Now Tech: Software Composition Analysis, Q1 2019

Forrester's Overview Of 17 Software Composition Analysis Providers

by Amy DeMartine

January 24, 2019

Why Read This Report

You can use software composition analysis (SCA) to eliminate vulnerable components, reduce license risk, and apply consistent policies during the software development life cycle (SDLC). But to access these benefits, you'll first have to select from a diverse set of vendors — vendors that vary by size, functionality, geography, and vertical market focus. Security professionals should use Forrester's Now Tech report to understand the value they can expect from an SCA provider and select vendors based on size and functionality.

Key Takeaways

Improve Open Source Security With Software Composition Analysis
Developers use open source components to achieve speed; however, vulnerabilities in these components represent a top target for successful external attacks. Embedding software composition analysis tools in the software delivery life cycle and using the results as a quality gate prevents the use of vulnerable open source while providing developers the speed they demand.

Select Vendors Based On Size And Functionality
SCA specialists have the most robust functionality in this segment, but they only provide SCA capabilities. Container security and repository-adjacent vendors offer broader functionality beyond SCA but have less robust SCA capabilities.

Encourage Your Developers To Aggressively Use Open Source
In the past, security pros approached the use of open source with reluctance or even disapproval, considering it too risky. By helping implement SCA tools into their firm's development practices, security pros can confidently encourage developers to use open source.

Now Tech: Software Composition Analysis, Q1 2019

Forrester's Overview Of 17 Software Composition Analysis Providers

by Amy DeMartine
with Christopher McClean, Kate Pesa, and Peggy Dostie
January 24, 2019

Table Of Contents

Recommendations

Related Research Documents

Application Security Market Will Exceed $7 Billion By 2023

The State Of Application Security, 2019

TechRadar™: Application Security, Q3 2017

FORRESTER®

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

Improve Open Source Security With Software Composition Analysis

Developers who use open source or third-party components are following the wisdom of not reinventing the wheel. Instead, they reuse what has already been written and focus on adding proprietary software that creates differentiating customer experiences. However, this code comes from a multitude of unvetted sources, has a multitude of license models, and has vulnerabilities that can propagate into otherwise clean enterprise code. And developers don't inherently know which components are vulnerable or which contain risky licenses.

Vulnerabilities remain a top concern for security decision makers: 35% of global security decision makers who experienced an external breach said that it occurred due to software vulnerabilities.[1] Security pros can help developers avoid these vulnerabilities using SCA tools, which can identify vulnerable or risky components early in the SDLC. Forrester defines SCA as:

> *Products that scan an application (without executing it) to identify vulnerabilities and conflicts in open source and third-party components, guiding users on where and how to remediate these flaws.*

Firms that excel at automating software composition analysis will:

- **Eliminate vulnerable components.** SCA tools can give developers early information about components that are vulnerable, which saves them time later in the SDLC, when defects are more costly to find and fix. In addition, some SCA tools can give early warning and prioritization on vulnerabilities not yet verified by the National Vulnerability Database.
- **Reduce license risk.** Historically, license assessments only happened during M&A activities, but it's gradually become a task that needs to be completed before each software release. Security pros can implement SCA to help their colleagues in the legal department actively assess risk and re-evaluate company policy immediately when licenses change.
- **Apply consistent open source policies.** Security pros need to assess the overall risk presented by open source components across all applications, set consistent policies to keep risk to acceptable levels, and work with development teams to guide vulnerability remediation. This can only be reliably and automatically done with SDLC embedded SCA.

