WAVE REPORT

The Forrester Wave™: Software Composition Analysis Software, Q4 2024

The 10 Providers That Matter Most And How They Stack Up

November 13, 2024

By Janet Worthington with Amy DeMartine, Caroline Provost, Peter Harrison

FORRESTER®

Summary

In our evaluation of software composition analysis (SCA) software providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps you select the right one for your needs.

Additional resources are available in the online version of this report.

SCA Is A Key Component To Secure The Software Supply Chain

Every business depends on software for operations, customer engagement, and back-end automation to expand its market reach. Developers responsible for creating vital software are under significant pressure to deliver value to customers more quickly than ever and accelerate product development. However, the key advantage for organizations lies in leveraging open-source and third-party software for foundational elements, like logging libraries. This strategy allows development teams to concentrate on crafting the unique business logic that sets the organization apart. An astonishing 77% of codebases are comprised of open-source software, which means a considerable amount of an application's risk is due to third-party sources. Application security and development leaders depend on SCA tools for insight into the security risks and licensing concerns associated with open-source and third-party libraries. SCA providers stand out by not only efficiently identifying and addressing security and license risks but also embracing use cases related to the software supply chain.

SCA customers using this evaluation to inform a purchase decision should look for software that:

- **Assists developers in remediating vulnerabilities and keeping libraries current.** Prioritizing vulnerabilities by using criteria such as exploitability, maturity, effort to fix, reachability (whether the vulnerable method is called), and production context (whether the vulnerable library is loaded into memory or the application is internet facing) reduces overhead for security and development. Solutions that provide remediation guidance in the form of best-fix option; alternative libraries; automated remediation; and transitive vulnerability root-level resolutions in the integrated development environment (IDE), pull request, and CI/CD pipelines rate higher for developer experience. SCA solutions help reduce tech debt by creating automated pull requests to keep libraries up to date.
- **Provides visibility into software supply chain risk.** SCA solutions that surface declared, observed, and embedded licenses — with the ability to mark the effective license — differentiate from other offerings. Third-party, closed-source, and source code snippet detection is limited to a few vendors. Package health, reputation, pedigree, provenance, and project activity give differentiated insights into operational risk. Software bill of materials (SBOM) generation in NTIA data formats is universal. Generation of AI BOMs, ML BOMs, and cryptography BOMs is on the horizon. A few vendors offer SBOM management, ingesting, analyzing, and monitoring SBOMs as a separate module.

