The Forrester Wave™: Software Composition Analysis, Q1 2017

The Six Providers That Matter Most And How They Stack Up

by Amy DeMartine

February 23, 2017

Why Read This Report

In our 38-criteria evaluation of software composition analysis (SCA) providers, we identified the six most significant ones — Black Duck Software, Flexera Software, Sonatype, Synopsys, Veracode, and WhiteSource Software — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security professionals make the right choice for their organization.

Key Takeaways

Black Duck Leads, With WhiteSource Close Behind

Our evaluation found that Black Duck Software leads the pack, while WhiteSource Software offers a competitive option. Sonatype, Synopsys, Flexera, and Veracode are relevant, albeit limited, solutions.

SCA Fundamentals Are Key Differentiators

SCA providers come from backgrounds in either license risk management or vulnerability identification, and those capabilities determine their value, along with supporting functionality such as policy management and integration with software development tools.

The Forrester Wave™: Software Composition Analysis, Q1 2017

The Six Providers That Matter Most And How They Stack Up

by Amy DeMartine
with Christopher McClean, Trevor Lyness, and Peggy Dostie

February 23, 2017

Table Of Contents

Related Research Documents

Secure Applications At The Speed Of DevOps

TechRadar™: Application Security, Q2 2015

Vendor Landscape: Software Composition Analysis

FORRESTER®

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

Open Source Risks Demand An Automated Solution

Customers expect applications to engage them in personal and relevant ways; otherwise, these customers will go elsewhere.[1] Companies are responding by rapidly creating new applications or modifying their existing applications. In the past two years, the number of applications on Google Play and in the Apple App Store has gone from 1.3 million each to more than 2 million each.[2]

In their haste to create applications, developers use open source components as their foundation, creating applications using only 10% to 20% new code.[3] Unfortunately, many of these components come with liabilities in their license agreements, and one out of every 16 open source download requests is for a component with a known vulnerability.[4] To reduce these risks, security pros are turning to SCA tools, with the expectation of, at a minimum, the following benefits:[5]

- **More information helps identify and remediate vulnerabilities quickly.** The most popular listing of source code vulnerability data is NIST's US National Vulnerability Database (NVD). However, companies relying solely on the NVD are left blind to the risk of new vulnerabilities that have not yet been vetted for inclusion. Because speed matters, SCA tools gather vulnerability data from multiple sources — including crowdsourcing — then mark which ones have been validated. The best SCA vendors also have research teams that add more-detailed information than the NVD provides and give developers the most up-to-date guidance on remediation.
- **Automated scanning highlights license risk exposure.** SCA tools give greater insight into license risks, helping companies reduce potentially significant risks hidden in open source license agreements. For example, when developers declare that they are using a certain license, SCA tools can report whether that declaration matches the actual license used. SCA tools can also scan license obligations across all components in an application to identify compatibility issues. Finally, SCA tools can be used to effectively block the use of components that have licenses that company has deemed too risky to use and even give remediation advice on alternatives.
- **Flexible policy enforcement increases alignment with business need.** Some software composition policies only apply to certain application types — such as mobile apps — while others may apply to a certain business or even a particular application. SCA tools enable users to group policies when applicable to reduce the workload on security pros and developers. Additionally, the best SCA tools allow security pros to quickly define whitelisting and blacklisting policies for both licenses and components based on chosen characteristics.
- **Product integration supports existing development processes.** Security testing processes should be seamlessly integrated into the software delivery life cycle (SDLC) with the goal of giving developers actionable data as early as possible. The best SCA tools integrate with either code repositories or integrated development environments (IDEs) to alert and even halt developers if they have a vulnerable or risky component. For policy exception requests, they can also kick off review and approval workflows with the proper legal and/or security pro to minimize delays.

