The Forrester Wave™: Software Composition Analysis, Q2 2019

The 10 Providers That Matter Most And How They Stack Up

by Amy DeMartine
April 8, 2019

Why Read This Report

In our 33-criterion evaluation of software composition analysis providers, we identified the 10 most significant ones — Flexera, FOSSA, GitLab, JFrog, Snyk, Sonatype, Synopsys, Veracode, WhiteHat Security, and WhiteSource — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security professionals select the right one for their needs.

Key Takeaways

WhiteSource And Synopsys Lead The Pack

Forrester's research uncovered a market in which WhiteSource and Synopsys are Leaders; Snyk and Sonatype are Strong Performers; WhiteHat Security, Flexera, and Veracode are Contenders; and GitLab, FOSSA, and JFrog are Challengers.

Remediation, Policy Management, And Reporting Are Key Differentiators

As developers continue to use open source to accelerate the release of new application functionality, remediation, policy management, and reporting will dictate which providers will lead the pack. Vendors that can provide developers with remediation advice and even create patches position themselves to significantly reduce business risk.

The Forrester Wave™: Software Composition Analysis, Q2 2019

The 10 Providers That Matter Most And How They Stack Up

by Amy DeMartine
with Stephanie Balaouras, Kate Pesa, and Peggy Dostie
April 8, 2019

Table Of Contents

Related Research Documents

Application Security Market Will Exceed $7 Billion By 2023

Now Tech: Software Composition Analysis, Q1 2019

The State Of Application Security, 2019

FORRESTER®

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

SCA Is Critical To Secure Modern Application Development

Developers face the challenge of creating differentiated, customized, and compelling customer experiences quickly. As a result, they no longer write all of their own code to solve every problem. Instead, they assemble, configure, and automate their code and often rely on common open source components to quickly add application functionality. One recent study showed a 21% year-over-year increase in the average number of open source components across the study's evaluated codebase.[1] However, these same critical open source components continue to present a risk to businesses. A recent study shows that one in eight open source component downloads contained a known security vulnerability.[2] And worse, security pros now have even less time to identify and remediate any newly disclosed vulnerabilities, as the same study found that the time between vulnerability disclosure and exploit shrank from 45 days to three days.[3]

As a result of these trends, software composition analysis (SCA) customers should look for providers that:

- **Advise developers about how to remediate vulnerabilities.** To dramatically reduce the risk that vulnerabilities and risky licenses present, developers need to be notified early in their software delivery life cycle (SDLC) about the security or license risk and how to remediate it. Not only do SCA products need to generate good remediation advice, but some products produce fixes to the code to reference a safe version of an open source component or create patches when safe versions are unavailable.
- **Create consistent policies across different business units and application types.** To increase release speeds, security pros are evolving from being manual SCA testers to consistent policy makers. In this new role, they create companywide policies that all applications must meet (such as no known critical or serious vulnerabilities will be released into production) and raise this minimum bar for more-critical customer applications. To be effective, security pros need flexible policy management from their SCA tools.
- **Report on strategic risk for security pros and CISOs.** CISOs must remove roadblocks when applications begin to experience overly long remediation velocity or exhibit excessive risk. In the past, security pros cobbled this information together from vulnerability and license risk data or simply did without. Today, security pros require out-of-the-box reports for CISOs and development teams that describe the risk applications present to the business and how fast developers are able to remediate known vulnerability and license risk.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our reports on SCA.[4]