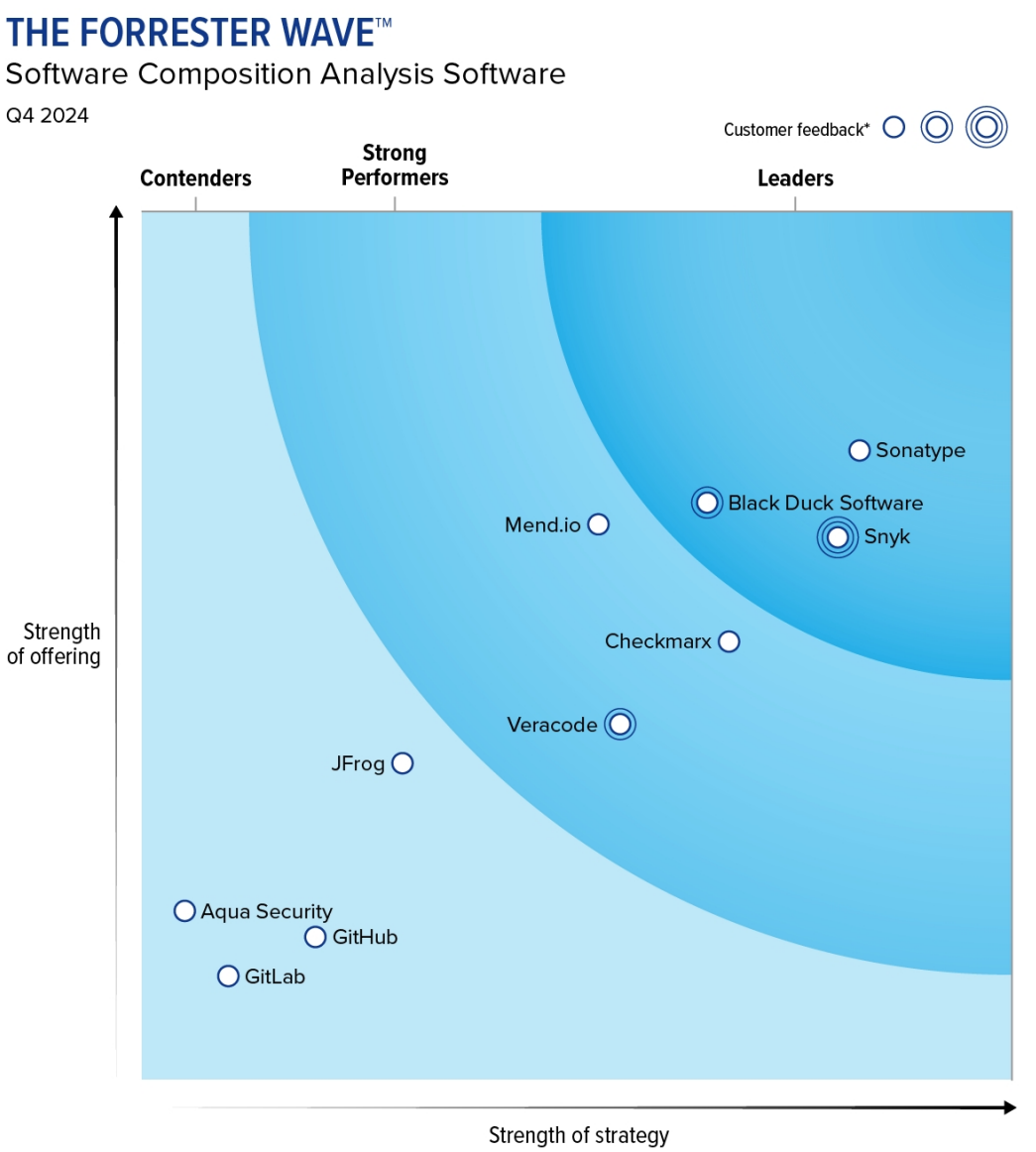
- **Prevents software supply chain attacks.** Solutions that detect, quarantine, and block suspicious and malicious packages, as well as identify malicious behavior, such as typosquatting, starjacking, repojacking, and dependency confusion, are becoming a necessity for enterprises. Build, delivery, and deployment tools are also potential attack vectors. More vendors are scrutinizing container images, infrastructure as code (IaC), Kubernetes clusters, and serverless functions, but vendors don't yet widely support capabilities such as identifying security misconfigurations in CI/CD pipelines, component integrity, and AI component analysis.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, and Contenders (see Figures 1 and 2). We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt the findings based on their priorities using Forrester's interactive provider comparison experience.

Figure 1

Forrester Wave™: Software Composition Analysis Software, Q4 2024



*A halo indicates above-average customer feedback. A double halo indicates that the vendor is a Customer Favorite.

