CATEGORY
SOFTWARE COMPOSITION ANALYSIS SOLUTION OVERVIEW

Software Composition Analysis (SCA) is the procedure of automating the visibility into open source software (OSS) utilization for the purposes of license compliance, security, and risk management. With the increasing use of open source (OS) in software in all sectors, there is a growing need to track components to safeguard firms from open source vulnerabilities and issues. Most software production includes OS which makes it hard to do manual tracking. This increases the need to utilize automation to scan dependencies, binaries, and source code.

SCA platforms have become an essential for app security. They enable enterprises to find OSS evidence via code scanning, to discover licensing issues and vulnerabilities early and minimize remediation expenses. The tools perform automated scans to identify and resolve issues effortlessly.
The FeaturedCustomers Customer Success ranking is based on data from our customer reference platform, market presence, web presence, & social presence as well as additional data aggregated from online sources and media properties. Our ranking engine applies an algorithm to all data collected to calculate the final Customer Success Report rankings. The overall Customer Success ranking is a weighted average based on 3 parts:

**Content Score** is affected by:

1. Total # of vendor generated customer references (case studies, success stories, testimonials, and customer videos)
2. Customer reference rating score
3. Year-over-year change in amount of customer references on FeaturedCustomers platform
4. Total # of profile views on FeaturedCustomers platform
5. Total # of customer reference views on FeaturedCustomers platform

**Market Presence Score** is affected by:

1. Social media followers including LinkedIn, Twitter, & Facebook
2. Vendor momentum based on web traffic and search trends
3. Organic SEO key term rankings
4. Company presence including # of press mentions

**Company Score** is affected by:

1. Total # of employees (based on social media and public resources)
2. Year-over-year change in # of employees over past 12 months
3. Glassdoor ranking
4. Venture capital raised

---

**Customer Success Report Award Levels**

**Market Leader**
Vendor on FeaturedCustomers.com with substantial customer base & market share. Leaders have the highest ratio of customer success content, content quality score, and social media presence relative to company size.

**Top Performer**
Vendor on FeaturedCustomers.com with significant market presence and resources and enough customer reference content to validate their vision. Top Performer's products are highly rated by its customers but have not achieved the customer base and scale of a Market Leader.

**Rising Star**
Vendor on FeaturedCustomers.com that does not have the market presence of Market Leaders or Top Performers, but understands where the market is going and has disruptive technology. Rising Stars have been around long enough to establish momentum and a minimum amount of customer reference content along with a growing social presence.
2019 Customer Success Awards

Check out this list of the highest rated Software Composition Analysis Solution software based on the FeaturedCustomers Customer Success Report.

**Market Leaders**

- BLACKDuck by Synopsys
- Veracode
- WhiteSource

**Top Performers**

- Flexera
- JFrog
- Sonatype
- WhiteHat Security

**Rising Stars**

- FOSSA
- GitLab
- Snyk
ABOUT BLACK DUCK SOFTWARE

Organizations worldwide use Black Duck Software’s industry-leading products to automate the processes of securing and managing open source software, eliminating the pain related to security vulnerabilities, open source license compliance and operational risk. Black Duck is headquartered in Burlington, MA, and has offices in San Jose, CA, London, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing.

“"The real game-changer for us in choosing Black Duck was how it allowed us to not only look into our code base and establish a clean bill of materials, including all OSS components, but also that it allowed us to encourage and support greater use of open source in current and future projects.”

Patrick Holden
Senior Programme Manager, Software Development, SITA

“When we built our business case for bringing in Black Duck, our internal information security group was a co-sponsor of the effort. This group now has a significantly easier way to determine which artifacts and versions are affected by any security vulnerability and which applications are impacted as a result. This capability did not exist before, so this is...”

Kostas Gaitanos
Senior Director of Development Services, FINRA

“Black Duck stands in a class of its own. From a return on investment standpoint, given the breadth of information we receive from the system and the ease of use, versus our expenditure, we find it to be a great investment. Life for us would be very difficult without Black Duck.”

Igor Lekht
Sr. Vice President, AxiomSL

“Black Duck has become a standard part of our due diligence when we buy a software company.”

