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

The Nine Providers That Matter Most And How They Stack Up

by Nick Hayes and Trevor Lyness

November 13, 2018

Why Read This Report

In Forrester's evaluation of the emerging market for cybersecurity risk rating solutions, we identified the nine most significant providers in the category — BitSight, FICO, iTrust, 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 (S&R) professionals can use this review to select the right partner for their cybersecurity risk rating solution needs.

Key Takeaways

BitSight, RiskRecon, Prevalent, And SecurityScorecard Lead The Pack
Forrester's research uncovered a market in which BitSight, RiskRecon, Prevalent, and SecurityScorecard are Leaders; Panorays and FICO are Strong Performers; and UpGuard, NormShield, and iTrust are Challengers.

Risk Analytics, Entity Attribution, And Rating Consistency Are Key Differentiators
The best cyber-risk rating solutions don't merely report on your third-party partners' security flaws, they contextualize and prioritize the risk information they collect so you can more strategically allocate resources and mitigate risk.

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

The Nine Providers That Matter Most And How They Stack Up

by Nick Hayes and Trevor Lyness
with Christopher McClean, Josh Zelonis, and Christine Turley

November 13, 2018

Table Of Contents

Related Research Documents

The Forrester Tech Tide™: Risk And Compliance Management, Q2 2018

Protect Your Extended Ecosystem With Third-Party Cyber-Risk Scoring

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 Tackle A Ballooning Third-Party Problem

S&R leaders we surveyed for this evaluation reported that their respective organizations work with more than 4,700 third-party partners on average — and that's not even accounting for the reference from a global manufacturer that cited more than 500,000 third parties worldwide. And even with formal third-party risk programs in place, only 14% of respondents said they are confident that they effectively track all of their third parties.[1] It's clear that current efforts fall short. Spreadsheets and ad hoc questionnaires fail as stopgaps, resulting in outdated data, widening information gaps, and, ultimately, security breaches. Third parties were the cause of 21% of confirmed breaches in 2018, and that's up from 17% in 2017.[2]

Cybersecurity risk rating solutions come in to help close these gaps. They automate the collection and analysis of externally available third-party risk data to help users more accurately assess their partners' relative cyberhygiene and risk exposure. To get the most out of these solutions, it's important to understand their strengths and limitations:

› **Cyber-risk rating tools track your third parties, and more.** In addition to tracking the security of your firm's third-party partners, these products can help you continuously monitor your own environment for cyber risk, track your third parties' third parties (i.e., fourth parties), or run single-firm reports for initiatives such as due diligence or board reporting. Some enterprise customers even use their own cyber-risk ratings for their client prospecting and sales meetings.[3]

› **They produce risk indicators, not certainty.** Recall your high school statistics teacher's voice: "Correlation does not equal causation." Even the most sophisticated risk modeling can't generate perfect fidelity, and cybersecurity risk ratings are no different. They offer valuable risk insight about your third-party security posture, which will help you to better track partners' activity, uncover potential exposures, and prioritize mitigation efforts accordingly. But none of the solutions in the market are 100% accurate, nor do they offer complete visibility of risk.

› **Their value rests on consistency and context.** To provide data that helps you make better decisions, ratings tools have to use consistent methodologies and algorithms over time, and they have to provide information that's contextual to your organization and the third parties you work with. This may include data and analysis for more accurate attribution to associate businesses with their actual IT assets or more granular detail of a parent company's operating model and its dozen subsidiaries and regional offices.

Cybersecurity Risk Rating Solutions 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 nine vendors in this assessment: BitSight, FICO, iTrust, NormShield, Panorays, Prevalent, RiskRecon, SecurityScorecard, and UpGuard (see Figure 2 and see Figure 3). Each of these vendors has:

› **Functionality to collect and analyze data from surface, deep, and dark web channels.** The participating vendors all offer capabilities to continually collect and analyze data from a wide range of surface, deep, and dark web channels, as well as other relevant security data and threat intelligence.

› **Capabilities to perform entity attribution and risk analysis of organizations worldwide.** All evaluated solutions apply various analytical techniques to accurately and efficiently build profiles of organizations' external digital footprint, such as relevant digital assets, infrastructure, and intellectual property. Based on additional context and relevant metadata, these solutions can automatically calculate a cyber-risk score for each of these subattributes.