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

FIGURE 1 Forrester Wave™: Software Composition Analysis, Q2 2019

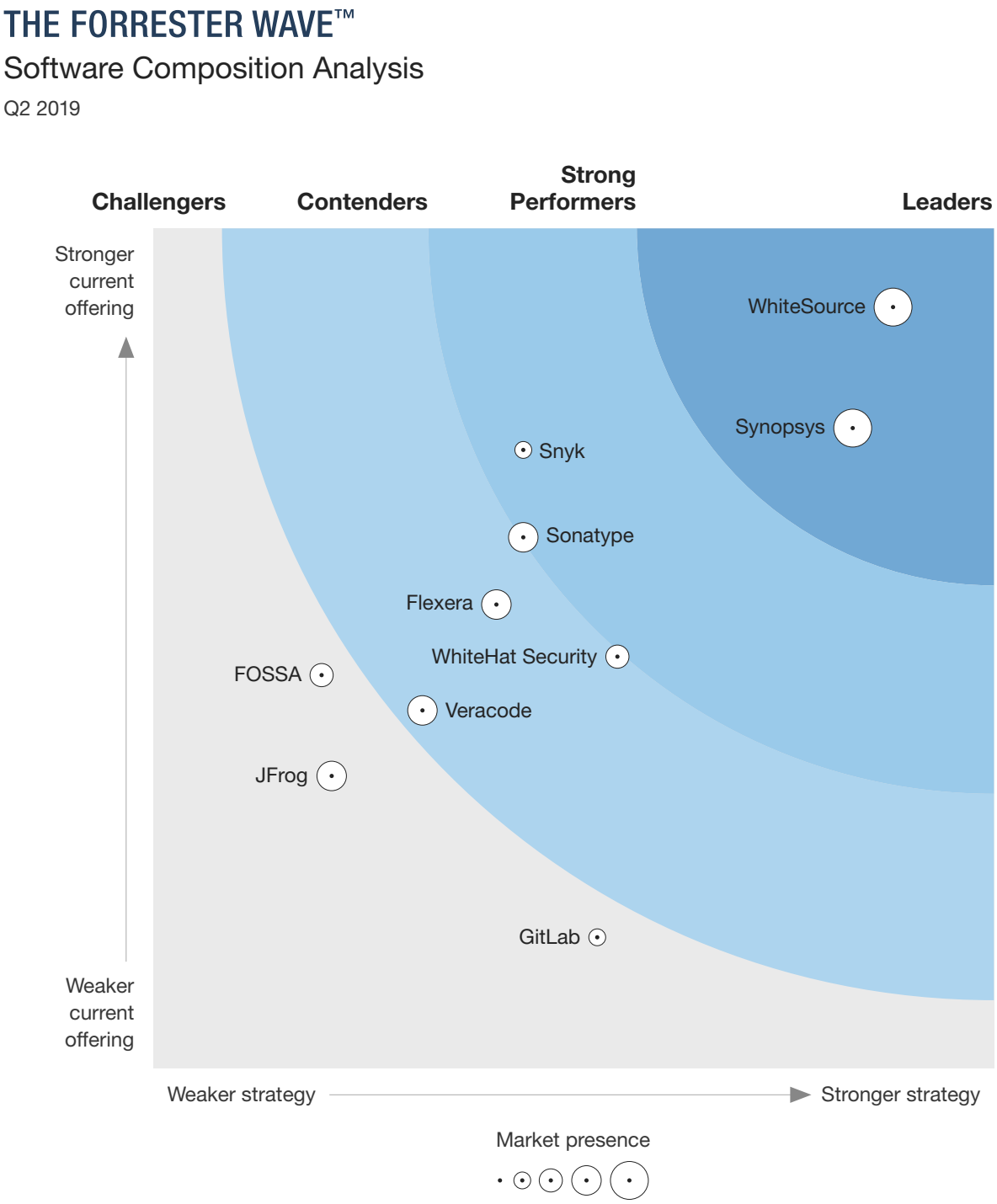

FIGURE 2 Forrester Wave™: Software Composition Analysis Scorecard, Q2 2019

	Forrester's weighting	Flexera	FOSSA	GitLab	JFrog	Snyk	Sonatype	Synopsys	Veracode	WhiteHat Security	WhiteSource
Current offering	50%	2.76	2.34	0.78	1.74	3.68	3.16	3.81	2.13	2.45	4.53
License risk management	10%	3.20	1.90	1.20	1.20	3.30	2.00	3.30	1.00	1.90	4.20
Vulnerability identification action	15%	2.60	1.80	0.90	1.30	4.00	2.70	3.50	2.00	1.80	4.50
Proactive vulnerability management	20%	3.20	2.80	0.60	2.20	5.00	2.20	4.40	3.80	3.60	3.80
Policy management	10%	2.60	2.60	0.60	0.60	3.40	4.20	5.00	1.80	1.20	5.00
SDLC integration	20%	2.50	2.30	0.80	3.60	4.10	3.70	5.00	2.95	3.35	4.60
Container and serverless scanning	5%	1.00	0.00	1.00	1.00	5.00	3.00	3.00	0.00	0.00	5.00
Audit reporting	4%	3.00	3.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	5.00
Risk reporting	9%	3.00	3.00	1.00	1.00	1.00	5.00	3.00	1.00	3.00	5.00
Remediation velocity reporting	5%	3.00	3.00	0.00	0.00	3.00	5.00	1.00	1.00	3.00	5.00
Vendor self-analysis	2%	3.00	3.00	0.00	1.00	3.00	3.00	3.00	1.00	1.00	5.00
Strategy	50%	2.04	1.00	2.64	1.06	2.20	2.20	4.16	1.60	2.76	4.40
Product strategy	30%	2.80	1.00	4.80	1.20	5.00	3.00	3.20	3.00	1.20	5.00
Market approach	25%	3.00	1.00	3.00	1.00	1.00	1.00	5.00	1.00	3.00	5.00
Execution road map	15%	1.00	1.00	1.00	1.00	1.00	1.00	3.00	1.00	1.00	5.00
Training	30%	1.00	1.00	1.00	1.00	1.00	3.00	5.00	1.00	5.00	3.00
Market presence	0%	3.96	2.98	1.88	3.20	2.00	3.40	4.50	3.28	2.50	4.16
Installed base	60%	3.60	1.80	1.80	4.00	2.00	5.00	5.00	4.80	2.00	4.60
Growth rate	10%	3.00	4.00	5.00	5.00	5.00	1.00	3.00	1.00	1.00	5.00
Corporate profitability	30%	5.00	5.00	1.00	1.00	1.00	1.00	4.00	1.00	4.00	3.00

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

Vendor Offerings

Forrester included 10 vendors in this assessment: Flexera, FOSSA, GitLab, JFrog, Snyk, Sonatype, Synopsys, Veracode, WhiteHat Security, and WhiteSource (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Products evaluated	Version
Flexera	FlexNet Code Insight	2019 R1
FOSSA	Compliance	1.8.0
GitLab	GitLab	11.6
JFrog	JFrog Xray	2.6
Snyk	Snyk	
Sonatype	Sonatype Nexus Platform: IQ Server Nexus Lifecycle Nexus Firewall Nexus Auditor Nexus Repository Nexus Vulnerability Scanner DepShield	 R57 R57 R57 R57 3.15 R57 1.22
Synopsys	Black Duck Black Duck Binary Analysis	2018.12.0 2018.09.0
Veracode	Veracode Software Composition Analysis SourceClear Software Composition Analysis	
WhiteHat Security	WhiteHat Sentinel SCA — Essentials Edition WhiteHat Sentinel SCA — Standard Edition	
WhiteSource	WhiteSource	18.12.1

Vendor Profiles

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

Leaders

