform support third-party security management and internal enterprise security risk management use cases and workflows?
Risk context	How does the vendor contextualize cybersecurity and other risk factors to help operationalize the rating? How does the platform map risk issues identified to compliance standards or frameworks? How does the vendor's platform enable end users to measure progress in risk reduction?
Issue and remediation management	How does the solution enable users to understand the issues they need to address to improve their overall rating score? How does the vendor's solution help users construct remediation plans linked to the risk and severity of the issues identified?
Market vision and product roadmap	What is the vendor's product roadmap for the next 12 to 18 months? What is the vendor's vision for how the cybersecurity risk ratings market will develop over the next 12 to 18 months?
Global go-to-market and partner strategy	How is the vendor's go-to-market strategy going to evolve over the next 12 to 18 months? How is the vendor's approach to strategic partnerships and alliances going to change over the next 12 to 18 months? How does the vendor market its product to an international audience?
Commercial strategy and pricing innovation	How is the vendor planning to evolve its commercial and pricing approaches in the next 12 to 18 months?

FIGURE 2 Forrester New Wave™: Cybersecurity Risk Ratings, Q1 2021

*A gray bubble indicates a nonparticipating vendor.

FIGURE 3 Forrester New Wave™: Cybersecurity Risk Ratings Scorecard, Q1 2021



Vendor QuickCards

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

SecurityScorecard: Forrester's Take

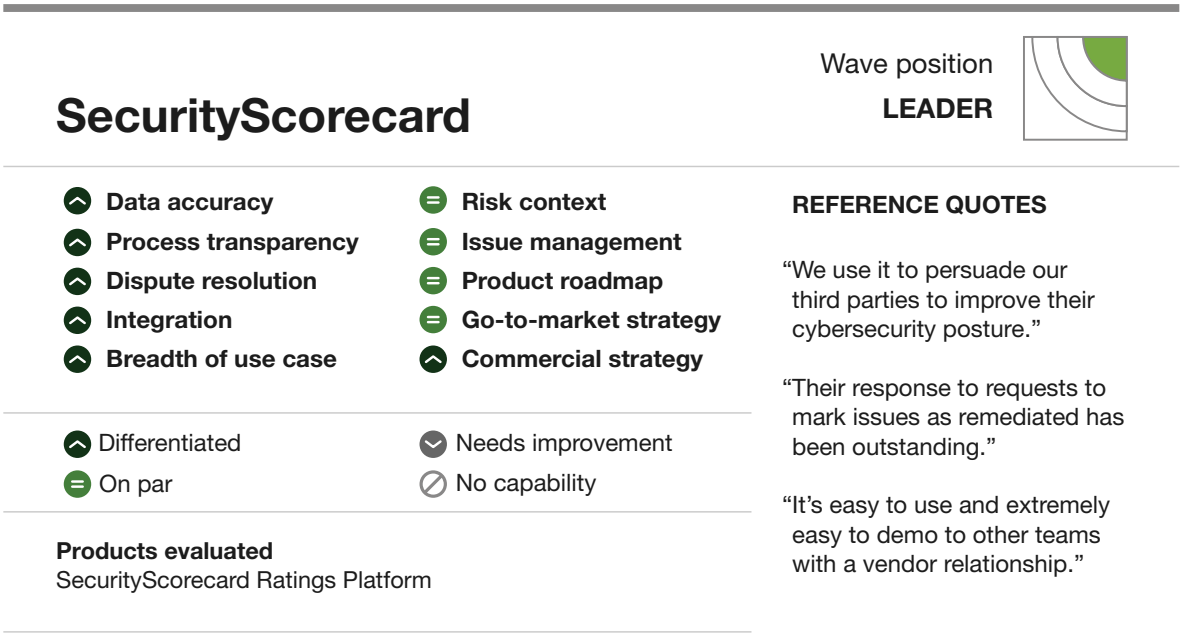
Our evaluation found that SecurityScorecard (see Figure 4):

- **Leads the pack with robust process transparency and workflow capabilities.** SecurityScorecard demonstrated some of the most detailed ratings model white papers and publicly available information through its Trust Portal. The Atlas module provides greater depth to the workflow process by matching ratings data to vendor questionnaires.
- **Still needs to improve issue management and third-party integration quality.** The issues and remediation management capabilities could be improved by adding additional issue context and offering remediation prioritization features. Third-party integrations are inconsistent between GRC and TPRM platforms.
- **Is a good fit for customers without GRC/TPRM platforms with survey capability.** They are a good fit for those that want strong ratings transparency and an inside-out perspective that comes from assessment surveys and that looking for a clear pricing structure.

