SOFTWARE COMPOSITION ANALYSIS 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.

An SCA tool permits safe risk management of open source utilization across the software supply chain. It allows developers and the security squad to produce a precise Bill of Materials (BOM) for all your apps, find and monitor all open source components, smoothly include open source code scanning in the build environment, enable continuous and proactive monitoring, and set and implement policies.
Customer Success Report
Ranking Methodology

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.
2020 Customer Success Awards

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

Market Leaders
- Black Duck by Synopsys
- Flexera
- JFrog
- Sonatype
- Veracode

Top Performers
- Checkmarx
- GitLab
- Snyk

Rising Stars
- CAST
- FOSSA
- Praetorian
OVERALL BEST OF SOFTWARE COMPOSITION ANALYSIS

BEST IN CATEGORY

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.

“Veracode enables me to provide better code, faster, so my time to market is less.”
Jim Nelms
Chief Information Security Officer, LabCorp

“The security of our products and services is very important to us, and Veracode helps us ensure that we never lose our customers’ trust and confidence.”
Tabrez Naqvi
Director of Information Security and Risk, Cox Automotive

“It has allowed us to scale and find vulnerabilities much faster than previous manual tools.”
Suzan Nascimento
SVP of Application Security, Union Bank

“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
2020 MARKET LEADERS

BLACKDUCK
by SYNOPSYS

FLEXERA
Inform IT. Transform IT.

JFROG

SONATYPE

8
ABSTRACT 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.

“Essentially, from a technical standpoint, Black Duck met Entersekt’s checklist of what we needed in an open source vulnerability management solution better than any other vendor. The responsiveness and support from both its customer success and technical support teams also led us to make the business decision to select Black Duck.”

Philip Botha
QA Manager, Entersekt

“What Black Duck does is put a light on open source code problems prior to release of a new version of our product. It’s helped us correct issues, plus ensure we don’t have similar issues in the future.”

Scott Martin
Director of Security Compliance, ScienceLogic

“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

“Automating the search and selection of OSS with Black Duck gives us the tools we need to put customers at ease.”

Kellen Ponikiewicz
IP Counsel, Nuance Communications

49
Customer references from happy Black Duck Software users

VIEW ALL REFERENCES
ABOUT FLEXERA

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.

194

Customer references from happy Flexera users

VIEW ALL REFERENCES

“When choosing our monetization platform, we were looking for more than just a licensing tool. We wanted better insight into our customer base, offer flexible and scalable monetization models and add the automation needed to run our growing software business. Flexera is the strong partner we need to deliver on these strategic goals.”

Mike Tresh
Product Management Director Platform, Thingworx

“Within weeks of deployment, FlexNet Manager Platform provided the information necessary to reduce our enterprise agreement license count by 125 licenses. Our return on investment took approximately seven months and over the next three years we are expecting six-figure savings.”

David Meacham
IT Disaster Recovery and Operations Support Coordinator, Osmose Holdings, Inc

“There is absolutely no reason to build your own licensing mechanisms when Flexera Software offers everything you need to protect your IP and fulfill your customer’s needs in today’s complex, relentlessly evolving technology markets.”

Bob Masson
Marketing Director, Convey Computer

“The FlexNet Manager solution has given us an automated process in which we can track license usage more accurately and maintain control over our EDA purchasing decisions.”

Dan Griffith
Manager, EDA Business Relations and Asset Management, Freescale Semiconductor
ABOUT JFROG

JFrog’s mission is to provide better technologies and tools for the everyday use and to increase the effectiveness of software development. 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.

“Customer references from happy JFrog users

Joe Lind
Best Buy

“As a long-time DevOps engineer, I know how difficult it can be to keep track of the myriad of package types – legacy and new – that corporations have in their inventory. JFrog has always done a phenomenal job at keeping our team supported, efficient and operational – because if JFrog goes out, we might as well go home. Thankfully, with AWS...

Joel Vasallo
Head of Cloud DevOps, Redbox

“With JFrog Artifactory & Xray, the engineering teams at Puppet have been able to overcome the complexity of working with different software package management systems (including RubyGems, npm, rpm and Maven) and we now have greater consistency and transparency of our CI/CD workflow.”

Rob Braden
Engineering Manager, Puppet

“Since we deliver critical communication infrastructure for our customers, we have to be sure each release is rock-solid. JFrog has always done an amazing job at keeping our team in sync, automating tasks, integrating with our external tools and delivering the tracking and support we need. With AWS infrastructure behind us, we know we can continue to...

Tyrone Johnson
Sr. SRE and Delivery Manager, Avaya
ABOUT SONATYPE

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.

"We are dealing with patient data and healthcare data. Security comes above everything. The fact that we can trace vulnerabilities and their dependencies with Nexus Lifecycle alleviates this from our list of things do.”

Tudor Groza
Chief Technology Officer, Genome.One

"We needed constant monitoring and notifications of open source vulnerabilities in our applications. That’s what Nexus Repository, Nexus Lifecycle and IQ Server delivered.”

Nick Alexander
Systems Architect, Discovery Health

“The biggest advantage of using IQ Server is to be able to report to our project team what specific libraries are used within our applications. We have immediate visibility into security issues.”

Olivier Router
Head of CI DevOps Engineering Team, The EDF Group

“Through the use of Nexus Lifecycle, our team can proactively ensure open source security vulnerabilities are precisely identified, managed and resolved before they can impact our customers.”

David Blevins
CEO, Tomitribe
ABOUT WHITESOURCE

Whitesource is the leading solution for agile open source security and license compliance management. It integrates with your development environments and DevOps pipeline to detect open source libraries with security or compliance issues in real-time. Whitesource doesn't only alert on issues, it also provides actionable, validated remediation paths to enable quick resolution and automated policy enforcement to speed up time-to-fix. It also helps you focus on what matters by prioritizing remediation based on whether your code is actually using a vulnerable method or not, and guaranteeing zero false positives. We've got you covered with support for over 200 programming languages, and continuous tracking of multiple open source vulnerabilities databases including the NVD, security advisories, peer-reviewed vulnerability knowledge bases, and open source projects issue trackers.