Figure 2

Forrester Wave™: Software Composition Analysis Software Scorecard, Q4 2024

	Forrester's weighting	Aqua Security	Black Duck Software	Checkmarx	GitHub	GitLab
Current offering		1.78	3.66	3.02	1.66	1.48
Component identification and analysis	10%	1.00	5.00	3.00	1.00	1.00
License detection, analysis, and guidance	6%	1.00	5.00	3.00	1.00	1.00
Risk intelligence	1%	3.00	5.00	3.00	5.00	1.00
Prioritization and reachability	15%	3.00	3.00	3.00	1.00	1.00
Remediation and automation	15%	1.00	3.00	3.00	3.00	1.00
SBOM generation, export, and sharing	7%	3.00	5.00	3.00	1.00	1.00
SBOM ingestion and analysis	3%	3.00	5.00	3.00	1.00	1.00
Policy management	5%	3.00	5.00	3.00	1.00	3.00
Reporting and analytics	10%	1.00	3.00	3.00	1.00	1.00
Developer experience	5%	1.00	3.00	3.00	3.00	1.00
Malicious package detection	5%	3.00	3.00	3.00	1.00	3.00
Language support	1%	1.00	5.00	5.00	3.00	3.00
Software supply chain coverage	1%	5.00	3.00	3.00	3.00	5.00
Software supply chain integration	1%	3.00	3.00	3.00	3.00	3.00
Software development toolchain integration	3%	1.00	3.00	3.00	3.00	1.00
Component health	5%	1.00	3.00	3.00	3.00	1.00
AI component analysis	2%	1.00	3.00	3.00	1.00	1.00
Product security	5%	1.00	3.00	3.00	1.00	5.00

Scores are on a scale of 1 (below par relative to others evaluated) to 5 (superior relative to others evaluated).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

	Forrester's weighting	Aqua Security	Black Duck Software	Checkmarx	GitHub	GitLab
Strategy		1.20	3.60	3.70	1.80	1.40
Vision	25%	1.00	3.00	3.00	1.00	1.00
Innovation	25%	1.00	5.00	3.00	3.00	1.00
Roadmap	25%	1.00	3.00	5.00	1.00	1.00
Partner ecosystem	5%	5.00	3.00	3.00	3.00	5.00
Adoption	5%	1.00	3.00	3.00	3.00	3.00
Pricing flexibility and transparency	5%	1.00	1.00	3.00	3.00	3.00
Supporting services and offerings	10%	1.00	5.00	5.00	1.00	1.00

Scores are on a scale of 1 (below par relative to others evaluated) to 5 (superior relative to others evaluated).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

	Forrester's weighting	JFrog	Mend.io	Snyk	Sonatype	Veracode
Current offering		2.46	3.56	3.50	3.90	2.64
Component identification and analysis	10%	3.00	3.00	3.00	5.00	3.00
License detection, analysis, and guidance	6%	3.00	3.00	1.00	5.00	1.00
Risk intelligence	1%	1.00	3.00	5.00	3.00	3.00
Prioritization and reachability	15%	3.00	5.00	3.00	3.00	3.00
Remediation and automation	15%	3.00	5.00	5.00	3.00	3.00
SBOM generation, export, and sharing	7%	3.00	3.00	3.00	5.00	3.00
SBOM ingestion and analysis	3%	1.00	3.00	1.00	5.00	1.00
Policy management	5%	3.00	1.00	3.00	5.00	3.00
Reporting and analytics	10%	1.00	3.00	5.00	3.00	3.00
Developer experience	5%	1.00	3.00	3.00	3.00	3.00
Malicious package detection	5%	3.00	5.00	3.00	5.00	1.00
Language support	1%	1.00	5.00	3.00	3.00	3.00
Software supply chain coverage	1%	3.00	3.00	3.00	1.00	3.00
Software supply chain integration	1%	3.00	3.00	3.00	3.00	3.00
Software development toolchain integration	3%	3.00	3.00	5.00	5.00	5.00
Component health	5%	1.00	3.00	5.00	5.00	1.00
AI component analysis	2%	1.00	5.00	3.00	5.00	1.00
Product security	5%	3.00	1.00	3.00	3.00	3.00

Scores are on a scale of 1 (below par relative to others evaluated) to 5 (superior relative to others evaluated).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