Steve Clark
Vice President Mergers and Acquisitions, Spirent Communications
Flexera helps executives succeed at what once seemed impossible: getting clarity into, and full control of, their company’s technology “black hole.” From on-premises to the cloud, Flexera helps business leaders turn IT insights into action. With a portfolio of integrated solutions that deliver unparalleled technology insights, spend optimization and agility, Flexera helps enterprises optimize their technology footprint and realize IT’s full potential to accelerate their businesses. For over 30 years, our 1,300+ team members worldwide have been passionate about helping our more than 20,000 customers fuel business success. To learn more, visit flexera.com.

“The benefit for our customers is simple: trouble-free installations that leverage the power of Java to provide the consistent look and feel that Infragistics’s customers have come to expect across all platforms.”

Tim Hitchings
Senior Product Manager, Infragistics, Infragistics

“The right way to provide scalable infrastructure today is via the cloud. To avoid vendor lock-in, organizations need the ability to run on multiple clouds. RightScale (now part of Flexera) gives us an elegant solution that also meets our need for rapid deployment.”

Shay Benchorin
Director of Cloud Services Platform, Mentor Graphics

“This tool provides our CERT team the timely vulnerability information they need to focus on managing IT incidents, rather than hunting down information.”

Angelika Mann
Service Manager, ESA CERT

“Flexera Software’s FlexNet Connect solution enabled us to release our Thomson Reuters Eikon product with best-in-class software update capabilities that gives our customers peace of mind that their real-time financial desktop software will be up-to-date and operational 24/7.”

Andrei Borsaru
Thomson Reuters
TRUSTED BY

ABOUT FOSSA

FOSSA’s flagship product helps teams track the open source used in their code and automate license scanning and compliance. Since then, over 3000 open source projects (Kubernetes, Webpack, Terraform, ESLint) and companies (Docker, Tesla, Mapbox, Hashicorp) rely on FOSSA’s tools to ship software. If you are in the software industry today, you’re now using code that runs FOSSA. Open Source has become a critical supplier for modern software companies, changing everything about how people think about their code. FOSSA builds the infrastructure for modern teams to be successful with open source.

8 Customer references from happy FOSSA users

“FOSSA handles a tremendous amount of compliance work that would normally take us months to do.”
Faryar Ghazanfari
IP Counsel, SolarCity

“FOSSA was a huge relief... the big surprise was how easy it was!”
Dean Hemstreet
Vice President Q/A & Release Engineering, SmartThings

“Every Open Source organization should implement license & dependency tracking. Based on our experience, we would recommend FOSSA to organizations that have large projects or lots of on-going projects. And especially if you’re using JavaScript.”
Kris Borchers
Executive Director, JS Foundation

“When I found FOSSA, I thought it sounded too good to be true – I had never heard of a solution that could do this. During our free trial, the FOSSA app found all the dependencies and licenses. The team was also great to work with – they were always incredibly responsive when we had questions or concerns during the on-boarding process.”
Rob Mason
Senior Vice President of Engineering, Applause, Inc.
ABOUT GITLAB

GitLab is a company based on the GitLab open-source project, helping developers collaborate on code to build great things and ship on time. They are an active participant in their global community of customers and contributors, trying to serve their needs and lead by example. They have one vision: everyone can contribute to all digital content, and their mission is to change all creative work from read-only to read-write.

“GitLab has allowed us to dramatically increase the velocity of development in our Engineering Division. We believe GitLab’s dedication to helping enterprises rapidly and effectively bring software to market will help other companies achieve the same sort of efficiencies we have seen inside Goldman Sachs. We now see some teams running and...

Andrew Knight
Managing Director, Goldman Sachs

“Essentially, we look at GitLab as a building block, and we just build whatever we need on top of it. Whether it’s a wiki or a custom integration, GitLab helps create an engineering culture.”

Jared Short
Director of Innovation, Trek10

“GitLab from my perspective was vastly outpacing the competition in terms of feature releases. GitLab was later to the SCM game in comparison to GitHub or BitBucket, for instance, but with the rate of features being released it was very clear that you guys were gaining so much ground compared to the competition.”