SecurityScorecard Customer Reference Summary

Customer references praised the ease of dealing with SecurityScorecard, its platform visibility, and UX. References noted limited custom reporting options and requested methodology improvements.

FIGURE 4 SecurityScorecard QuickCard



BitSight: Forrester's Take

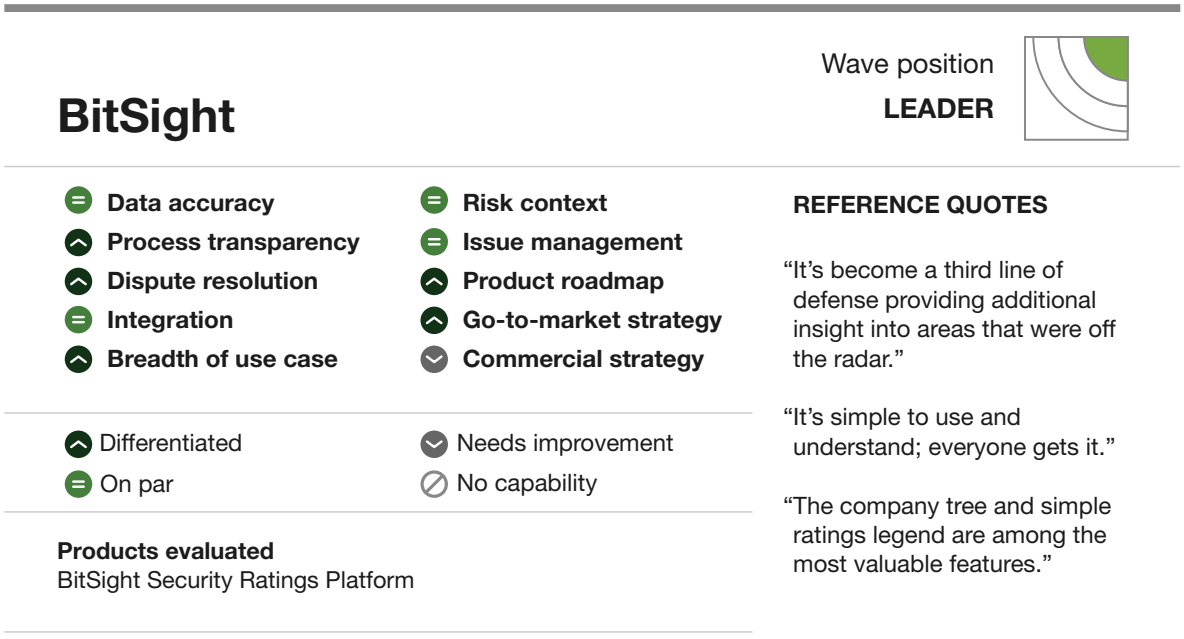
Our evaluation found that BitSight (see Figure 5):

- **Differentiates with ratings process transparency and high-quality integrations.** BitSight has developed robust processes for assessing dispute resolutions and provides a lot of details on its methodology. Benchmarking and asset entity mapping details the structure of companies being evaluated. BitSight's high-quality, third-party integrations are a strength.
- **Must simplify its pricing packages, which are opaque.** BitSight has recently increased the level of complexity in its third-party pricing packages, making it more challenging for customers to establish the right package for them. In addition, BitSight could improve its ratings for IT service providers, which are lower due to customer security issues.
- **Best suited for firms with a wide range of use cases and reporting requirements.** BitSight is best for firms looking to use a well-established rating firm that supports a broad range of use cases, require high-quality benchmarking, and have dedicated CSR budget.

BitSight Customer Reference Summary

BitSight customer references indicated high levels of satisfaction with accuracy and ratings process transparency. Customer references flagged board reporting as an area for improvement.

FIGURE 5 BitSight QuickCard



Panorays: Forrester's Take

Our evaluation found that Panorays (see Figure 6):

- **Stands out for its workflow capabilities, accuracy, and risk context.** Panorays differentiates with its complete questionnaire capabilities, accuracy, and workflow. The risk context delivered by Panorays combines human factors, questionnaire management for third parties, and a simple-to-use fourth-party discovery feature.
- **Must improve the documentation of its ratings methodologies and reporting.** Panorays needs to improve the depth and clarity of its ratings methodology documentation. The reporting displays a lot of information in table formats, but some of the reports need to be more visual and easier to view.
- **Fits customers who need a ratings platform combined with TPRM workflow.** Panorays is particularly well suited to organizations that have no prior investments in GRC or TPRM technology and need a solution that combines ratings data with questionnaire workflow.

