The Forrester Wave™: Vulnerability Risk Management, Q1 2018

Tools And Technology: The Security Architecture And Operations Playbook

by Josh Zelonis

March 14, 2018

Why Read This Report

In our 22-criteria evaluation of vulnerability risk management (VRM) providers, we identified the 12 most significant ones — Beyond Security, BeyondTrust, Digital Defense, IBM, Kenna Security, NopSec, Qualys, Rapid7, Skybox Security, Symantec, Tenable, and Tripwire — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways

Rapid7, BeyondTrust, Qualys, And NopSec Lead The Pack

Forrester's research uncovered a market in which Rapid7, BeyondTrust, Qualys, And NopSec lead the pack. Tenable, IBM, Digital Defense, Skybox Security, and Symantec offer competitive options. Kenna Security, Tripwire, and Beyond Security lag behind.

Security And Risk Pros Are Looking For Capabilities Beyond Enumeration

The vulnerability risk management market is growing because more S&R professionals see VRM as a way to address their top challenges. This market growth is, in large part, due to the fact that S&R pros increasingly trust VRM providers to act as strategic partners, advising them on top vulnerability and risk decisions.

Visibility, Priority, And Context Are Key Differentiators

As legacy vulnerability-scanning technology becomes outdated and less effective, presentation of risk as a function of vulnerabilities will dictate which providers lead the pack. Vendors that can provide risk-aware intelligence; superior remediation capabilities; and clear, meaningful reporting position themselves to successfully deliver clarity, oversight, and control to their customers.

The Forrester Wave™: Vulnerability Risk Management, Q1 2018

Tools And Technology: The Security Architecture And Operations Playbook

by Josh Zelonis
with Stephanie Balaouras, Bill Barringham, and Diane Lynch

March 14, 2018

Table Of Contents

Related Research Documents

The Forrester Wave™: Governance, Risk, And Compliance Platforms, Q1 2018

Lessons Learned From The World's Most Notable Privacy Abuses And Security Incidents, 2017

Vendor Landscape: Vulnerability Management, 2017

FORRESTER®

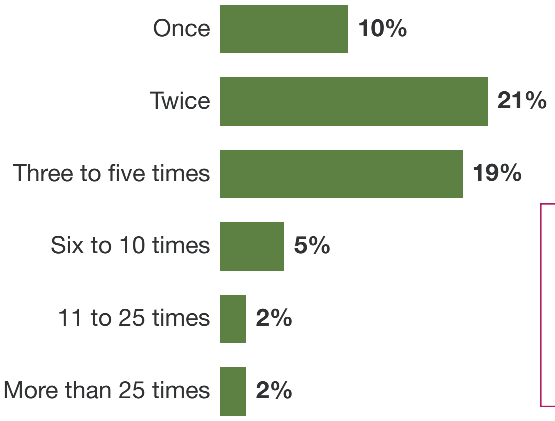
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Vulnerability Management Is Risky Business

According to Forrester's data, we're standing on a precipice where 58% of enterprise organizations suffered a breach at least once in the past year, and over 41% of those external breaches exploited some manner of software vulnerability (see Figure 1).[1] The increasing complexity of our ever-changing environments has outpaced our ability to maintain them using traditional vulnerability management techniques.[2] For this reason, Forrester has endeavored to reframe the S&R discussion around vulnerability management to become one of understanding and prioritizing risk.

FIGURE 1 Many Enterprises Are Dealing With Security Breaches

"How many times do you estimate that your firm's sensitive data was potentially compromised or breached in the past 12 months?"



In cases involving an external breach, 42% were carried out via a web application and 41% via a software vulnerability.*

Base: 604 global network security decision makers at firms with 1,000+ employees

*Base: 245 global network security decision makers at firms with 1,000+ employees that have had an external security breach in the past 12 months

Note: These results do not show the "no breaches in the past 12 months" or "don't know" responses.

Source: Forrester Data Global Business Technographics® Security Survey, 2017

VRM Requires More Than Identifying Vulnerable Systems

Traditionally, vulnerability management vendor selection has centered around a vendor's ability to enumerate vulnerabilities in an environment with low false-positive reporting. While acquisition of vulnerability data is an essential part of helping S&R professionals understand their security posture, it's only one piece of the VRM process (see Figure 2).[3] Forrester has identified four additional areas as critical to a mature vulnerability risk management capability.