› **A consistent rating methodology to dynamically generate cyber-risk scores.** As a foundational piece of their product offering, all participating vendors maintain a rating methodology that can measure and score any organization's cyber-risk exposure based on a consistent set of underlying parameters. In addition, the solutions all dynamically update cyber-risk ratings for all covered (i.e., evaluated) third parties as they collect new intelligence. Solutions that only generate ad hoc, "snapshot" reports do not meet this requirement.

› **A clear focus on third-party cyber-risk use cases serving multiple industries.** One of the primary use cases of these cyber-risk rating solutions must be to support security teams' third-party and vendor risk management efforts. The vendor must support customer organizations in multiple industries.

› **Demonstrated success and market relevance.** The cyber-risk rating solutions evaluated in this report are all standalone product offerings with an active, growing enterprise customer base and a market presence strong enough to appear in competitive situations in the market and among Forrester clients.

FIGURE 1 Assessment Criteria

Criteria	Platform evaluation details
Surface and deep web intelligence	How well does the vendor collect and normalize data from surface and deep web channels? How robust and differentiated are the vendor's other open and surface web data sources and APIs? How does the vendor measure the efficacy of this collection strategy?
Dark web and technical intelligence	How well does the product collect data from closed criminal or otherwise nefarious darknets, marketplaces, and chat rooms? To what extent does the tool collect data from threat feeds, security reporting, and other technical sources (e.g., malware, CVEs, phishing data, etc.)?
Risk analysis and attribution	How well does it build and maintain accurate profiles of organizations and their associated digital footprints? How well does the solution correlate these attributes to cybersecurity hygiene and exposure to cyberattacks? How well does it calculate, classify, and prioritize risk?
Rating efficacy and transparency	How does the vendor ensure its cyber-risk rating methodology maintains a strong, statistically significant correlation to real-life cyber-risk exposure and events? To what degree is the ratings methodology accurate and transparent to all customers and noncustomers?
Internal and enterprise risk context	To what extent can the solution integrate additional risk context about third parties with internal security and risk data (e.g., via SIEMs, GRC platforms, etc.)? To what extent does it provide enterprise, noncybersecurity risk context about third parties (e.g., financial, reputational, and regulatory)?
Risk assessments and review portal	To what extent can customers develop and distribute their own risk assessments and questionnaires? How well does the product facilitate collaboration and communication between customers and third parties, including suggested action and remediation plans?
Dashboard and alerts	To what extent can the product generate reports and dashboards of system risk data for different audiences? To what degree can users tailor business and risk weightings for their unique risk requirements (e.g., severity, business criticality, risk type, etc.)?
Vision and execution	How well does the vendor articulate a clear vision of the future of the cyber-risk ratings market? Is it well positioned to capitalize on this vision? Does it have a strong track record of innovation, and how well is it positioned to grow its commitment to product development and R&D?
Global reach	How well does the vendor support global customers in terms of native-speaking analysts, regional offices, and specialized analytics or IP? How many risk and threat analysts are dedicated to ongoing risk analysis and threat intelligence activities, and which languages do they support?
Thought leadership and strategic partnerships	To what extent does the vendor produce content and thought leadership to maintain an active presence in the market? How does the vendor differentiate from competitors through proprietary features, patents, and IP, as well as strategic partnerships?