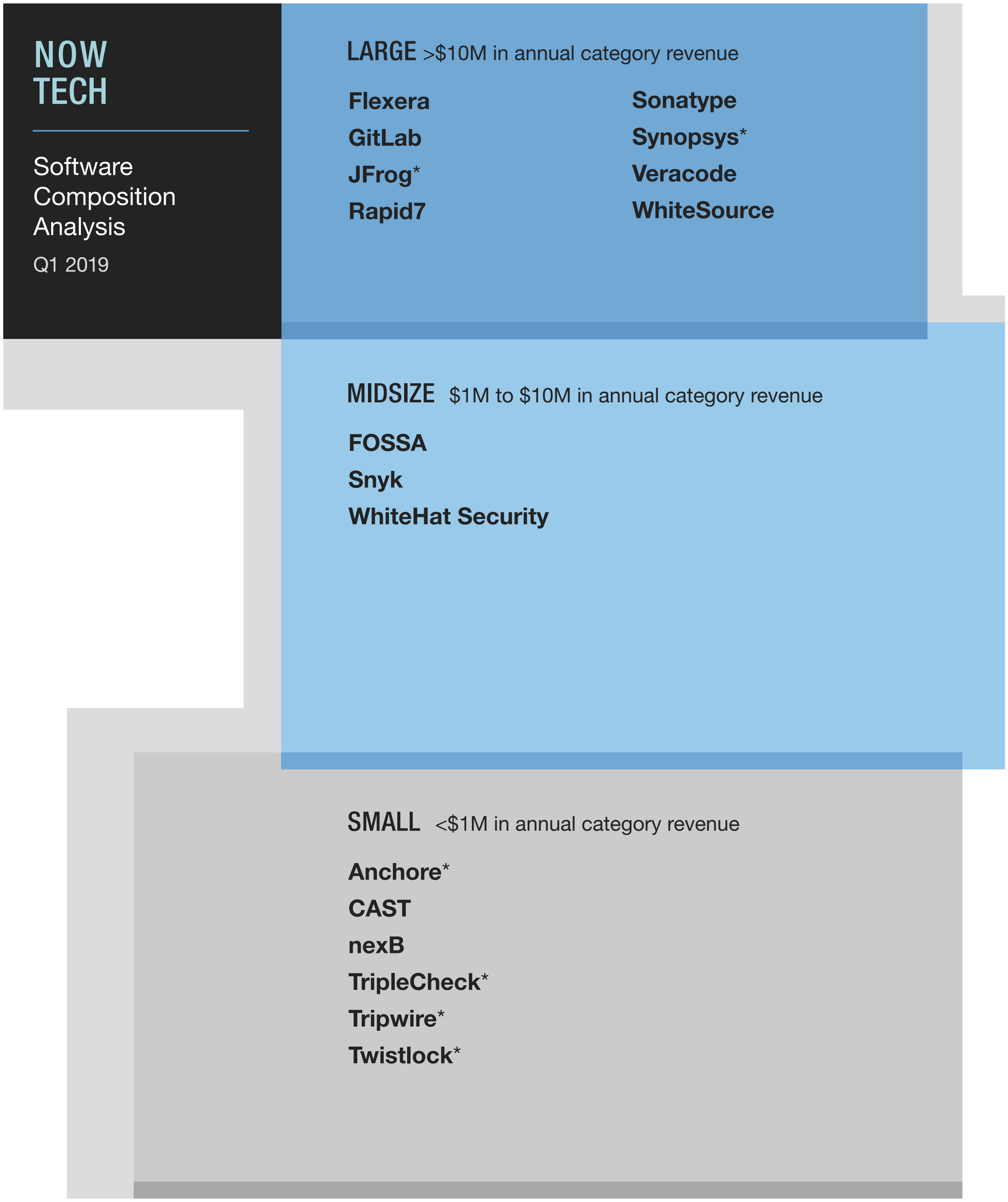
Select Vendors Based On Size And Functionality

We've based our analysis of the SCA market on two factors: market presence and functionality.

Software Composition Analysis Market Presence Segments

We segmented the vendors in this market into three categories based on SCA revenue: large, established vendors (more than $10 million in SCA revenue), midsize vendors ($1 million to $10 million in revenue), and smaller vendors (less than $1 million in revenue) (see Figure 1). We did not include vendors that we estimated to have less than $250,000 in revenue.