Panorays Customer Reference Summary

Panorays references praised the accuracy of the platform, high-quality ratings reports, and low false positives rates, but desired online editing of compliance questionnaires as a roadmap feature.

FIGURE 6 Panorays QuickCard

Panorays

Wave position
STRONG PERFORMER

Data accuracy	**Risk context**
Process transparency	**Issue management**
Dispute resolution	**Product roadmap**
Integration	**Go-to-market strategy**
Breadth of use case	**Commercial strategy**

Differentiated
On par
Needs improvement
No capability

Products evaluated
Panorays

REFERENCE QUOTES

"We chose Panorays due to their transparency in reporting."

"Panorays is key for determining deeper level of cyber assessment by our information security team."

"Exceptional customer service — unlike any we have used!"

RiskRecon: Forrester's Take

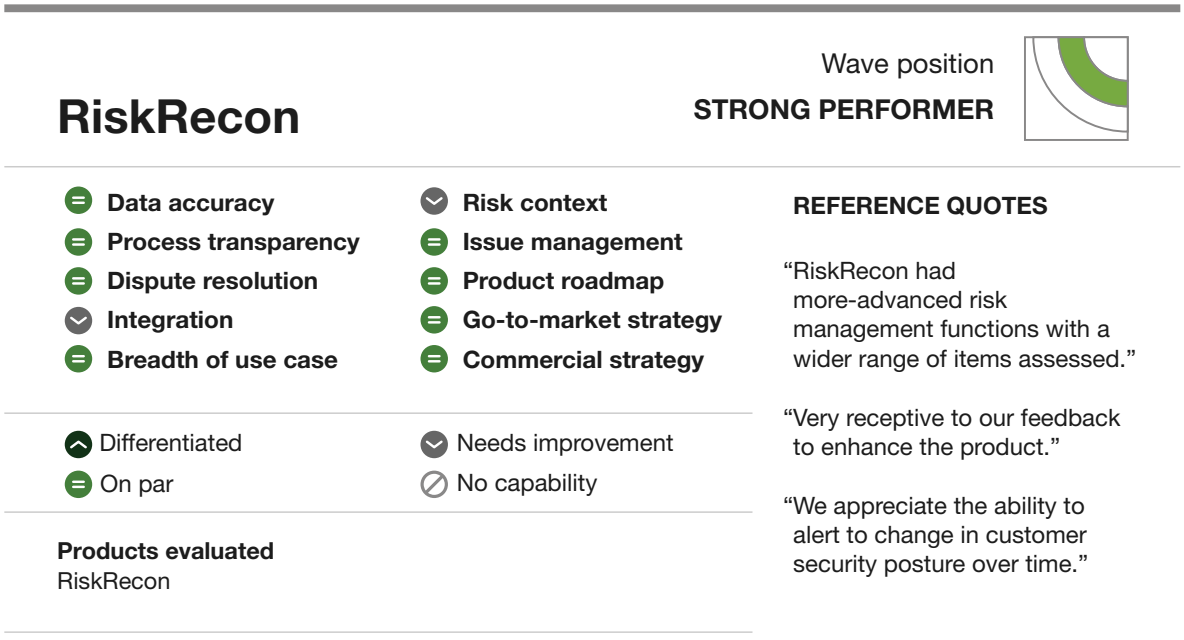
Our evaluation found that RiskRecon (see Figure 7):

- **Delivers granular ratings data and clear pricing.** RiskRecon offers a range of data points, helpful for deeper investigation. The Risk Priority matrix supports findings visualization. RiskRecon has clear pricing packages for customers.
- **Needs to improve its third-party integrations and board-level reporting capabilities.** RiskRecon lags in the range and quality of third-party integrations it offers. Some of the board-reporting features are too detailed and granular to be usable by executives.
- **Best for customers who want to get deep into their ratings data.** RiskRecon's depth of data and download options are a good fit for customers wishing to use the ratings data for attack surface monitoring use cases.

RiskRecon Customer Reference Summary

RiskRecon customer references praised the vendor for the receptiveness to feedback and the depth of the data collected as strengths. Reference customers mentioned improved mapping to compliance frameworks. Some customer references also expressed extreme dissatisfaction with the user interface and said that email notifications lacked actionability.