FIGURE 2 Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018

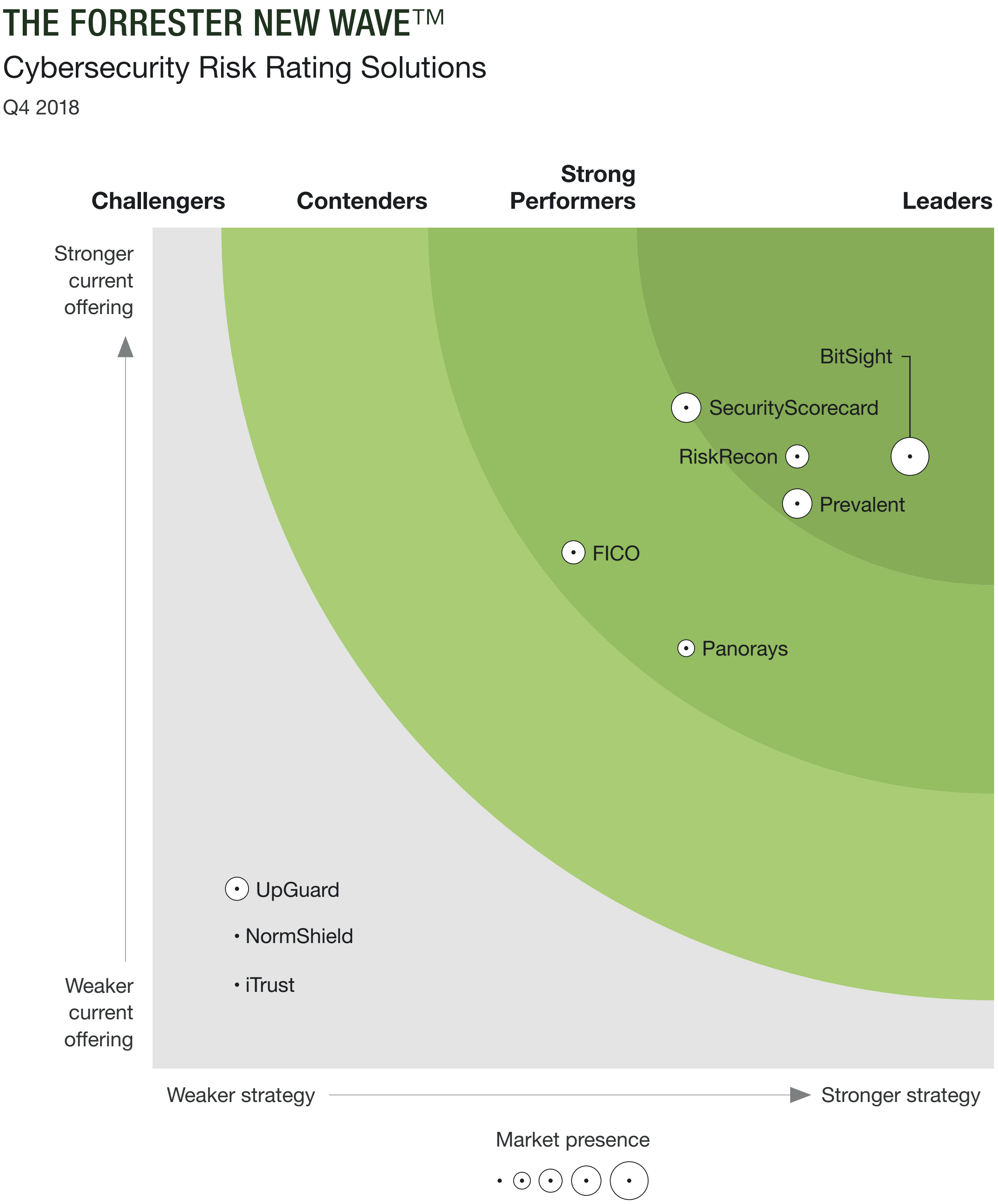


FIGURE 3 Vendor QuickCard Overview

Company	Surface and deep web intel.	Dark web and technical intel.	Risk analysis and attribution	Rating efficacy and transp.	Internal and enterprise risk context	Risk assess./review portal	Dashboard and alerts	Vision and execution	Global reach	Thought leadership and strategic partnerships
BitSight	⌃	⌃	=	⌃	=	=	⌃	⌃	⌃	⌃
RiskRecon	=	⌃	⌃	=	⌃	⌃	=	⌃	=	⌃
Prevalent	=	=	⌃	=	⌃	⌃	=	⌃	⌃	=
SecurityScorecard	⌃	⌃	⌃	⌃	=	=	⌃	=	=	⌃
Panorays	⌄	=	=	=	⌃	⌃	⌄	=	⌃	=
FICO	⌃	=	=	⌃	⌄	=	⌃	=	=	=
UpGuard	=	⌄	⌄	⌄	⌄	⌄	=	⌄	⌄	⌄
NormShield	⌄	⌄	⌄	⌄	=	⌄	⌄	⌄	⌄	⌄
iTrust	⌄	⌄	⌄	⌄	⌄	⌄	⌄	⌄	⌄	⌄

⌃ Differentiated = On par ⌄ Needs improvement

Vendor QuickCards

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

BitSight: Forrester's Take

Our evaluation found that BitSight (see Figure 4):

- **Leads the pack with a reliable rating methodology and flexible platform.** BitSight's name is well-known and respected in this budding market, and it offers one of the strongest platforms in terms of scale, reach, and partner network. BitSight places a premium on the accuracy of its ratings, incorporating strong data model governance practices and third-party validation of its scoring methodology.
- **Needs to flesh out its risk assessment and contextual analysis capabilities.** It offers native integration with several GRC platforms to incorporate its data into risk management workflows.[4] But how customers can incorporate internal risk context in the tool is limited.
- **Is the best fit for companies that want an established, well-developed solution.** S&R pros will find value in sharing a common view with many of their industry peers and partners who also use BitSight as well as detailed and flexible dashboards.