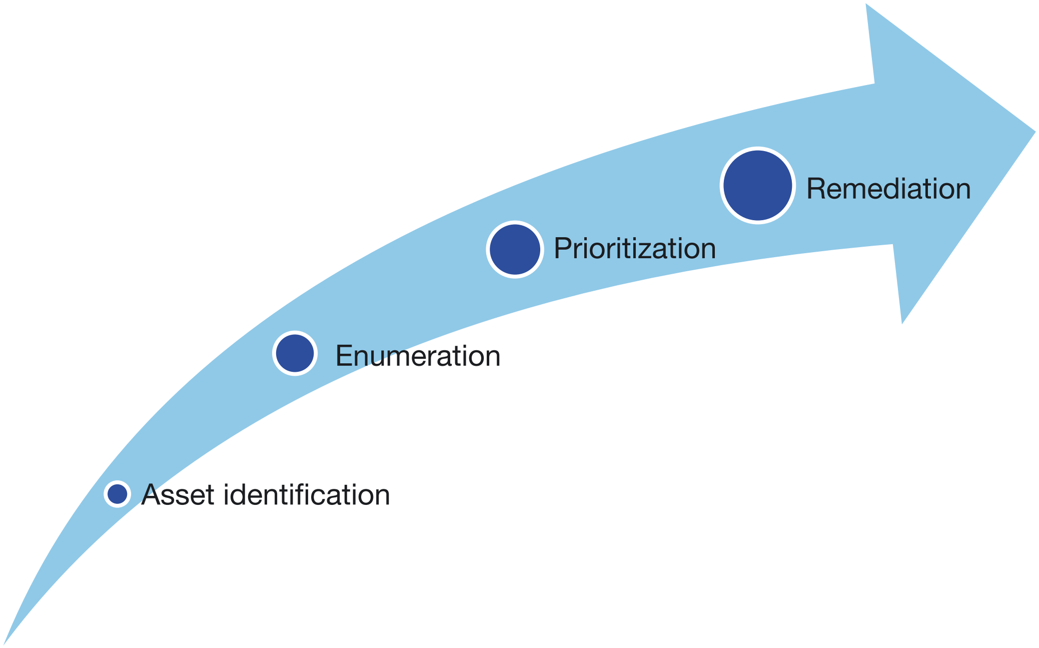
- **Asset management is the foundation of a mature VRM capability.** Without knowing what's in your environment, you have no hope of securing it. While teams can scan an environment and hope to find vulnerable assets, system criticality is key to understanding the potential impact of these risk exposures. A prerequisite for a mature VRM capability is understanding what's in the environment and the criticality of those systems.

- **Patch prioritization must extend beyond vulnerability scores.** Organizations must consider the confidentiality, integrity, and availability requirements of a system when prioritizing remediation. Remediation of any given vulnerability may require testing and downtime and, in some cases, will even require custom code. Understanding that VRM isn't a game of whack-a-mole is critical to building a mature process.

- **Threat intelligence provides an additional pathway for strategic patching.** Threat intelligence plays two important roles in a VRM program: 1) helping security teams focus on frequently targeted exposures and 2) communicating the urgency of prioritizations. Many security teams are focused on how they can use threat intelligence to detect attacks, but many attacks can be effectively neutered with the use of strategic patching.[4] Threat intelligence adds this extra dimension to prioritization.[5]

- **Reporting capabilities facilitate your ability to identify procedural vulnerabilities.** It's not enough to enumerate the vulnerabilities of a group of systems. Risk exposure metrics are critical to measuring the risk associated with an organization's operational footprint and allow prioritization of security sensitive systems.[6] Further, the ability to effectively track service level adherence over time is an important baseline for measuring and communicating the effectiveness of a VRM program.

FIGURE 2 The Vulnerability Risk Management Process



Vulnerability Risk Management Evaluation Overview

To assess the state of the vulnerability risk management market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top VRM vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 22 criteria, which we grouped into three high-level buckets:

- **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, asset management, patch prioritization, and reporting capabilities.
- **Strategy.** Placement on the Wave's horizontal axis indicates the strength of vendors' strategies. We evaluated product vision, road map, and market approach.
- **Market presence.** Represented on the Wave graphic by the size of each vendor's bubble, our market presence scores reflect each vendor's product revenue and number of VRM clients.