	Forrester's weighting	JFrog	Mend.io	Snyk	Sonatype	Veracode
Strategy		2.20	3.10	4.20	4.30	3.20
Vision	25%	1.00	3.00	5.00	5.00	3.00
Innovation	25%	3.00	3.00	5.00	5.00	3.00
Roadmap	25%	3.00	3.00	3.00	5.00	3.00
Partner ecosystem	5%	3.00	1.00	3.00	1.00	3.00
Adoption	5%	1.00	1.00	3.00	1.00	5.00
Pricing flexibility and transparency	5%	3.00	5.00	3.00	3.00	1.00
Supporting services and offerings	10%	1.00	5.00	5.00	3.00	5.00

Scores are on a scale of 1 (below par relative to others evaluated) to 5 (superior relative to others evaluated).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Leaders

Sonatype

Sonatype offers Sonatype Lifecycle, Sonatype Repository Firewall, Sonatype SBOM Manager, Sonatype Developer, and Sonatype Nexus Repository. The Advanced Legal Pack and Sonatype Container are add-ons.

- **Strategy.** Sonatype's vision of blocking software supply chain attacks at the network firewall and endpoint protection systems is revolutionary. The stellar roadmap includes SBOM sharing, regulation-specific templates, SBOM and supplier quality scoring, AI/ML supply chain coverage, and AI BOM management, which would catapult Sonatype ahead on both software supply chain and generative AI (genAI) SCA. Sonatype is a suite of individual products that each require setup, which is a weakness; however, reference customers rate the cost to value as superior.
- **Capabilities.** Sonatype is a trailblazer for detection of inner-source and associated transitive dependencies to efficiently manage internal shared components. AI component analysis for open-source frameworks, libraries, and models detects malicious behavior. Sonatype Repository Firewall works with Sonatype Nexus Repository and JFrog Artifactory, blocking malicious open-source code — a differentiator. Sonatype policy management can be set for each software development lifecycle (SDLC) stage for vulnerability, license, and open-source health conditions. Policy is displayed in the IDE, Chrome plug-in, and CI pipelines, along with alternative healthy options. Reachability is only available on Java, which

is a weakness.

- **Customer feedback.** Reference customers told us that Sonatype is the best provider for blocking malicious packages, which is imperative to secure the software supply chain.
- **Forrester's take.** Sonatype is an excellent choice for enterprises looking to manage dependency, license, operational, and malicious package risk across the portfolio.

View Sonatype's detailed scorecard.

Snyk

Snyk, a developer-first application security platform, provides SCA, static application security testing (SAST), container image and IaC security, and application risk management.

- **Strategy.** Snyk's strategy is to place the onus of secure software on the development systems and process, not the developer. This is reflected in the vision to provide autonomous remediation and a development platform to automatically distribute secure, healthy components. Snyk's AppRisk, its latest innovation, automagically detects and analyzes assets in code repositories and cataloging controls. The SCA roadmap is a mixture of improving existing features, such as reachability for more languages, and on-par features, such as private package fixes. Snyk provides a breadth of application and supply chain security that is hard to match but has a variable user experience between the back end and UI.
- **Capabilities.** Snyk's vulnerability explanations and guidance are in developer, not security, speak. Automated pull requests are created for new vulnerabilities, security debt, and dependency updates. Snyk lacks robust license approval workflows relative to others we evaluated. Snyk provides ways to analyze an SBOM, but ingesting and monitoring SBOM components are on the roadmap, and it refers customers to the ServiceNow integration for now. Snyk's advisory and vulnerability databases are public and used by customers, noncustomers, and other security tools.
- **Customer feedback.** Reference customers told us that Snyk stands out for holding itself accountable for customer commitments and providing great services as well as balancing the needs of both security and development with product functionality. Snyk is a Customer Favorite in this evaluation.

- **Forrester's take.** Snyk is a great fit for enterprises implementing development, security, and operations (DevSecOps) at scale.

View Snyk's detailed scorecard.

Black Duck Software

Black Duck Software, the new name for the company recently spun off from Synopsys Software Integrity Group, was a standalone company acquired in 2017.