Software Composition Analysis Evaluation Overview

To assess the state of the SCA market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top SCA vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of 38 evaluation criteria, which we grouped into three categories:

- **Current offering criteria evaluate a broad set of functionality.** To evaluate current offering, we analyzed key functionality in the areas of license risk, vulnerability identification, proactive vulnerability management, policy management, software delivery life cycle (SDLC) integration, risk reporting, vendor self-analysis, and product deployment.
- **Strategy criteria assess how vendors address the market.** Our assessment of strategy included product strategy, market approach, execution road map, and training.
- **Market presence criteria reflect market stability.** To score market presence, we analyzed install base, growth rate, and corporate profitability.

Evaluated Vendors And Inclusion Criteria

Forrester included six vendors in our SCA assessment: Black Duck Software, Flexera Software, Sonatype, Synopsys, Veracode, and WhiteSource Software. Each of these vendors has (see Figure 1):

- **A comprehensive, enterprise-class SCA tool.** All vendors in this evaluation offer a range of SCA capabilities suitable for roles such as legal professionals, application developers, and security pros. Participating vendors were required to have most of the following capabilities: license risk management, vulnerability identification, policy management, and software delivery life cycle integration.
- **Interest from and relevance to Forrester clients.** Forrester clients often discuss the participating vendors and products during inquiries and interviews. Alternatively, the participating vendor may, in Forrester's judgment, warrant inclusion in this evaluation because of technical capabilities and market presence.

FIGURE 1 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated	Product version evaluated
Black Duck Software	Black Duck Hub Black Duck Protex	3.4 7.5
Flexera	Palamida Enterprise Edition	6.10.3
Sonatype	Nexus IQ Server Nexus Lifecycle Nexus Firewall Nexus Auditor Nexus Repository Pro	1.23 1.23 1.23 1.23 3.1
Synopsys	Protecode ES (Protecode Enterprise) Protecode SC (Protecode Supply Chain)	5.2 Fronted: 20161114-0745 Worker: 20161114-0646-7e01d69
Veracode	Veracode Software Composition Analysis	2016.8
WhiteSource Software	Open Source Lifecycle Management	16.3

Vendor inclusion criteria

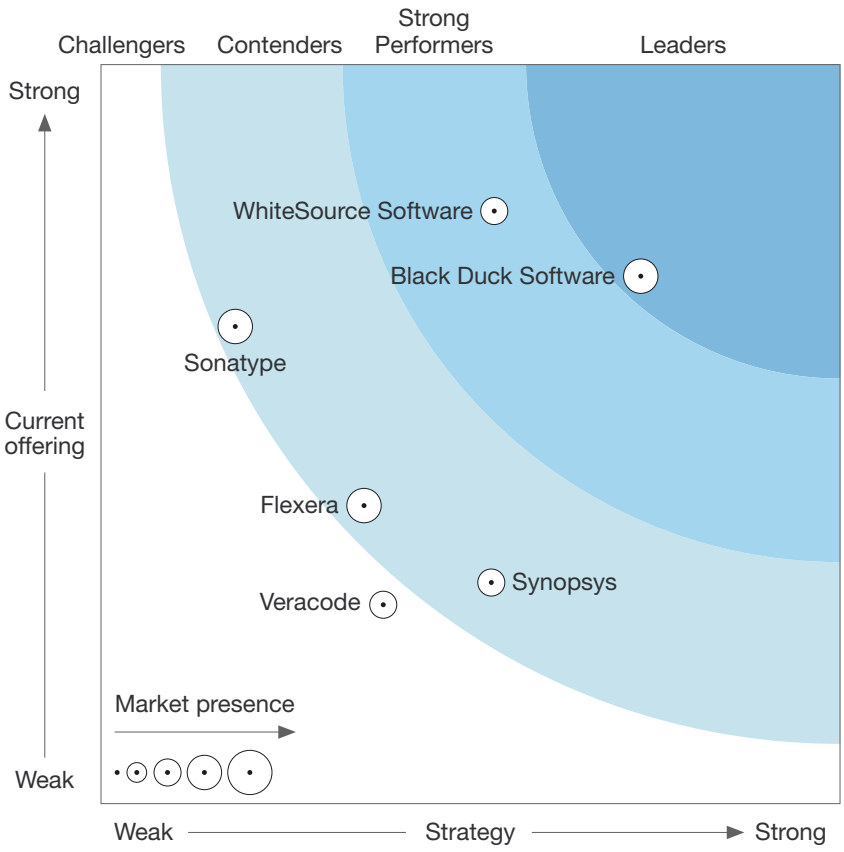
A comprehensive enterprise-class SCA tool. All vendors in this evaluation offer a range of SCA capabilities suitable for roles such as legal professionals, application developers, and security pros. Participating vendors were required to have most of the following capabilities: license risk management, vulnerability identification, policy management, and software delivery life cycle integration.