BitSight Customer Reference Summary

Customers praise BitSight's broad industry adoption and intuitive UI but note some instances of high alert and false-positive rates due to errors in its business and IT asset attribution.

FIGURE 4 BitSight QuickCard

BitSight

Wave position
LEADER

- ⌃ **Surface/deep web intel.**
- ⌃ **Dark web/technical intel.**
- = **Risk analysis/attribution**
- ⌃ **Rating efficacy/transp.**
- = **Internal/enterprise risk context**
- = **Risk assess./rev. portal**
- ⌃ **Dashboard/alerts**
- ⌃ **Vision/execution**
- ⌃ **Global reach**
- ⌃ **Thought leadership/ strategic partnerships**

⌃ Differentiated = On par ⌄ Needs improvement

REFERENCE QUOTES

"Industrywide acceptance and an intuitive UI made BitSight an easy choice for us."

"Its action-plan tracking helps us stay on top of our vendors to make sure they follow through."

Products evaluated
BitSight Security Ratings

RiskRecon: Forrester's Take

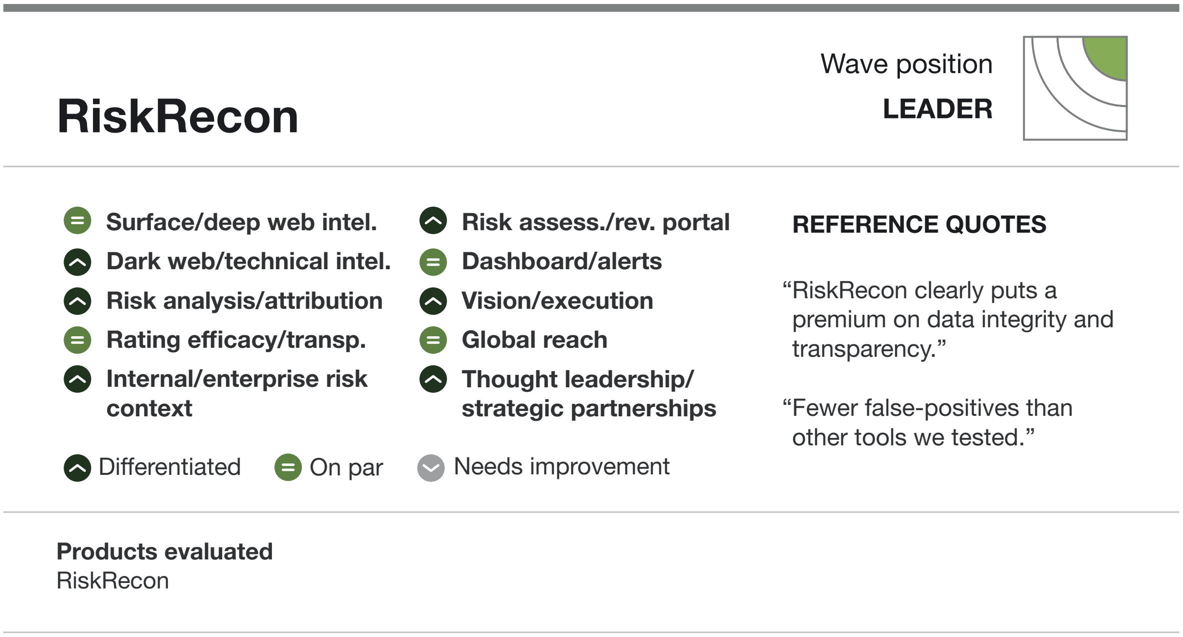
Our evaluation found that RiskRecon (see Figure 5):

- **Leads the pack with robust risk analysis, assessments, and context.** RiskRecon stands out with its focus on contextualized, action-oriented cyber-risk ratings. Its Risk Priority Matrix tool helps customers narrow down, prioritize, and take action on their top third-party cyber risks based on their unique business assets and security posture. Once prioritized, RiskRecon applies AI to suggest mitigation steps and facilitate action plans.
- **Needs further validation of its ratings efficacy and accuracy.** RiskRecon is still fairly untested and needs to run more open and detailed analysis to validate its ratings efficacy.
- **Is the best fit for S&R pros that want contextualized cyber-risk ratings.** S&R pros who want to understand and prioritize third-party cyber risks based on their own unique business needs and threat landscape should add RiskRecon to their shortlist.