FIGURE 1 Now Tech Market Presence Segments: Software Composition Analysis, Q1 2019



NOW TECH

Software Composition Analysis

Q1 2019

LARGE >$10M in annual category revenue

- Flexera
- GitLab
- JFrog*
- Rapid7
- Sonatype
- Synopsys*
- Veracode
- WhiteSource

MIDSIZE $1M to $10M in annual category revenue

- FOSSA
- Snyk
- WhiteHat Security

SMALL <$1M in annual category revenue

- Anchore*
- CAST
- nexB
- TripleCheck*
- Tripwire*
- Twistlock*

*Forrester estimate

Software Composition Analysis Functionality Segments

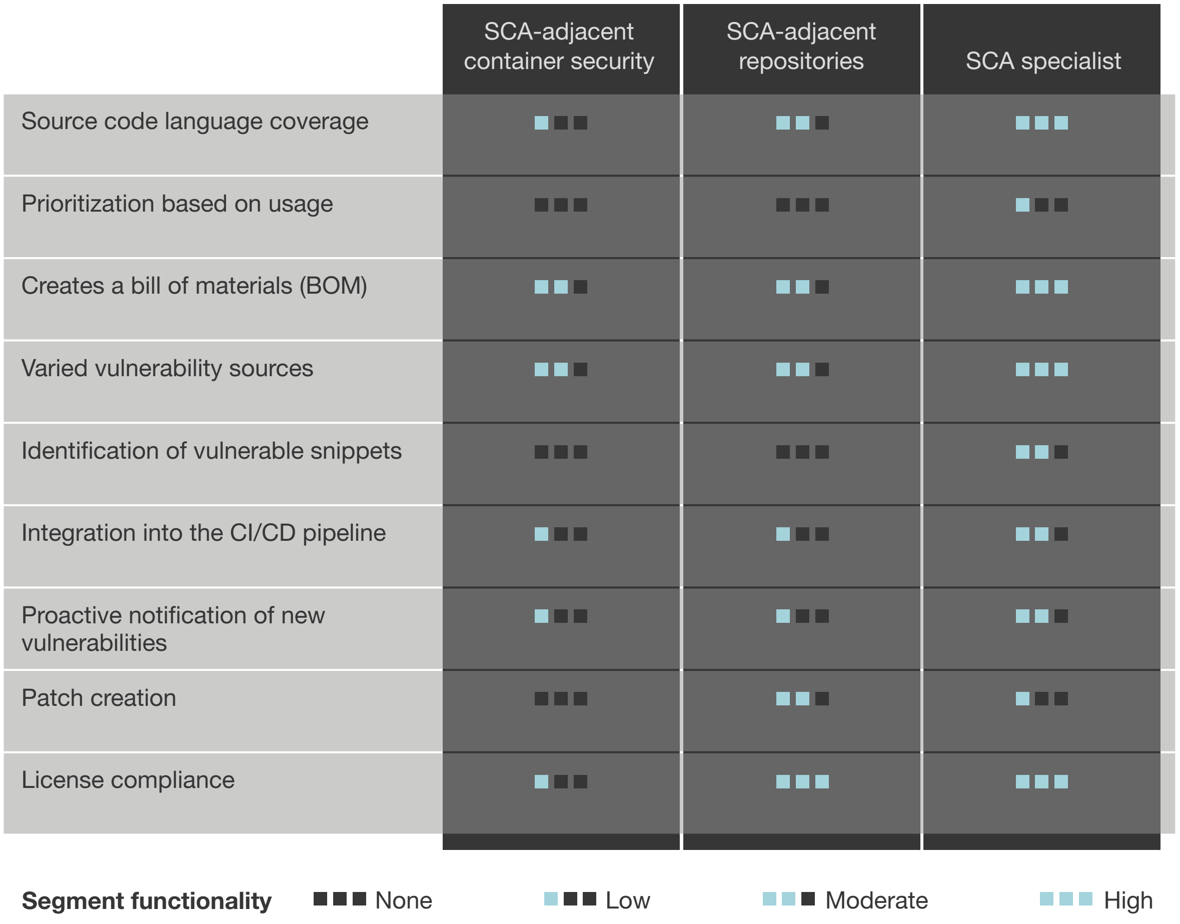
To explore functionality at a deeper level, we broke the SCA market into three segments, each with varying capabilities (see Figure 2):

› **Container security tools scan at-rest containers for vulnerabilities.** These vendors provide SCA functionality with a scope limited to containers as part of their broader container security capabilities. Because these tools scan an instantiated container, they often do not have access to source code, which limits their ability to do much more than scan for vulnerabilities and create a bill of materials.