- **Strategy.** Black Duck Software has a history of innovation, with the largest research group in this evaluation and one of the largest open-source software knowledge bases. The Black Duck professional edition is the choice for manufacturing and regulated industries, where tracking components and licenses is a must, and customers are willing to pay for it. The vision is to help enterprises manage open-source and third-party components, binaries, and code snippets and to help software operators manage vendor SBOMs, incident response, and compliance. This plays well to its existing customer base. The roadmap — which includes genAI snippet analysis and SBOM management, including secure SBOM sharing — is interesting, but not differentiating, and customers cite struggles to get new features in a timely manner.
- **Capabilities.** Black Duck Software offers exceptional open-source, third-party, and closed-source component and snippet analysis for vulnerability, license, and copyright detection. SBOM management, generation, export, ingestion, and analysis capabilities are among the best in this evaluation. Policy management is a strength, with more than 40 criteria for operational health, license risk, and security risk. Reporting and analytics are available in the UI, via API, and with BI templates, but user experience is poor, and the overall UI is out of date.
- **Customer feedback.** Reference customers appreciate Black Duck Software's superior license and component tracking capabilities.
- **Forrester's take.** Enterprises in highly regulated industries should shortlist Black Duck Software.

View Black Duck Software's detailed scorecard.

Strong Performers

Checkmarx

Checkmarx One is a cloud-based platform for application security testing that offers SAST, API security, dynamic application security testing (DAST), application security posture management (ASPM), container security, and IaC scanning.

- **Strategy.** Checkmarx's vision encompasses the evolution of application development with the advent of genAI and the need to arm customers with a proactive posture that utilizes AI/ML to identify, triage, and resolve vulnerabilities faster. It also includes expanded software supply chain coverage and the ability to address new risk from open-source LLMs, but the focus is on cloud-native applications. The roadmap outperforms the vision with malicious image protection, artifact integrity, malicious LLM detection, and AI private packages. Cloud insights, the latest innovation, show attack-path visualization, utilizing Sysdig, Wiz, and Amazon Web Services partnerships. It will soon incorporate SCA and IaC.
- **Capabilities.** Checkmarx's extensive language and technology support are differentiators. Remediation effort and impact, upgrade steps, reachability, and malicious indicators equip security with the necessary information to take back to developers, but the AppSec Knowledge Center provides limited information. The IDE plug-ins offer one-click-fix version updates but not automated PR functionality.
- **Customer feedback.** Reference customers said that Checkmarx One has an improved user experience but that pertinent information is buried several pages deep. They also told us that the UI and API need more filtering capabilities and that reporting and analytics need improvement.
- **Forrester's take.** Checkmarx is ideal for enterprises with a broad software development tech stack and application security engineers or developer security champions to optimize use.

View Checkmarx's detailed scorecard.

Mend.io

Mend.io is an application security provider for SCA, SAST, container image and Kubernetes cluster scanning, IaC, and AI component scanning.

- **Strategy.** Mend.io's new pricing strategy is a strength: It offers one price for all products and services, including SCA, dependency updates, SAST, container security, and AI security, and it reflects the vision that customers need a holistic

view of the application stack. Mend.io pioneered reachability, acquired Renovate for dependency updates, and is one of the first to market with AI component analysis. However, it shows up less and less on shortlists due to its multiyear consolidation, resulting in a single UI and CLI agent that covers all the products but gives competitors the ability to go beyond Mend.io's original differentiators.

- **Capabilities.** Utilizing feedback from the free version of Renovate, Mend.io provides merge confidence ratings to paid customers. Mend.io provides static reachability and runtime reachability with its Sysdig partnership. Autoremediation for newly discovered vulnerabilities is a strength. Mend.io provides solid vulnerability and license detection and is good for customers who want to manage licenses without the higher price point of others. Policy management is a weakness, with fewer criteria compared with other vendors and a legacy UI, which customers are continuing to use. Mend.io earns low marks on product security due to a lack of transparency.
- **Customer feedback.** Reference customers view Renovate as a differentiator. They say that the new combined UI and CLI agent is better but are holding onto policy management features in the legacy UI.
- **Forrester's take.** Mend.io is a great fit for enterprises that need an all-in-one solution for security, license, and operational risk as well as supporting services.