RiskRecon Customer Reference Summary

RiskRecon customers extol the tool's low false-positive rates and the value of its integrated mitigation plans. They want to see improvements to reporting and vendor collaboration features.

FIGURE 5 RiskRecon QuickCard



RiskRecon

Wave position
LEADER

= **Surface/deep web intel.**
⌃ **Dark web/technical intel.**
⌃ **Risk analysis/attribution**
= **Rating efficacy/transp.**
⌃ **Internal/enterprise risk context**

⌃ **Risk assess./rev. portal**
= **Dashboard/alerts**
⌃ **Vision/execution**
= **Global reach**
⌃ **Thought leadership/ strategic partnerships**

⌃ Differentiated = On par ⌄ Needs improvement

REFERENCE QUOTES

"RiskRecon clearly puts a premium on data integrity and transparency."

"Fewer false-positives than other tools we tested."

Products evaluated
RiskRecon

Prevalent: Forrester's Take

Our evaluation found that Prevalent (see Figure 6):

- **Leads the pack with a third-party risk management platform.** Prevalent aims to support all third-party risk management (TPRM) functions. The product provides some common GRC platform capabilities (e.g., risk assessments, workflow, and reporting), and it overlays customer-collected data with its own risk intelligence to generate three core risk scores for each third party: "cyber," "business," and "assessment."
- **Needs to work on platform flexibility, technical integration, and partnerships.** Prevalent is largely a closed system, with no pre-built integrations or formal partners. It has a public API for customer integration, but connectivity to S&R tools is otherwise limited.
- **Is best for companies that want one TPRM tool with integrated cyber-risk ratings.** Given its robust risk intelligence and comprehensive risk management features, Prevalent is a worthy option for S&R pros seeking one tool for all cyber TPRM activities.

Prevalent Customer Reference Summary

Customers commend Prevalent for its wide range of capabilities and breadth of vendor risk data. They cite the platform's difficult navigation and limited reporting as top areas for improvement.

FIGURE 6 Prevalent QuickCard

Prevalent

Wave position
LEADER

= **Surface/deep web intel.**	⌃ **Risk assess./rev. portal**
= **Dark web/technical intel.**	= **Dashboard/alerts**
⌃ **Risk analysis/attribution**	⌃ **Vision/execution**
= **Rating efficacy/transp.**	⌃ **Global reach**
⌃ **Internal/enterprise risk context**	= **Thought leadership/ strategic partnerships**

⌃ Differentiated = On par ⌄ Needs improvement

REFERENCE QUOTES

"No other tool matched the breadth and depth of its data and risk domain coverage."

"Rapid alerts and ratings updates."

Products evaluated
Prevalent TPRM Platform

SecurityScorecard: Forrester's Take

Our evaluation found that SecurityScorecard (see Figure 7):

- **Leads the pack with robust collection and risk analysis.** SecurityScorecard was one of the first to market with its cyber-risk rating tool. It continues to improve its capabilities at each phase of the cyber-risk rating process — including data collection, normalization, attribution, risk analysis, and scoring. Reports contain detailed summaries of third parties along with helpful mitigation suggestions to support customer reviews and action plans.
- **Needs to work on internal risk context and assessments.** SecurityScorecard partners with several GRC tool providers, but the product offers little functionality to supplement or facilitate any TPRM workflows itself.
- **Is best for S&R pros seeking well-curated data from a straightforward rating tool.** SecurityScorecard stands out for its core cyber-risk rating capabilities: data collection, rating efficacy and transparency, and vendor review and collaboration.

SecurityScorecard Customer Reference Summary

Customers praise SecurityScorecard's easy-to-understand methodology, intuitive UI, and unique data visualizations. They want to see business risk context and assessment capabilities improve.