Evaluated Vendors And Inclusion Criteria

Forrester included 12 vendors in the assessment: Beyond Security, BeyondTrust, Digital Defense, IBM, Kenna Security, NopSec, Qualys, Rapid7, Skybox Security, Symantec, Tenable, and Tripwire. Each of these vendors has (see Figure 3):

- **Remediation prioritization based on threat intelligence.** We included vendors that help their clients remediate vulnerabilities, based on significant integration with one or more sources of threat intelligence.
- **Substantial enterprise level experience.** To be included, vendors needed at least 300 enterprise customers.
- **Significant mindshare with Forrester clients.** Forrester considered the level of interest from our clients based on our various interactions, including, but not limited to, inquiries, advisories, and consulting engagements.

FIGURE 3 Evaluated Vendors: Product Information And Inclusion Criteria

Vendor	Product name	Version number
Beyond Security	AVDS	7.12.10
BeyondTrust	Retina CS	6.3.1
Digital Defense	Frontline Vulnerability Manager	6.0
IBM	IBM QRadar Vulnerability Manager	7.3
Kenna Security	Kenna Security	N/A
NopSec	Unified VRM	4.6
Qualys	Threat Protection	N/A
Rapid7	InsightVM	6.5.6
Skybox Security	Skybox Security Suite: Vulnerability and Threat Management	8.5.600
Symantec	Symantec Control Compliance Suite	12.0
Tenable	Tenable.io	N/A
Tripwire	Tripwire IP360	8.1.2

Vendor inclusion criteria

1. Remediation prioritization based on threat intelligence. We included vendors that help their clients remediate vulnerabilities, based on significant integration with one or more sources of threat intelligence.

2. Substantial enterprise level experience. To be included, vendors needed at least 300 enterprise customers.

3. Significant mindshare with Forrester clients. Forrester considered the level of interest from our clients based on our various interactions, including, but not limited to, inquiries, advisories, and consulting engagements.

Vendor Profiles

We intend this evaluation of the vulnerability risk management market to be a starting point only and encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 4 and see Figure 5). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 4 Forrester Wave™: Vulnerability Risk Management, Q1 2018