› **Code repositories have expanded to scan components they store for vulnerabilities.** Development teams use repositories to store code once it's checked in or as a holding location for code between different phases of the SDLC. As such, repositories are prime locations for SCA scanning. Because SCA is not their primary value proposition, these tools lack advanced functionality, such as supporting multiple vulnerability feeds or integrations with other SDLC tools.

› **SCA specialist tools provide analysis for legal and security teams.** These vendors offer comprehensive capabilities, although the focus from one vendor to the next is variable. For example, they have different degrees of source code language coverage, policy creation capabilities, and license compliance management. Customers typically appreciate the one-stop-shop experience but may feel limited by their SCA focus and instead want tools that are either part of a wider portfolio of application security or tools such as repositories or container security tools that do more than just SCA.

FIGURE 2 Now Tech Functionality Segments: Software Composition Analysis, Q1 2019



	SCA-adjacent container security	SCA-adjacent repositories	SCA specialist
Source code language coverage	🟦⬛⬛	🟦🟦⬛	🟦🟦🟦
Prioritization based on usage	⬛⬛⬛	⬛⬛⬛	🟦⬛⬛
Creates a bill of materials (BOM)	🟦🟦⬛	🟦🟦⬛	🟦🟦🟦
Varied vulnerability sources	🟦🟦⬛	🟦🟦⬛	🟦🟦🟦
Identification of vulnerable snippets	⬛⬛⬛	⬛⬛⬛	🟦🟦⬛
Integration into the CI/CD pipeline	🟦⬛⬛	🟦⬛⬛	🟦🟦⬛
Proactive notification of new vulnerabilities	🟦⬛⬛	🟦⬛⬛	🟦🟦⬛
Patch creation	⬛⬛⬛	🟦🟦⬛	🟦⬛⬛
License compliance	🟦⬛⬛	🟦🟦🟦	🟦🟦🟦

Segment functionality ⬛⬛⬛ None 🟦⬛⬛ Low 🟦🟦⬛ Moderate 🟦🟦🟦 High

Align Individual Vendor Solutions To Your Organization's Needs

The following tables provide an overview of vendors with details on functional category, geography, and vertical market focus (see Figure 3, see Figure 4, and see Figure 5).

FIGURE 3 Now Tech Large Vendors: Software Composition Analysis, Q1 2019

LARGE >$10M in annual category revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (top three by revenue %)	Sample customers
Flexera	SCA specialist	NA 60%; LATAM 5%; EMEA 30%; AP 5%	Technology; manufacturing; legal	Adobe; Software AG; Wind River
GitLab	SCA-adjacent repositories	NA 65%; LATAM 1%; EMEA 23%; AP 11%	Technology; financial services; insurance	Alteryx; TrueBlue Enterprises Inc.
JFrog	SCA-adjacent repositories	NA 60%; EMEA 30%; AP 10%	Financial services; technology; telecommunications	Vendor did not disclose.
Rapid7	SCA-adjacent container security	NA 50%; LATAM 5%; EMEA 30%; AP 15%	Vendor did not disclose.	American Express; Cerner; Rite Aid
Sonatype	SCA specialist	NA 67%; EMEA 30%; AP 3%	Financial services; technology; healthcare	Equifax; Goldman Sachs; Salesforce
Synopsys	SCA specialist	NA 62%; EMEA 18%; AP 20%	Technology; financial services	Dynatrace; Exact Group; OpenText
Veracode	SCA specialist	NA 86%; LATAM 1%; EMEA 9%; AP 4%	Financial services; technology	McKesson; Unum; VMware
WhiteSource	SCA specialist	NA 65%; LATAM 1%; EMEA 31%; AP 3%	Financial services; technology; healthcare	Comcast; Deloitte; Microsoft