View Mend.io's detailed scorecard.

Veracode

Veracode is an application security SaaS platform, best known as a leader in SAST, that offers SCA, DAST, ASPM, and container image and IaC scanning.

- **Strategy.** Veracode aims to minimize risk by merging various scans, automating fixes, and incorporating Longbow for security risk management into its platform. Veracode's roadmap focuses on software supply chain security capabilities, such as SBOM management, malicious package detection, and regulatory standards templates. An autoprotect feature for securing AI-generated code and patching for breaking updates are anticipated future enhancements. Veracode's support and services offering is a differentiator that helps enterprises scale their application security programs.
- **Capabilities.** Veracode customers can scan binaries to get SCA results as a by-product of a SAST policy scan and can scan source code to get results from the SCA agent that runs in the pipeline. Both find vulnerabilities not listed in the National Vulnerability Database, but the SCA agent, with vulnerable method

analysis, provides more actionable results than the SCA upload and scan. However, the two sets of results cause reporting headaches. Veracode will detect and provide policy violations on noncompliant open-source licenses, but not on third-party, commercial, or closed-source licenses. In addition, workflow around license management is a weakness, and customers are looking for more information from Veracode on the risks that different licenses pose.

- **Customer feedback.** Reference customers commented on the fact that there are two scanners, which means security must be mindful when showing results to development teams.
- **Forrester's take.** Veracode SCA is an ideal add-on for enterprises using Veracode's SAST offering and seeking to understand open-source dependency risk.

View Veracode's detailed scorecard.

Contenders

JFrog

JFrog is a software supply chain platform well known for its artifact management system, Artifactory. The enterprise edition includes Xray SCA. Advanced Security and Curation are add-ons.

- **Strategy.** JFrog's Advanced Security includes SCA contextual analysis, secrets detection, IaC security, misconfiguration detection, and SAST. Curation brings policy governance. The recent acquisition of Qwak, an ML developer platform, reflects JFrog's vision to be the secure MLOps platform for securing binaries and reducing AI component supply chain risk. But the focus is on the JFrog environment, so customers using multiple ecosystems will continue to need separate SCA solutions. The roadmap contains a mix of forward-looking features, such as runtime SBOM creation, image integrity, contextual prioritization, and pinpointing which production workloads are impacted by a vulnerability, and catch-up features, such as transitive vulnerability detection, SBOM ingestion, and augmentation.
- **Capabilities.** Together, Xray, Advanced Security, Curation, and Artifactory provide vulnerability and license detection, policy management, and software supply chain coverage. JFrog can detect and block malicious packages from entering the SDLC and attacks such as dependency confusion — a strength — but it's limited to its ecosystem. It applies the same analysis to open-source AI/ML models and

packages, where teams are blocked from seeing packages on Hugging Face in real time. Analytics and reporting have improved, as one customer noted, but more security-defined metrics, persona-based dashboards, and configurable report downloads are missing.

- **Customer feedback.** Reference customers commented that JFrog's security tools integrate with Artifactory, streamlining developer adoption, but that they must purchase Advanced Security for contextual analysis; otherwise, developers will be overwhelmed by nonimpacting vulnerabilities.
- **Forrester's take.** JFrog is great for development organizations utilizing the JFrog ecosystem.

View JFrog's detailed scorecard.

GitHub

GitHub, a software development platform, hosts open-source code globally. The Advanced Security add-on for GitHub Enterprise and Azure DevOps includes Dependabot, secrets scanning, and SAST.