FIGURE 7 SecurityScorecard QuickCard

SecurityScorecard

Wave position
LEADER

- ⌃ **Surface/deep web intel.**
- ⌃ **Dark web/technical intel.**
- ⌃ **Risk analysis/attribution**
- ⌃ **Rating efficacy/transp.**
- = **Internal/enterprise risk context**
- = **Risk assess./rev. portal**
- ⌃ **Dashboard/alerts**
- = **Vision/execution**
- = **Global reach**
- ⌃ **Thought leadership/ strategic partnerships**

⌃ Differentiated = On par ⌄ Needs improvement

REFERENCE QUOTES

"Great UI; compelling reporting and data visualization features."

"The scoring methodology is easy to understand and explain."

Products evaluated
SecurityScorecard Security Ratings Platform

Panorays: Forrester's Take

Our evaluation found that Panorays (see Figure 8):

› **Offers a competitive cyber-risk rating solution with well-rounded capabilities.** It aims to provide customers with an internal and external view of their third-party risk environment by coupling its cyber-risk ratings with tools for internal risk assessments, policy management, and risk prioritization. It also maps its results to security and industry standards (e.g., NIST, PCI/DSS, and GDPR) and runs simulations to assess risk related to user behavior.

› **Needs to keep investing in its data collection techniques and UI.** Founded in 2016, Panorays must keep expanding its open and closed source data collection to catch up with competitors in the space.

› **Is best for S&R pros that want a dedicated tool to conduct all cyber-TPRM activity.** S&R pros seeking a tool that provides solid cyber-risk ratings along with other TPRM features for cybersecurity will find Panorays an intriguing option.

Panorays Customer Reference Summary

Customers value the Panorays platform's ease-of-use and the combined internal and external visibility it enables. They cite API integration and vendor collaboration as top improvement areas.

FIGURE 8 Panorays QuickCard

Panorays

Wave position
STRONG PERFORMER

- ⌄ **Surface/deep web intel.**
- = **Dark web/technical intel.**
- = **Risk analysis/attribution**
- = **Rating efficacy/transp.**
- ⌃ **Internal/enterprise risk context**
- ⌃ **Risk assess./rev. portal**
- ⌄ **Dashboard/alerts**
- = **Vision/execution**
- ⌃ **Global reach**
- = **Thought leadership/ strategic partnerships**

⌃ Differentiated = On par ⌄ Needs improvement

REFERENCE QUOTES

"Deep threat analysis and an intuitive questionnaire-builder."

"Gives us a true 360-degree view of our vendor risk."

Products evaluated
Panorays Platform

FICO: Forrester's Take

Our evaluation found that FICO (see Figure 9):

- **Stands out with its sophisticated and reliable rating methodology.** As part of its June 2016 Quadmetrics acquisition, FICO obtained some of the foundational cyber-risk rating research and IP in the industry. Applying advanced analytics, strong model governance, and empirical breach and threat data, it ensures a rating spectrum in which the worst third-party scores are 24 times more likely to experience a cyber-risk event than those with top scores.
- **Needs better support for S&R practitioners.** FICO's capabilities are limited when it comes to supporting TPRM-related workflows, such as risk assessments, third-party coordination, and mitigation plans; few native integrations exist for GRC and security tools.
- **Is best for cyberinsurance and due diligence use cases.** FICO rivals or surpasses the competition when the primary objective is to assess the point-in-time and ongoing cyber-risk exposure of distinct entities and minimal use of risk management support or contextual data.

FICO Customer Reference Summary

Customers extol FICO for the accuracy and performance of its predictive cyber-risk data model. They hope for a simpler UI to support less-experienced cyberinsurance and risk manager users.

FIGURE 9 FICO QuickCard

FICO

Wave position
STRONG PERFORMER

⌃ **Surface/deep web intel.**
⊜ **Dark web/technical intel.**
⊜ **Risk analysis/attribution**
⌃ **Rating efficacy/transp.**
⌄ **Internal/enterprise risk context**

⊜ **Risk assess./rev. portal**
⌃ **Dashboard/alerts**
⊜ **Vision/execution**
⊜ **Global reach**
⊜ **Thought leadership/ strategic partnerships**

⌃ Differentiated ⊜ On par ⌄ Needs improvement

REFERENCE QUOTES

"The accuracy and performance of the data model are as close to predictive as they come."

"The depth and proficiency of the data science team is impressive."