Brendan Mannix
Vice President, Engineering, EAB

“Moving into a system like GitLab will help any organization or enterprise to get into DevOps methodology and continuously improve the deployment workflows to achieve quality, agility, and self-serviceability.”

Bala Kannan
Senior Software Engineer, Equinix
JFrog's mission is to provide better technologies and tools for the everyday use and to increase the effectiveness of the software development software. JFrog's core values are based on non-compromising professionalism, superior quality code, first-class service, strong customer relationships, mutual trust and integrity. Through Artifactory, it is the first company to provide software developers with a binary repository management solution. Winner of the JavaOne Duke's Choice Award, JFrog has established itself as a technology leader in the software industry. The company continues to set the standard for solving developer pains with the launch of Bintray, deemed “the missing link in social software distribution” by peers.
ABOUT SNYK

Snyk’s mission is to help developers use open source code and stay secure. Snyk’s unique developer focused product enables developers and enterprise security to continuously find & fix vulnerable dependencies without slowing down, with seamless integration into Dev & DevOps workflows. Snyk is adopted by over 100,000 developers, has multiple enterprise customers (such as Google, New Relic, ASOS and others) and is experiencing rapid growth.

“Snyk’s immediate notification on a newly disclosed critical Ruby vulnerability enabled us to react quickly and upgrade our front-door applications using Snyk’s automation.”
Tom Czarniecki
Tech Lead, DigitalOcean

“Snyk is one of the most important security tools we use at Skyscanner. You’ll realise how important it is when you actually get it integrated.”
Alex Harriss
Security Engineer, Skyscanner

“One of the development teams tried Snyk’s open source free version and highly recommended it would be adopted throughout the organization. The team claimed it is better than our existing solution by a different vendor.”
David Mark
DevOps Team Lead & Cloud Architect, StartApp

“Prior to having Snyk, out-dated dependencies were definitely a major concern. We didn’t have time to research each package for security posture or for security vulnerabilities or put a system in place to apply manual patches.”
Girish Nair
Head of Engineering, Comic Relief
The Sonatype journey started 10 years ago, just as the concept of “open source” software development was gaining steam. From our humble beginning as core contributors to Apache Maven, to supporting the world’s largest repository of open source components (Central), to distributing the world’s most popular repository manager (Nexus), we’ve played a meaningful role in helping the world embrace the power of open innovation. Over time, we witnessed the staggering volume and variety of open source libraries that began flowing into every development environment in the world. We understood that when open source components are properly managed, they provide a tremendous energy for accelerating innovation. Conversely, when unmanaged, open source “gone wild” can lead directly to security vulnerabilities, licensing risks, enormous rework, and waste. Our vision today is simple. We are laser focused on helping organizations continuously harness all of the good that open source has to offer, without any of the risk. In order to do this, we have invested in knowing more about the quality of open source than anyone else in the world. This investment takes the form of machine learning, artificial intelligence, and human expertise, which in aggregate produces highly curated intelligence that is infused into every Nexus product. Organizations equipped with Nexus products make better decisions, innovate faster at scale, and rest comfortably knowing that their applications always consist of the highest quality open source components. Today, more than 150,000 organizations, and 10 million developers, depend on Sonatype’s Nexus platform to govern the volume, variety, and quality of open source components flowing into modern software applications. Sonatype is privately held with investments from TPG, Goldman Sachs, Accel Partners, and Hummer Winblad Venture Partners.

“By layering automation and instrumentation through our pipelines we were able to reduce the average time for new applications from 25 days to 2.5 days, with the record of 8 minutes from desktop to cloud.”
Edward Webb
Director, Software Delivery Platforms, Liberty Mutual

“Before Lifecycle, we really had no way to monitor policy violations or licensing risks. Lifecycle gave us a way to actually prioritize what to fix.”
Edwin Kwan
Application and Software Security Team Lead., Tyro Payments

“Without Nexus Lifecycle, you just don’t know the true composition of your applications, and what elements of security, legal, and licensing risk you’re exposed to. A security breach that results in just a 1% hit to the customer base can manifest itself as hundreds of millions of dollars lost.”
Brian Heemsoth
Director of Software & Mobile Security, Addteq