- **Strategy.** Dependabot is free for open-source repositories, and therefore, many developers are familiar with it. The secure-by-design-heavy roadmap provides synergy with GitHub's Copilot, the GitHub AI pair programmer, and the Advanced Security offering. The roadmap also includes utilizing Copilot to streamline breaking change updates. The narrow focus of the vision and roadmap on developer remediation makes sense for the current user base. However, customers looking for more sophisticated legal workflows, malicious package blocking, or runtime reachability must rely on other security solutions.
- **Capabilities.** The GitHub advisory database is publicly available, one of the largest of its kind, and relied on by other security tools. While automated PRs for vulnerabilities and outdated packages are a strength, transitive dependency detection is weak. Reporting on mean time to remediate, reopen alerts, and unresolved rate provide security with valuable insight. However, reports are canned, and analytics is only based on the current snapshot.
- **Customer feedback.** Reference customers commented that the security scanning is automated and integrated into the development process, which reduces context switching and increases developer adoption.
- **Forrester's take.** GitHub Advanced Security is best suited to development organizations on GitHub Enterprise or Azure DevOps.

View GitHub's detailed scorecard.

Aqua Security

Aqua Security secures and protects cloud-native applications. Dev security includes code repository, container image, IaC, SAST, and pipeline analysis and complements the cloud security offering.

- **Strategy.** Aqua Security's vision to address security early in the SDLC and provide runtime protection for cloud-native applications is not unique, but the execution of that vision in a single platform is. Aqua Security has a strong research team that publishes vulnerability threat reports on novel attacks. Its robust partner program is a differentiator. The vendor incorporates open-source dependency analysis from code to cloud — SCA is a feature but not a product. The roadmap includes runtime workload context for prioritization, enhanced remediation, and KPI dashboards. The absence of a vision or roadmap to improve developer experience and manage security and legal risk beyond open-source components is a weakness.
- **Capabilities.** Multiple development toolchains can be scanned to identify Center for Internet Security (CIS) Benchmarks violations in pipelines, which is a differentiator. Dynamic Threat Analysis exercises container images in a sandbox, identifying malware, backdoors, and additional threats — a unique offering that is limited to containers. Aqua Security maintains Trivy, a popular open-source container image scanner utilized by other vendors in this evaluation. Users can customize assurance policies with multiple criteria and conditions. SBOMs and reports are exportable, but overall reporting and analytics, along with non-open-source dependency management, are weaknesses.
- **Customer feedback.** Customers told us that they choose Aqua Security for container image scanning, but most augment it with another SCA tool for scanning beyond containers.
- **Forrester's take.** Aqua Security's dev security is best when layered with cloud security tools.

View Aqua Security's detailed scorecard.

GitLab

GitLab, a DevSecOps platform, offers a breadth of security scanners and testing with the Ultimate edition.

- **Strategy.** GitLab's defining vision is to enable organizations to adopt DevSecOps. It has the largest number of partners in this evaluation. Compliant-by-default is the theme of its roadmap, with security scanners enabled, configured, and automated to trigger on push events and new advisories. Incorporating development, DevOps, and security activities into one platform increases developer adoption. However, the focus has been on the breadth, not depth, of capabilities. Innovation has focused on development capabilities, typically causing security teams to augment SCA findings with additional intelligence. GitLab plans to rectify this by integrating its GitLab Duo genAI assistant with the security offering and incorporating its two 2024 acquisitions (Rezilion for runtime analysis and Oxeye for SAST) into the platform to prioritize vulnerabilities with runtime and static reachability context, autogenerate fixes, and support binary scanning for SCA users.
- **Capabilities.** Developers appreciate that results from SCA and other scanners are visible in the software development pipeline. However, a lack of reachability analysis keeps GitLab from achieving an on-par score for developer experience. Analytics provides vulnerability trends, and reports, such as SBOMs, are downloadable, but both lack flexibility and metrics compared with others in this evaluation. GitLab has a transparent and comprehensive product security program. It demonstrates secure-by-default best practices with the GitLab CIS Benchmark and component integrity capabilities. In addition, GitLab provides customers with coverage of the software supply chain through an array of security testing tools and controls.
- **Customer feedback.** Customers willingly sift through more alerts and false positives in exchange for a single pane of glass and a single platform for both development and security.
- **Forrester's take.** GitLab Ultimate is a good fit for development organizations that want to integrate security within DevOps practices.