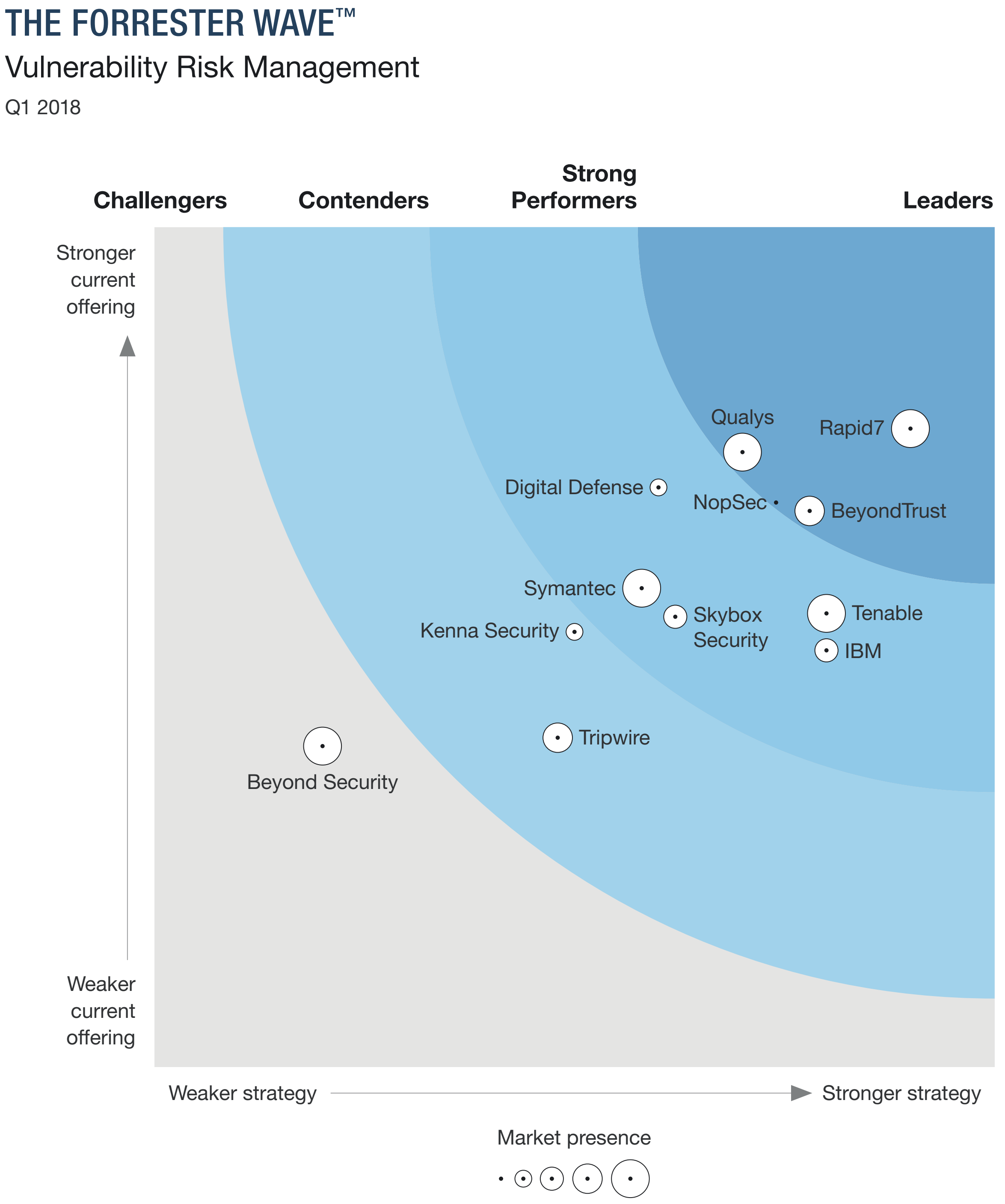


FIGURE 5 Forrester Wave™: Vulnerability Risk Management Scorecard, Q1 2018

	Forrester's weighting	Beyond Security	BeyondTrust	Digital Defense	IBM	Kenna Security	NopSec
Current offering	50%	1.91	3.31	3.45	2.48	2.59	3.36
Vulnerability enumeration	10%	2.40	3.60	3.70	3.60	2.30	2.50
Asset management	20%	2.00	3.00	4.00	3.00	2.00	3.00
Patch prioritization	20%	1.10	3.00	3.55	2.80	1.65	3.10
Reporting capabilities	20%	2.10	3.40	3.20	1.10	3.80	2.80
Security operations center (SOC) integration	5%	3.00	2.33	3.67	4.33	2.33	4.33
Solution usage	25%	1.90	3.80	3.00	2.10	3.00	4.45
Strategy	50%	1.00	3.90	3.00	4.00	2.50	3.70
Product vision	50%	1.00	4.00	3.00	5.00	2.00	4.00
Product road map	20%	1.00	5.00	3.00	3.00	3.00	1.00
Market approach	30%	1.00	3.00	3.00	3.00	3.00	5.00
Market presence	0%	5.00	4.00	2.00	3.00	2.00	1.00
Number of clients	50%	5.00	3.00	3.00	3.00	1.00	1.00
Product revenue	50%	5.00	5.00	1.00	3.00	3.00	1.00

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

FIGURE 5 Forrester Wave™: Vulnerability Risk Management Scorecard, Q1 2018 (Cont.)

	Forrester's weighting	Qualys	Rapid7	Skybox Security	Symantec	Tenable	Tripwire
Current offering	50%	3.66	3.80	2.68	2.85	2.70	1.96
Vulnerability enumeration	10%	3.80	4.00	1.70	3.00	4.40	3.10
Asset management	20%	4.00	4.00	1.00	3.00	2.00	2.00
Patch prioritization	20%	3.90	4.55	4.10	2.55	2.30	1.40
Reporting capabilities	20%	4.00	2.80	2.50	3.40	2.10	1.60
Security operations center (SOC) integration	5%	3.00	4.33	4.33	3.00	3.67	3.00
Solution usage	25%	3.00	3.65	3.10	2.45	3.20	2.00
Strategy	50%	3.50	4.50	3.10	2.90	4.00	2.40
Product vision	50%	4.00	4.00	2.00	4.00	5.00	3.00
Product road map	20%	3.00	5.00	3.00	3.00	3.00	3.00
Market approach	30%	3.00	5.00	5.00	1.00	3.00	1.00
Market presence	0%	5.00	5.00	3.00	5.00	5.00	4.00
Number of clients	50%	5.00	5.00	1.00	5.00	5.00	3.00
Product revenue	50%	5.00	5.00	5.00	5.00	5.00	5.00