“With Lifecycle, we can help programmers make the right decisions and make their software more secure. That’s why we chose Nexus Lifecycle.”
Stefan Simenon
Head of Centre of Expertise Software Development & Tooling, ABN AMRO
ABOUT VERACODE

Veracode delivers the most widely used cloud-based platform for securing web, mobile, legacy and third-party enterprise applications. By identifying critical application-layer threats before cyber-attackers can find and exploit them, Veracode helps enterprises deliver innovation to market faster — without sacrificing security. Veracode’s powerful cloud-based platform, deep security expertise and programmatic, best practices approach provide enterprises with a simpler and more scalable way to reduce application-layer risk across their global software infrastructures. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world’s largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 25+ of the world’s top 100 brands.

“Deployment of Static Analysis was smooth, easy and the results were something we could act on immediately, helping us prioritize development activities.”

Dave Casion
Co-founder and Chief Technology Officer, Rekener

“When I talk to people about Veracode, I talk about the ease of use and the rollout. As compared to on premise options, the startup time is in minutes. And it’s easy to use by the developers because it makes it easy to fix the flaws. It’s been a huge success.”

US state government
State Government

“When I talk to people about Veracode, I talk about the ease of use and the rollout. As compared to on premise options, the startup time is in minutes. And it’s easy to use by the developers because it makes it easy to fix the flaws. It’s been a huge success.”

Nikki Veit
State of Missouri

“I don’t think that we would have been able to expand the program [that we had before Veracode] to the point that we have now, due to the added complexity of our legacy application estate. We would have needed to add 15 FTEs to the team.”

Head of application security
Financial Services Organization
ABOUT WHITEHAT SECURITY

Headquartered in Santa Clara, California, WhiteHat Security is a leading provider of website vulnerability management services. WhiteHat delivers turnkey solutions that enable companies to secure valuable customer data, comply with industry standards and maintain brand integrity. WhiteHat Sentinel, the company’s flagship service, is the only solution that incorporates expert analysis and industry-leading technology to provide unparalleled coverage to protect critical data from attacks.

“WhiteHat Sentinel Source immediately improved security and saved us time and effort, all without having to change any of our infrastructure. Importantly, with Sentinel Source running in parallel with Sentinel Dynamic, we now have full coverage throughout our entire SDLC.”

Alper Ümit Yilmaz
Director of IT Service & System Operations, N11.com

“Sentinel is validation for us that our website security program is headed in the right direction. We now have more visibility into our security posture and the ability to effectively solve issues.”

Josh Sokol
Information Security Program Owner, National Instruments, National Instruments

“WhiteHat has the validation if the vulnerability that’s discovered is a false positive or not, and that’s extremely powerful for us since we’re a small group focusing on building the software securely. When you have WhiteHat as a strategic partner in the solution, it’s easier to figure out.”

John Pescatore
Director of Emerging Security Trends, Sans What Works

“We’ve used Sentinel reports to clearly illustrate the state of security across the front line of our products to prospects and clients. It has actually become a valuable sales and compliance tool for us.”

Jason Shah
Chief Technology Officer, Mediafly
ABOUT WHITESOURCE

WhiteSource is the leader in continuous open source security and license compliance management. Its vision is to empower businesses to develop better software by harnessing the power of open source. Industry leaders like Microsoft, IBM, and hundreds more trust WhiteSource to secure and manage the open source components in their software.

“Our agile framework and demanding ecosystem made it clear that we must use a solution like WhiteSource to automatically manage our open source components, dependencies and versions.”

Gev Decktor
VP Software Development, Panoramic Power

“We chose WhiteSource because of its ease of use, its excellent data, and for the in-depth security vulnerability information that comes with the reporting engine.”

Neil Langmead
Code Clinic Lead, Siemens Healthineers

“With WhiteSource I have full view of what's in each of the software versions, no matter where and by whom it was customized.”

Yvan Perrenoud
Software & Controls Quality Manager, Swisslog

“WhiteSource helps us reduce legal and security risks associated with the use of certain open source components. WhiteSource continuously alerts us on security vulnerabilities that affect our product. When the question of open source usage came up during a due diligence process, we created an open source inventory report in one click.”

Arik Priel
Vice President of R&D, LetMobile