Interest from and relevance to Forrester clients. Forrester clients often discuss the participating vendors and products during inquiries and interviews. Alternatively, the participating vendor may, in Forrester's judgment, warrant inclusion in this evaluation because of technical capabilities and market presence.

Vendor Profiles

This evaluation of the SCA market is intended to be a starting point only. We encourage clients to view the detailed product evaluations and adapt criteria weightings to fit their individual needs using the Forrester Wave Excel-based vendor comparison tool (see Figure 2).

FIGURE 2 Forrester Wave™: Software Composition Analysis, Q1 '17



FORRESTER® **RESEARCH**
The Forrester Wave™

Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

FIGURE 2 Forrester Wave™: Software Composition Analysis, Q1 '17 (Cont.)

	Forrester's weighting	Black Duck Software	Flexera	Sonatype	Synopsys	Veracode	WhiteSource Software
Current Offering	50%	3.56	2.01	3.22	1.49	1.34	4.00
License risk management	20%	3.05	2.70	2.70	2.00	0.00	2.85
Vulnerability identification	20%	3.75	1.35	3.20	1.35	1.75	4.05
Proactive vulnerability management	5%	4.35	2.30	1.65	1.95	1.70	4.35
Policy management	15%	3.20	3.20	3.40	0.80	1.00	4.00
SDLC integration	25%	3.80	1.60	3.20	2.00	1.80	4.60
Risk reporting	5%	5.00	0.00	3.00	0.00	3.00	3.00
Vendor self-analysis	5%	1.00	1.00	5.00	1.00	0.00	5.00
Product deployment options	5%	5.00	3.00	5.00	1.00	3.00	5.00
Strategy	50%	3.65	1.78	0.91	2.64	1.91	2.66
Product strategy	30%	5.00	2.10	1.20	4.80	3.20	3.20
Market approach	25%	2.00	1.00	1.00	3.00	2.00	5.00
Execution road map	15%	1.00	0.00	0.00	1.00	1.00	1.00
Training	30%	5.00	3.00	1.00	1.00	1.00	1.00
Market Presence	0%	3.80	3.14	3.30	2.40	2.30	2.60
Installed base	60%	5.00	2.40	5.00	2.00	3.00	3.00
Growth rate	10%	2.00	2.00	3.00	3.00	5.00	5.00
Corporate profitability	30%	2.00	5.00	0.00	3.00	0.00	1.00

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

Leaders

› **Black Duck Software builds on its foundation of source code coverage.** Black Duck Hub boasts over 80 supported source code language formats, and it uses this strength to scan a broad range of developer preferences for both license risk management and vulnerability identification. Additionally, Black Duck provides an application bill of materials (BOM) for as long as users choose, and it monitors for any new open source vulnerabilities using vulnerability data that gets

updated hourly. Users are notified of newly identified vulnerabilities in their BOM via the user interface, email/SMS, and automatically generated JIRA tickets. Black Duck Software has very strong risk reporting and strong proactive vulnerability management capabilities, but its biggest differentiation comes from sound support for the fundamentals of license risk management, vulnerability identification, and policy management.