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

Leaders

› **Rapid7 has already implemented what VRM will look like in the future.** Rapid7's InsightVM solution has a dashboard that not only breaks out risk exposure quantitatively but also includes a prioritized list of active campaigns to which customers are exposed, allowing them to strategically patch in response to actual threat intelligence. Rapid7 leverages the same agent for endpoint detection and response (EDR) as well as VRM to ease deployment, management, and, most importantly, to marry all your endpoint data at the point of collection. There are some areas where the provider has traded functionality for ease of use, such as granular control over how to define system criticality, but these are the decisions that clients most often rave about.

- **BeyondTrust supports a robust set of features at an incredible price point.** The asset management and reporting capabilities of the BeyondInsight product differentiate by giving customers a holistic view of the security posture of all the groups within the organization; the service-level agreement (SLA) reporting even has an email subscription capability so stakeholders can have regular updates without logging into the dashboard. Client feedback is positive with regard to BeyondTrust's responsiveness to both feature requests and support issues, and professional services are available as needed. If you're looking for a cost-effective solution for scanning your infrastructure with risk and compliance reporting, this is an excellent choice.

- **Qualys has a powerful combination of reporting capabilities.** Qualys utilizes a concept that it markets as real-time threat indicators and that allows customers to intuitively configure prioritization based on specific concerns they may have regarding a group of systems. This provider also integrates a threat intelligence feed that helps customers stay abreast of exploit trends to further ensure that they understand the threat landscape and are prioritizing effectively. Interestingly, the majority of clients we spoke with are leveraging only limited use cases in a product with a shocking amount of functionality — a gap in usage that can't be explained away by cost and is more easily attributed to exposure.

- **NopSec is a strategic choice for expanding VRM capabilities.** NopSec has an excellent understanding of the market and differentiates by offering its VRM capabilities, with or without its native scanning functionality, at compelling price points to provide value to any VRM implementation. Clients have granular control over defining system criticality, which in turn informs risk exposure scores that the platform presents well. One glaring weakness is NopSec's inability to define or track SLAs, but its bidirectional ticketing system integrations would allow customers to track those metrics elsewhere.

Strong Performers

- **Tenable excels in ease of deployment and vulnerability enumeration.** Tenable has a vision for building a "cyber exposure" platform that integrates VRM into development and operations (DevOps) processes to help organizations keep pace with their ever-changing environments. While this report surfaces Tenable's attention to vulnerability enumeration in both information technology and operational technology environments, its road map for 2018 focuses on bringing threat intelligence and risk to the forefront.

- **IBM offers integrated vulnerability management with BigFix, QRadar, and X-Force.** IBM approaches the QRadar Vulnerability Manager (QVM) as the next logical step for VRM, using QRadar to contextualize risk and simultaneously leveraging vulnerability information to identify exploitation. Similarly, IBM leverages X-Force Intelligence to show clients what campaigns they're currently vulnerable to and allows them to dig into that intelligence to prioritize remediation and deploy patches with BigFix. Client feedback is positive and indicates that a lot of the challenges of developing an integrated system such as this have stabilized into a very functional product.

- **Digital Defense is a deeply integrated VRM solution with an eye on ease of use.** Digital Defense focuses on building the best scanning platform out there, emphasizing business requirements such as data residency and a user interface design that's as easy as scheduling an Outlook meeting. One of Digital Defense's most popular features is its analyst-on-demand service, which lets clients engage the research team directly with questions about vulnerability exposures, allowing them to get the answers they need before meeting with the board to talk about the next Meltdown or Spectre.[7]

- **Skybox Security sets up a federated system for asset management and VRM.** Skybox Security combines network modeling with attack simulation to more accurately understand the exposure of a particular vulnerability for prioritizing and understanding risk. Skybox's total solution includes firewall management and compliance auditing and even hooks into Microsoft's SCCM.[8] Clients are positive about the end results but caution that it's best to be "all in" with Skybox to realize the full benefits of the platform. This is a powerful solution, but it's expensive from a licensing and management perspective.