FIGURE 7 RiskRecon QuickCard



Prevalent: Forrester's Take

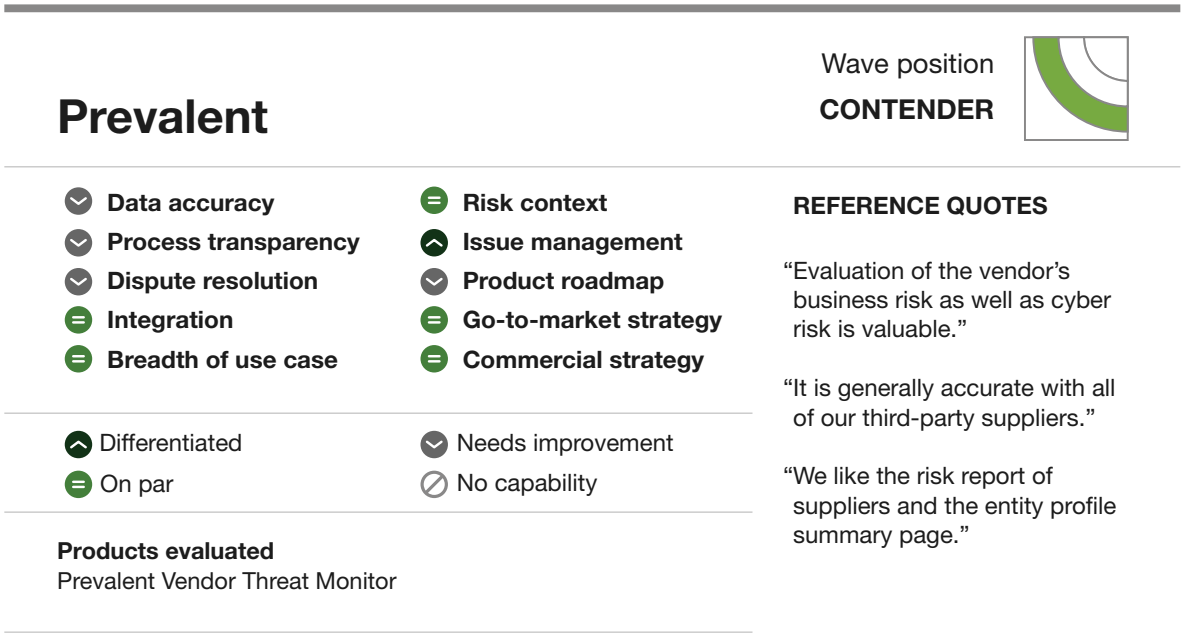
Our evaluation found that Prevalent (see Figure 8):

- **Has strong integrations with its TPRM product and broader noncyber data.** Prevalent supplements the standard security-focused ratings data with broader financial risk and business data. The platform stands out for its functionality and workflow.
- **Struggles to differentiate in the cybersecurity ratings market with its VTM product.** Prevalent has partnered with other firms in the ratings market to provide its underlying data. It struggled to articulate its unique differentiation in the ratings market. Its security ratings roadmap and vision, therefore, don't align with CSR customer needs.
- **Is best suited to customers who want ratings as an add-on to Prevalent TPRM.** The Prevalent VTM product is best consumed by customers as part of a broader Prevalent TPRM product purchase. Firms looking for managed service support should consider Prevalent.

Prevalent Customer Reference Summary

Reference customers liked that it offers business and cyber risk reporting, and praised its managed services. They noted licensing structure improvements, and that some supplier breaches were not picked up by Prevalent's cyber risk intelligence sources.