FIGURE 4 Now Tech Midsize Vendors: Software Composition Analysis, Q1 2019

MIDSIZE $1M to $10M in annual category revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (top three by revenue %)	Sample customers
FOSSA	SCA specialist	NA 70%; EMEA 20%; AP: 10%	Legal; technology; security	Docker; Twitter; Zendesk
Snyk	SCA specialist	NA 70%; LATAM 1%; EMEA 20%; AP 9%	Technology; financial services; retail	ASOS; New Relic; SkyScanner
WhiteHat Security	SCA specialist	NA 89%; EMEA 11%	Financial services; healthcare; technology	Lattice Engines

FIGURE 5 Now Tech Small Vendors: Software Composition Analysis, Q1 2019

SMALL <$1M in annual category revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (top three by revenue %)	Sample customers
Anchore	SCA-adjacent container security	NA 100%	Security	Best Buy; Q2E Banking; Sysdig
CAST	SCA specialist	NA 40%; LATAM 10%; EMEA 40%; AP 10%	Financial services; retail; entertainment	ATOS; Broadridge; French Ministry of Education
nexB	SCA specialist	NA 90%; EMEA 10%	Technology	Vendor did not disclose.
TripleCheck	SCA specialist	NA 5%; EMEA 95%	Aerospace; security; transportation	Vendor did not disclose.
Tripwire	SCA-adjacent container security	NA 80%; EMEA 20%	Financial services; retail; manufacturing	Vendor did not disclose.
Twistlock	SCA-adjacent container security	NA 80%; EMEA 15%; AP 5%	Financial services; healthcare; technology	Aetna; PayPal; Walgreens

Recommendations

Encourage Your Developers To Aggressively Use Open Source

According to global security decision makers, the top two business priorities for their firms are to grow revenue and improve the experience of customers (41% and 38% of respondents, respectively, said this is a high or critical priority).[2] Accelerating the use of open source components can help achieve both priorities by letting developers focus on creating new and unique features rather than recreating basic functionality. It's long past time for security pros to realize the benefits of open source components and embrace its use in development. By pairing the aggressive use of open source components with SCA capabilities, you can also:

› **Automate the curation of open source components.** Many companies offer their developers a private repository of trusted open source components. However, these repositories are often limited and cause delays in development, because developers have to submit manual requests for reviews of new components. Connecting SCA products using APIs, security pros can automate the process of obtaining, scanning, and approving components, which will free up resources. However, don't forget that an SCA scan in the SDLC is mandatory to create an up-to-date bill of materials as well as to prevent any vulnerable components that have been obtained outside this process from sneaking into a release.

› **Reduce the dependence on old or multiple versions of a component.** When an open source component is especially useful, developers may use many different versions, including very old ones, throughout a company. This situation creates an upgrade nightmare when a new vulnerability is disclosed, as open source communicates only release fixes to the latest version of code. To further reduce the risk of open source components, security pros can use SCA tools to highlight the most frequently used or oldest components, then use this information to request upgrades in the affected application's backlog.

› **Increase customer trust through greater visibility.** Some companies provide their current and potential customers with the results of SCA scans to prove they've done their due diligence with regards to using open source. As this trend becomes more prevalent, companies in many industries will face pressure from demanding customers — both B2B and B2C — or security standards that will demand that firms in verticals such as banking, insurance, or healthcare are actively analyzing and remediating their risky code.

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

Market Presence Methodology

We defined market presence in Figure 1 based on revenue.

To complete our review, Forrester requested information from vendors. If vendors did not share this information with us, we made estimates based on available secondary information. We've marked companies with an asterisk if we estimated revenues or information related to geography or industries. Forrester fact-checked this report with vendors before publishing.

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Anchore

CAST Software

Flexera

FOSSA

GitLab

JFrog

nextB

Rapid7

Snyk

Sonatype

Synopsys

TripleCheck

Tripwire

Twistlock

Veracode

WhiteHat Security

WhiteSource

Endnotes

[1] Source: Forrester Analytics Global Business Technographics® Security Survey, 2018.

[2] Source: Forrester Analytics Global Business Technographics Security Survey, 2018.

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. 145117