- **Symantec partners to offer a VRM module in its risk management platform.** Symantec has a number of policy and risk management modules in its Control Compliance Suite (CCS) that deserve attention beyond the Vulnerability Manager, which it chose to highlight. Client feedback is positive for the CCS Vulnerability Manager, but this is an OEM product, so cost and support are noticeable concerns. Many organizations are happy making these concessions to work with a single portfolio vendor, and Symantec has an excellent product to work with.

Contenders

- **Kenna Security leverages threat intelligence and machine learning.** While Kenna Security frequently leads with messaging around threat intelligence, the vendor is really leveraging it on its end to quantify risk for its customers — without ever letting them see behind the curtain. A common theme when speaking with clients is how transformative this product has been for their organizations, although they see cost and enterprise scalability as challenges. This offering is an excellent choice if you need help tracking risk metrics or are looking for a platform to compute patch prioritization.

- **Tripwire offers a powerful, customizable risk-ranking system.** Functionally, IP360 is excellent at allowing clients to group assets and set sensitivities that get combined with vulnerability details to create a risk rating. The challenge is that the way this provider has implemented risk prioritization is so unique and flexible that it could easily become a nightmare to manage or could even impede skills transfer between different organizations that may use different scales for labelling sensitivity. Perhaps consequently, the product tends to be most popular when customers deploy it in limited use cases.

Challengers

- **Beyond Security tries to take the decision-making process out of threat prioritization.** In spite of offering a lot of the core functionality that clients look for in a VRM product, this feels like the same product it was 10 years ago. Nowhere is this more painfully obvious than the SecuriTeam threat intelligence portal, which Beyond Security isn't integrating into the platform; seems to be actively exploiting, based on the hex encoding in some of the blog titles; and is monetizing with advertisements. Beyond Security is responsive to clients when it comes to support and feature requests but suffers from a lack of investment. This vendor has fallen behind the pack.

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

The online version of Figure 4 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at the beginning of this report on Forrester.com to download the tool.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by February 28, 2018.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted or attempted to conduct reference calls with three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate or contributed only partially to the evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, please visit The Forrester Wave™ Methodology Guide on our website.

Integrity Policy

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

Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2017 was fielded between May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Data's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Data's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] We asked 604 global network security decision makers at firms with 1,000-plus employees, "How many times do you estimate that your firm's sensitive data was potentially compromised or breached in the past 12 months?" We asked 245 global network security decision makers at firms with 1,000-plus employees that have had an external security breach in the past 12 months, "How was the external attack carried out?" Source: Forrester Data Global Business Technographics Security Survey, 2017.

When software vulnerabilities are the leading attack vector for external breaches, it's clear that security teams must stop struggling with spreadsheets and homegrown vulnerability management tools. There are commercial offerings that simplify your life by coalescing scanner data, tying in threat intelligence to help you quantify risk, and communicating prioritization to the relevant teams for remediation. See the Forrester report "Vendor Landscape: Vulnerability Management, 2017."

[2] We asked 1,700 global security decision makers at firms with 1,000-plus employees, "Which of the following are the biggest information/IT security challenges for your firm?" Forty-one percent of respondents selected "the changing/evolving nature of IT threats (internal and external)." Source: Forrester Data Global Business Technographics Security Survey, 2017.

See the Forrester report "Lessons Learned From The World's Most Notable Privacy Abuses And Security Incidents, 2017."

[3] See the Forrester report "Define And Articulate The Role Of Risk Management."

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

[5] See the Forrester report "Vendor Landscape: External Threat Intelligence, 2017."

[6] See the Forrester report "Remove The Mystery From Security Metrics."

[7] Meltdown and Spectre are two critical flaws that affect billions of mobile phones, laptops, servers, and cloud services running on chips from suppliers, including AMD, ARM, and Intel. See the Forrester report "Quick Take: Fatal Chip Flaws Set Security Back Decades."

[8] SCCM is Microsoft's System Center Configuration Manager.

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.