Products evaluated
FICO Cyber Risk Score

UpGuard: Forrester's Take

Our evaluation found that UpGuard (see Figure 10):

- **Offers competitive technical collection and risk intelligence.** UpGuard made headlines a few times in the past year for its role in discovering high-profile data breaches, including the leaked voting data of 198 million US citizens and the microtargeting tools used in various Republican influence campaigns.[5] These discoveries showcase the intelligence capabilities UpGuard deploys as part of its cyber-risk scoring tool. Moreover, it offers solid reporting and alerts capable of aligning collected risk data to industry standards (e.g., ISO, PCI, and NIST).
- **Needs to work on its risk analytics and rating accuracy.** UpGuard offers little insight into how it validates rating accuracy and has limited features for users to measure risk.
- **Is the best fit for companies that want visibility into their cyberthreat landscape.** S&R pros less concerned about risk analysis and scoring who want real-time monitoring and quick detection of new exposures will find UpGuard an enticing solution.

UpGuard Customer Reference Summary

Customers praised UpGuard's reporting functionality and flexible customer support. They want to see improvements to the consistency of its collection and better insight into system vulnerabilities.

FIGURE 10 UpGuard QuickCard

UpGuard

Wave position
CHALLENGER

- ⊜ **Surface/deep web intel.**
- ⌄ **Dark web/technical intel.**
- ⌄ **Risk analysis/attribution**
- ⌄ **Rating efficacy/transp.**
- ⌄ **Internal/enterprise risk context**
- ⌄ **Risk assess./rev. portal**
- ⊜ **Dashboard/alerts**
- ⌄ **Vision/execution**
- ⌄ **Global reach**
- ⌄ **Thought leadership/ strategic partnerships**

⌃ Differentiated ⊜ On par ⌄ Needs improvement

REFERENCE QUOTES

"Intuitive UI with flexible tagging for vendor coordination."

"Every feature I request, they do it and go a step further."

Products evaluated
UpGuard CyberRisk

NormShield: Forrester's Take

Our evaluation found that NormShield (see Figure 11):

› **Covers the basics with its cyber-risk rating tool.** NormShield runs quick assessments to determine almost any firm's cyber-risk posture. Its collection and scoring include core cyber-risk components like patch management, SSL strength, website security, DNS health, IP reputation, and brand and app monitoring.[6] Users can delve into the analysis to view identified assets, risks, and mitigation advice and can generate reports based on the details.

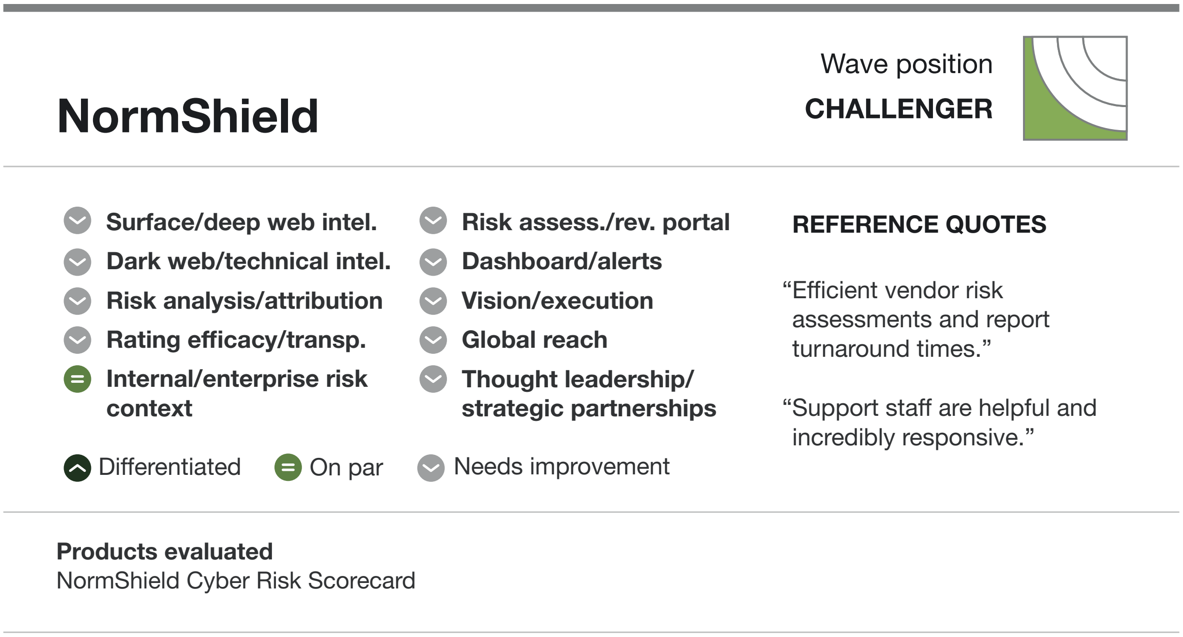
› **Primarily runs one-time reports.** Customers license NormShield based on the number and frequency of reports they want to run, which often means more static, time-based views and gaps in real-time monitoring and event detection. Risk management features are also limited.