FIGURE 8 Prevalent QuickCard



UpGuard: Forrester's Take

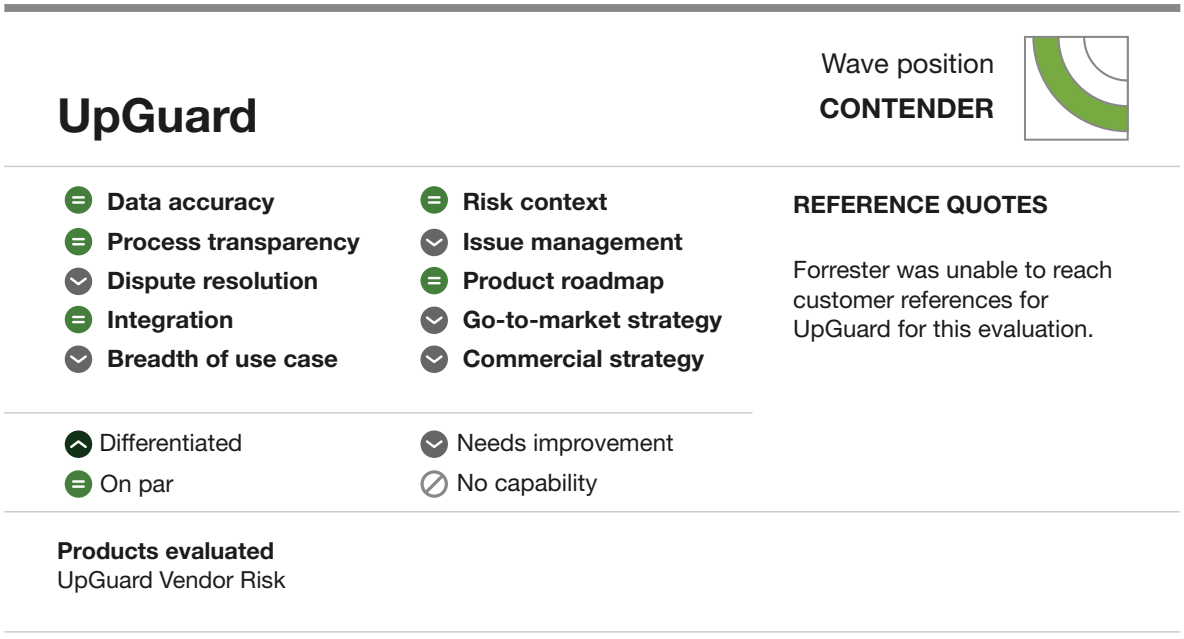
Our evaluation found that UpGuard (see Figure 9):

- **Offers deep data collection and research.** UpGuard collects a deep set of threat intelligence indicators and information about organizations' attack surface. UpGuard's focus on third parties and fourth-party concentration risk are helpful features for customers.
- **Should address transparency for its dispute resolution procedures.** UpGuard has more limited documentation for some of its processes in public compared to others in the market. UpGuard needs to expand its methodology and dispute resolution procedures in public to cater to nonclients who have been rated using the service.
- **Fits customers who have attack surface monitoring use cases.** UpGuard is a good fit for customers wishing to build a detailed understanding of their own attack surface. It's also well fitted for performing vulnerability discovery, such as wishing to understand exposure to specific vulnerabilities within a company's own supply chain.

UpGuard Customer Reference Summary

UpGuard was a nonparticipant in our research so no customer reference summary is available.

FIGURE 9 UpGuard QuickCard



Black Kite (Previously Normshield): Forrester's Take

Our evaluation found that Black Kite (see Figure 10):

- **Incorporates a range of data points in its ratings model.** Black Kite tracks and gathers a range of data points on rated companies in its model. It adds compliance and financial quantification data for clients' consumption, and offers aggressive pricing for its products.
- **Must substantially improve most aspects of its platform and dispute process.** Black Kite's reporting and visualizations are basic and difficult to navigate. Financial quantification metrics using OpenFAIR are far too broad to be useful for decision-making. Rated entities can make changes to their own ratings, undermining independence and ratings integrity.
- **Is the best fit for companies with sophisticated data analysis requirements.** Black Kite is a good fit for customers who want to get into the weeds with their ratings data. It's also a good fit for customers with budget constraints.

Black Kite Customer Reference Summary

Black Kite customers praised the level of detail available from the data provided. Customers desired better-quality integrations with platforms with third-party security risk questionnaire capability to allow ratings data to be combined with their existing TPRM program security questionnaires.

FIGURE 10 Black Kite QuickCard

Black Kite

Wave position
CONTENDER

Data accuracy	**Risk context**
Process transparency	**Issue management**
Dispute resolution	**Product roadmap**
Integration	**Go-to-market strategy**
Breadth of use case	**Commercial strategy**

Differentiated	Needs improvement
On par	No capability

REFERENCE QUOTES

"The tools are easy enough that adoption of the platform for users is quick and simple."

"I like Black Kite's wide range of data categories that they scan for."

Products evaluated
Cyber Risk Ratings Platform, 4.9

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] See the Forrester report "The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018."

[2] At the time of evaluation, Normshield was in the process of changing its brand name to Black Kite, which occurred at the beginning of January 2021. The underlying product evaluated did not change during this period.

FORRESTER®

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.

161625