› **WhiteSource reduces the time it takes to remediate through prioritization.** WhiteSource has recently introduced the ability to prioritize vulnerabilities by performing static scans to understand if the vulnerable part of a component is being directly called by the application. If it isn't, the vulnerability is deprioritized. Another recently released feature is to automatically remediate vulnerabilities by creating pull requests to upgrade to a version that complies with company policy.

Customers praise WhiteSource's broad language coverage and customer support but note that the product could do a better job of visualizing transitive dependencies. WhiteSource has very few weaknesses, but the bill of materials (BOM) functionality falls short, and to keep pace, WhiteSource will need to offer out-of-the-box comparison between current and historic BOMs. WhiteSource is best for companies that require scanning at the earliest points of the SDLC and are looking for prioritization and automatic remediation.

› **Synopsys capitalizes Black Duck acquisition with binary scanning and reporting.** Synopsys has consolidated all of its former SCA functionality into the Black Duck (Black Duck Hub and Protecode SC) product. However, for more complex license compliance practices, customers must also use Black Duck Protex and Black Duck. For example, you can analyze the difference between declared and detected licenses, but you must use two different tools to do it. Synopsys has other functionality to cover interactive and static scanning and has recently released its Polaris platform with the goal of combining all data from their prerelease scanning tools.

Customers credit Synopsys with scans that are fast and reliable with detailed remediation advice but feel that false positives seem high. Synopsys has very strong policy management and SDLC integrations and strong proactive vulnerability management, including a BOM compare feature that highlights what has changed over time. However, Synopsys falls short when it comes to autoremediation features that other top vendors include. Synopsys is best for companies that have application teams with exacting requirements of integrating in the SDLC and need differentiating policies for different types of applications.

Strong Performers

› **Snyk focuses on developer use cases to update versions and provide patches.** Snyk's goal is to enable developers to remediate vulnerabilities and, as a result, not only offers the ability to patch by creating pull requests but also offers custom patches when an acceptable version of a component is not available. Snyk also gives developers a call graph that shows transitive dependencies and associated vulnerabilities that their direct dependencies include, to help developers understand why certain patches are required.