› **Will mostly meet the needs of small and medium enterprises.** S&R pros with more restricted security budgets will find value in the flexibility, breadth, and cadence of the third-party cyber-risk reports they can request with NormShield.

NormShield Customer Reference Summary

Customers highlighted NormShield's rapid turnaround time for both reports and customer support. They called out some issues with high false-positive rates and inexact business attribution.

FIGURE 11 NormShield QuickCard



NormShield

Wave position
CHALLENGER

- ⌄ **Surface/deep web intel.**
- ⌄ **Dark web/technical intel.**
- ⌄ **Risk analysis/attribution**
- ⌄ **Rating efficacy/transp.**
- = **Internal/enterprise risk context**

- ⌄ **Risk assess./rev. portal**
- ⌄ **Dashboard/alerts**
- ⌄ **Vision/execution**
- ⌄ **Global reach**
- ⌄ **Thought leadership/ strategic partnerships**

⌃ Differentiated = On par ⌄ Needs improvement

REFERENCE QUOTES

"Efficient vendor risk assessments and report turnaround times."

"Support staff are helpful and incredibly responsive."

Products evaluated
NormShield Cyber Risk Scorecard

iTrust: Forrester's Take

Our evaluation found that iTrust (see Figure 12):

- **Aims to provide a 360-degree view of third-party cyber risk.** iTrust offers the core functionality of a cyber-risk rating solution, incorporating standard open source and technical data collection and basic risk scoring. It allows customers to add third-party risk context using canned questionnaires that map to regulations (e.g., NIST) and to field reputation surveys to other customers of the selected third parties.
- **Needs to work on its core offering.** iTrust seeks to differentiate with features for reputation and breach monitoring, yet it falls well short in core functionality (e.g., data collection, risk analysis, attribution, and rating efficacy), let alone in standing out from the competition.
- **Is the best fit for companies willing to experiment.** It's still early days for iTrust's cyber-risk rating tool, but it has a team of experienced security analysts and consultants that can keep development on the right trajectory.

iTrust Customer Reference Summary

Customers point to iTrust's real-time monitoring as one of its top strengths, and they cite better third-party onboarding and automated email alerts as top areas they want to see improved.

FIGURE 12 iTrust QuickCard

iTrust

Wave position
CHALLENGER

⌄ **Surface/deep web intel.**
⌄ **Dark web/technical intel.**
⌄ **Risk analysis/attribution**
⌄ **Rating efficacy/transp.**
⌄ **Internal/enterprise risk context**

⌄ **Risk assess./rev. portal**
⌄ **Dashboard/alerts**
⌄ **Vision/execution**
⌄ **Global reach**
⌄ **Thought leadership/ strategic partnerships**

^ Differentiated = On par ⌄ Needs improvement

REFERENCE QUOTES

"We saw immediate results from iTrust's real-time vendor risk monitoring."

"Required little effort to get up and running and to maintain."

Products evaluated
iTrust Cyber Risk Ratings

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.

Endnotes

[1] Source: Forrester's Q4 2018 Cybersecurity Risk Rating Solutions Forrester New Wave™ Customer Reference Survey.

[2] Base: global enterprise network path security decision makers who had experienced a breach in the past 12 months at the time of being surveyed. Source: Forrester Analytics Global Business Technographics® Security Survey, 2018 and Forrester Analytics Global Business Technographics Security Survey, 2017.

[3] We should note that cyberinsurance is also a common use case. Insurers are major customers of many of these vendors, but we evaluated vendors in this Forrester Wave based on the capabilities they offer to enterprise and government customers in which the primary users are primarily IT, security, and risk practitioners.

[4] GRC stands for governance, risk, and compliance.

[5] Source: Stephanie Condon, "Data breach exposes Cambridge Analytica's data mining tools," ZDNet, March 27, 2018 (https://www.zdnet.com/article/data-breach-exposes-cambridge-analyticas-data-mining-tools/).

[6] SSL stands for Secure Sockets Layer, DNS for domain name system, and IP for internet protocol.

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.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.