Strong Performers

› **WhiteSource Software relies on both curated and crowdsourced data.** Because identifying and resolving license risk and vulnerabilities demands reliable data, WhiteSource's research team adds only curated information into its database in an effort to reduce false positives. Additionally, WhiteSource uses crowdsourced input from thousands of users to enhance its guidance on resolution actions and then ranks the different alternatives from both crowdsourcing and vulnerability data sources. WhiteSource Software offers strong support for proactive vulnerability management, policy management, and SDLC integration, with sound vulnerability identification capabilities as well.

Contenders

› **Sonatype offers a family of products that provides risk information early in the SDLC.** Sonatype markets the Nexus family of software supply chain solutions, which enables the selection, traceability, policy enforcement, and remediation of software components. Within this portfolio, users will need to understand which product combination offers the right functionality for their use case. Sonatype tools integrate into the integrated development environment (IDE), affording the ability to track how well all versions of a component comply with company policy. Developers can use this data to pick a version of a component that complies with policy for both licenses and vulnerabilities across the SDLC instead of simply choosing the latest version. Sonatype is known for its coverage of Java open source components, and the company is working to catch up on its number of languages supported.

› **Flexera Software provides audit-friendly reports for license management.** In 2016, Flexera Software purchased Palamida to help customers reduce open source software risks. Palamida Enterprise Edition and Standard Edition produce several audit-friendly reports, such as license usage, license obligation, and license compatibility. Additionally, the products capture the full history of change requests approval dates and times, as well as reviewers, which can be used for audits. Flexera offers sound policy management but has weak license risk management and very weak vulnerability identification.

› **Synopsys relies on two separate products to deliver SCA.** In 2015, Synopsys acquired the companies Protecode and Codenomicon, and now it offers two products: Protecode ES, which scans source code and binaries, and Protecode SC, which just scans binaries. Synopsys is working to integrate the two products, but for now, most customers have to utilize both, and

managing policy between the two products is difficult. The company found early market validation when Docker chose to use Protecode SC as a back end for its security scanning functionality. Synopsys offers weak SDLC integration and license risk management and very weak vulnerability identification and policy management.

Challengers

› **Veracode utilizes its static analysis tools to provide insight into proprietary code.** While other SCA vendors rely on extensive component databases, such as the NVD, to provide information about open source components, if a source code component is unknown to Veracode SCA, users can run Veracode's Static Analysis tool to identify potential security flaws. Veracode SCA does not currently offer license risk management, but the company has included this capability as a part of its possible road map. Veracode provides sound risk reporting but has very weak vulnerability identification and policy management.

Supplemental Material

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of two 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 November 16, 2016.

- **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.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then 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.

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, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

Endnotes

[1] For more information on how customers are now more mobile, consume more reviews, and buy more online than ever before, and how companies must respond by becoming customer-obsessed, see the Forrester report "Winning In The Age Of The Customer."

[2] For more information on mobile application usage and what it means to developing mobile applications, see the Forrester report "Build Five-Star Mobile Apps."

[3] Source: "2015 State of the Software Supply Chain Report: Hidden Speed Bumps on the Road to 'Continuous,'" Sonatype (http://cdn2.hubspot.net/hubfs/1958393/White_Papers/2015_State_of_the_Software_Supply_Chain_Report-.pdf?t=1466775053631).

For more information on the dangers of open source software, see the Forrester report "The Seven Habits Of Rugged DevOps."

[4] Source: "2016 State of the Software Supply Chain," Sonatype (https://www.sonatype.com/software-supply-chain).

For more information on the use of open source in modern applications, see the Forrester report "Secure Applications At The Speed Of DevOps."

[5] For more information on the drivers for SCA tools and the different roles that SCA serve, see the Forrester report "Vendor Landscape: Software Composition Analysis."

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.