Customers are excited about Snyk and its focus on the developer use case, including easy integration into the SDLC, autoremediation including its custom patching for vulnerabilities without an easy upgrade path, and visualization of dependencies. However, to complete the

developer experience, customers would like Snyk to be the go-to resource for open source knowledge with search information — even beyond security information — about all versions of a component to discover which version is the best fit. Snyk has focused so much on the developer use case that the security pro use case has been neglected, and Snyk needs to boost its out-of-the-box audit and risk reporting. Snyk is best for companies trying to lure reluctant developers to autoremediate vulnerabilities.

› **Sonatype continues to build on the Nexus platform for improved value.** Sonatype scans its own Nexus repository to hone its general vulnerability identification. Sonatype's research team then enhances the data associated with identified vulnerabilities with remediation steps and advice about configuration changes, component upgrade details, and code change requirements. The Nexus platform has several licenses for different functionality — DepShield, IQ Server, Nexus Auditor, Nexus Firewall, Nexus Lifecycle, Nexus Repository, and Nexus Vulnerability Scanner — and you will need the right mix of them to maximize the benefits.

Customers noted Sonatype's low false positives, integration into the Nexus repository, and great customer support. However, customers also emphasized that Sonatype needed better tracking of transitive dependencies and that getting scan data into a format that is shareable is difficult. Additionally, Sonatype believes its product structure is transparent and easy for customers to understand — it isn't. This pricing and licensing can make choosing the right solution from the vast number of products difficult. Customers who already own Nexus will find Sonatype an appealing option, along with customers who demand very low false positives.

Contenders

› **WhiteHat Security offers SCA without manual intervention to achieve speed.** WhiteHat Security has been known for reducing false positives by having its security team review scan results before sending them back to customers. Now, WhiteHat is able to offer a fully automated solution with Sentinel SCA Essentials in addition to WhiteHat Sentinel SCA Standard, which still has security team verification.

Because WhiteHat Sentinel Essentials is new, customers will feel the broad SCA functionality is uneven. Customers confirmed that role-based access was not complete and that it was difficult to determine if transitive dependencies were vulnerable, while also praising vulnerability details. We expect WhiteHat Security to continue to fill these gaps while it works to fulfill its mission to provide SCA, SAST, and DAST scanning at IDE, build, and production phases of the SDLC. WhiteHat Security is best for companies whose developers range in maturity, where some require speed and are able to rely on tool-only feedback and others require additional assistance through manual review of security vulnerabilities.

› **Flexera differentiates based on its security research.** Flexera's security research team, Secunia, conducts primary vulnerability research, giving Flexera customers early warning to vulnerabilities before they're officially accepted in the National Vulnerability Database (NVD). This team's success

is measured based on accuracy and response times, and all of their submissions to the NVD have been accepted and published. The vulnerabilities that Secunia finds are displayed in Flexera FlexNet Code Insight and is identified as a Secunia finding.

Although Flexera customers confirmed the flexible UI, useful workflow features, and quality of the license analysis capabilities, they also reported that documentation and training were minimal and needed to be augmented by implementation services, and that the APIs had limited functionality. Security pros and developers will be able to deliver the most common SCA use cases using Flexera without the advanced features such as autoremediation or serverless scanning.

› **Veracode provides disjointed user experience between its two products.** In 2018, Veracode acquired SourceClear to augment its own Veracode Software Composition Analysis. SourceClear Software Composition Analysis is an agent-based scanning tool, while Veracode Software Composition Analysis remains a SaaS-based offering. To get SCA, you must also perform a static analysis scan when using the SaaS option but not when using the agent scanning. Customers will find the dual functionality between two products disjointed, because they can perform only certain tasks in one or the other until the products are merged more fully at a future date. Veracode also offers static and dynamic prerelease scanning as a complement to its SCA products.

Customers will experience Veracode's awkward teenage years until it unifies both SourceClear and Software Composition Analysis, with customers frustrated with uncertain license agreements, delayed functionality, and uneven API support. However, as integration work is ongoing, we expect Veracode to work hard to shore up remaining product differences, especially consistent language support and a unified policy engine. Veracode is best for companies trying to limit their number of security vendors, and current Veracode customers will appreciate the vision of a true application security platform where SCA data augments other Veracode scan data.