View GitLab's detailed scorecard.

Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

Figure 3

Evaluated Vendors And Product Information

Vendor	Product evaluated
Aqua Security	Aqua Software Supply Chain Security: SCA
Black Duck Software	Black Duck SCA Supply Chain Edition (2024.7.0)
Checkmarx	Checkmarx One, Checkmarx SCA
GitHub	GitHub Advanced Security Dependabot dependency review
GitLab	GitLab Ultimate DevSecOps platform: dependency and container scanning
JFrog	JFrog Software Supply Chain Platform: JFrog Security Essentials, JFrog Advanced Security, JFrog Curation
Mend.io	Mend.io SCA
Snyk	Snyk Open Source, Snyk Container
Sonatype	Sonatype Platform: Sonatype Lifecycle, Sonatype Repository Firewall, Sonatype SBOM Manager, Sonatype Developer, Sonatype Nexus Repository
Veracode	Veracode Software Composition Analysis (3.8.70)

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Evaluation Overview

We evaluated vendors against three categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies, including elements such as vision and innovation.
- **Customer feedback.** A halo on a vendor's marker indicates above-average customer feedback relative to the other evaluated vendors. A double halo indicates outstanding customer feedback: We consider the vendor to be a Customer Favorite. As part of this evaluation, we speak with up to three customers of each vendor. We also consider customer input from our previous research.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **Comprehensive, enterprise-class SCA.** All vendors in this evaluation offer a range of SCA capabilities suitable for security, development, and risk pros. Vendors have most of the following capabilities out of the box: Prioritize and provide remediation advice on both open-source license risk and vulnerabilities, integrate with common SDLC automation tools, provide proactive vulnerability management, edit and create policies, visually report on open-source risk, generate software bills of materials in one or more NTIA-approved formats, guide users in selecting healthy and secure components, and block malicious packages.
- **$40 million or more in SCA revenue.** All vendors in this evaluation earned $40 million or more in global revenue with no more than 90% of direct SCA software revenue attributed to a single region.
- **Interest from and relevance to Forrester clients.** Forrester clients ask about the vendors we included during inquiries and interviews or have use cases that these vendors are well suited to support. Inclusion in this evaluation also means that the vendors actively compete in the SCA market and show up in discussions among Forrester clients.

Other Notable Vendors

The Forrester Wave evaluation is an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market and additional vendors that Forrester considers to be notable for enterprise clients in our corresponding report: The Software Composition Analysis Software Landscape, Q2 2024.

SCA customers may be familiar with or considering the following vendors, which we did not evaluate in this report:

- **Palo Alto Networks.** The vendor utilizes runtime context to prioritize vulnerabilities — a strength — but it does not have the market share to meet the inclusion criteria.
- **Revenera.** The vendor has shifted product strategy focus to the enterprise SBOM management use case (critical for securing the software supply chain) and is deprioritizing differentiating in the SCA market.

Supplemental Material

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 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 and briefings, and reference customer 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 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 August 21, 2024, 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 our vendor review policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. We score vendors that met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation in accordance with our vendor participation policy and publish their positioning along with those of the participating vendors.

Aqua Security declined to participate in the full Forrester Wave evaluation process. For vendors that are not full participants, Forrester uses primary and secondary research in its analysis. For example, we might use public information, data gathered via briefings, and independently sourced customer interviews to score the vendor. We may ask the vendor for an abbreviated briefing and/or to provide reference customers. We may also rely on estimates to score vendors.

Integrity Policy

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

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

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