Challengers

› **GitLab is off to a fast start, but security pros will find developer focus frustrating.** GitLab has been offering security products since 2017 and now offers static and dynamic analysis in addition to binary SCA. However, some of the developer use case-focused features of SCA will be uncomfortable to security pros. For example, the dismissing feature gives developers the ability to dismiss any vulnerability of any severity. This forces security pros to keep careful track of what vulnerabilities developers have chosen to ignore. Also, GitLab's leaning is not to stop the build via quality gates. Instead, it recommends using a reviewer feature, which causes security pros to manually review the status of each build.

GitLab has aggressively built its security functionality in a short amount of time and has an aggressive road map for additional features. However, many of the features are still in their infancy or in the to-do stage. Customers echoed this sentiment by giving lukewarm ratings and

highlighting a lack of broad language support, uneven discovery of vulnerabilities, and basic policy management features. Consider GitLab when most, if not all, of your development teams use it or when creating an internal GitLab open source repository.

- **FOSSA enhances product through open source and proprietary license identification.** FOSSA Compliance can automatically detect raw copyright headers as well as differentiate between private, third-party, and copyrighted external code. To help with this detection knowhow, FOSSA claims to be working with some of the legal counsels who have been involved in the early days of open source licensing. FOSSA's analysis layer is open source, which enables anyone to enhance product functionality as well as add support for new languages and frameworks.

  Customers like FOSSA's evaluation of vulnerabilities at build time and feel that as a result, vulnerability scans can be relied on even if license scan results can be uneven. Some FOSSA customers publish scan results and source FOSSA publicly. Because FOSSA is itself open source, it's best to consider it a toolkit, with customers confirming a lack of documentation and advanced functionality such as scanning containers. Additionally, a detailed, long-term road map is hard to achieve for an open source product, as FOSSA can't predict when outside contributors will create new functionality. Consider FOSSA if you have the inclination and ability to customize an SCA product to meet specific company requirements.

- **JFrog is limited to scanning binaries that reside in its repository, Artifactory.** With JFrog XRay, you can granularly define what is scanned inside binaries using their watches functionality and then map policies onto what you want scanned. Policies can be applied to all binaries and builds stored in JFrog even across multiple JFrog repositories that have indexing turned on.

  Customers gave JFrog lukewarm ratings and noted that features could be more flexible and intuitive and that reporting was especially restrictive. However, they also noted that not only was the integration with JFrog Artifactory important and well implemented, but that JFrog has rapidly developed new features and fixed any identified issues. Consider JFrog XRay when widely or solely implementing JFrog Artifactory and when autoremediation is a must.

Evaluation Overview

We evaluated vendors against 33 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 license risk management, vulnerability identification action, proactive vulnerability management, policy management, SDLC integration, container and serverless scanning, and out-of-the-box strategic reporting.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product strategy, market approach, execution road map, and training.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's installed based, growth rate and corporate profitability.

Vendor Inclusion Criteria

Forrester included 10 vendors in the assessment: Flexera, FOSSA, GitLab, JFrog, Snyk, Sonatype, Synopsys, Veracode, WhiteHat Security, and WhiteSource. Each of these vendors has:

› **A comprehensive, enterprise-class SCA tool.** All vendors in this evaluation offer a range of SCA capabilities suitable for security pros. Participating vendors were required to have most of the following capabilities out of the box: ability to provide remediation advice on both open source license risk and vulnerabilities; ability to integrate into SDLC automation tools; ability to provide proactive vulnerability management; ability to edit and create policies; and ability to visually report on open source risk.

› **$10 million or more in SCA revenue.** All vendors in this evaluation earned $10 million or more in global revenue directly from SCA capabilities.

› **Interest from Forrester clients or relevance to them.** Forrester clients often discuss the participating vendors and products during inquiries and interviews. Alternatively, in Forrester's judgment the participating vendor may have warranted inclusion because of technical capabilities and market presence.

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 January 28, 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] Source: "2018 Open Source Security and Risk Analysis," Synopsys (https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2018-ossra.pdf).

[2] Source: "2018 State of the Software Supply Chain," Sonatype (https://www.sonatype.com/2018-ssc).

[3] Source: "2018 State of the Software Supply Chain," Sonatype (https://www.sonatype.com/2018-ssc).

[4] For more information on the SCA market, see the Forrester report "Now Tech: Software Composition Analysis, Q1 2019."

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.