44
Customer references from happy WhiteSource users

“With Whitesource, we are able to see all our open source information in one place. The dashboards give us a good, up-to-date overview of the open source in our software.”
Albrecht Scheidig
Head of Product Development, HYPE Innovation

“We looked for a solution that would provide us with an up-to-date, open source report whenever we need it. Whitesource does just that – the report is always a click away.”
Gil Maletski
CTO, Sapiens

“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

“With Whitesource we have a comprehensive inventory of all the Open Source components, and can ensure full compliance with our license policies. This also means we can rapidly answer any questions from prospects and be certain we are 100% accurate in the information we are providing, all without wasting any of our developers’ valuable time.”
Martin Bailey
Product Director, Temenos
2020 TOP PERFORMERS

Checkmarx

GitLab

snyk

WhiteHat Security
AN NTT COMPANY
ABOUT CHECKMARX

Checkmarx, founded in 2006, is a leader in application security solutions, having developed the first platform for true Source Code Analysis (SCA) with its marquee solution: Static Application Security Testing (SAST). Checkmarx’s mission is to enable organizations to secure applications from the start, reducing risk and cost along the way. Platforms offer maximum application security for software developers and security experts throughout the Software Development Life Cycle (SDLC), in both Enterprise and Cloud platform models.

"Checkmarx was by far the most integrated and simplest to get up and running. It allowed our development team, with minimal effort, to gain tremendous insights into our code in very short order."

Jason Barr
CIO and CISO, Aptean

"Having the capability with Checkmarx to scan in different languages makes it much easier for us as we can unify all the analytics in one single platform."

Rafael Santos
Cybersecurity Analyst, Globo.com

"Checkmarx simply had the best solution for us. Their product was very easy-to-use. Being able to "remember" what was non-exploitable from one scan to the next really helped our effectiveness. Due to the success we've seen with the Checkmarx application security testing, we are looking to expand the use of static analysis to other areas outside..."

Chris Kings-Lynne
R&D Manager, Navitas

"Checkmarx’s technology is highly accurate and easy to use. It offers great performance and the ability to scan incomplete code samples. Checkmarx was agile enough to support specific requests we had for our secure SDLC and was the most sensible decision commercially."

Yair Rovek
Security Specialist, LivePerson
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.

"We applaud GitLab for dropping their CLA in favor of a more OSS-friendly approach. Open source communities are born from a sea of contributions that come together and transform into projects. This gesture affirmed GitLab’s willingness to protect the individual, their creative process, and most importantly, keeps intellectual property in the..."

Carlos Soriano
Board Director, GNOME

"With GitLab and Kubernetes, I can have three deploys a day — unlike the classic release cycle of every three months. I know from my steps that the test has passed, and I can promote automatically from staging to production directly in GitLab."

Paride Martino
Senior System Engineer, Glispa

"We decided to use an Open Source based platform so we can participate in the development and contribute to the features and concepts we need such as file size statistics, OpenID Connect, GPG, and Docker Registry. GitLab’s built-in Continuous Integration and independent CI Runners allows our developers to integrate very specific environments,..."

Roger Meier
Social Coding Platform, Siemens Healthineers

"One tool for SCM+CI/CD was a big initial win. Now wrapping security scans into that tool as well has already increased our visibility into security vulnerabilities. The integrated Docker registry has also been very helpful for us. Issue/Product management features let everyone operate in the same space regardless of role."

Adam Dehnel
Product Architect, BI Worldwide
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 hosted services are so simple for Coveo to manage. Now our developers are empowered to handle vulnerability and license management on their own.”
Jean-Philippe Lachance
Security Analyst, Coveo

“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

“Open source license compliance wasn’t on our radar initially but Snyk changed that and makes it a lot easier for us to effectively manage the different licenses we use across our projects.”
Ryan Kimber
Founder and CEO, FormHero

“Snyk simplifies our continuous delivery pipelines by directly integrating security. Now, our pipelines are shorter, and new applications and features go into production faster. Ultimately, this means we can deliver value to the business faster and more securely.”
Kirill Kolyaskin
Lead Cloud Engineer, New10
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.

51
Customer references from happy WhiteHat Security users

"We have remediated critical security vulnerabilities on our premium customer facing websites. Since WhiteHat performs continuous scanning, it keeps us always on our toes to the next imminent threats. WhiteHat has helped us immensely to make our critical customer facing web properties safer."

Ravi C.
NetApp

"WhiteHat has identified some significant vulnerabilities in our code that we might not have detected ourselves. We were able to share this information with our entire development team, which has led to more secure code being deployed to production."

Benjamin Mallo
IT Director, AssetMark

“We were able to develop a process that integrated WhiteHat Sentinel’s scoring system and prioritized vulnerabilities into our own security KPI scores to inject security as a part of the SDLC.”

Mikhael Felker
Director of Regulatory and Compliance, ReachLocal

“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
RISING STARS
2020 RISING STARS

CAST
Software Intelligence for Digital Leaders

FOSSA

PRAETORIAN
ABOUT CAST

CAST is an independent software vendor that is a pioneer and world leader in Software Analysis and Measurement (SAM). With more than $120 million cumulative investment in R&D, CAST provides the most advanced technology in the world to capture and quantify the reliability, security, complexity and size of business applications. CAST introduces fact-based transparency into software asset management, application development, maintenance and sourcing to transform it into a management discipline. More than 250 companies across all industry sectors and geographies rely on CAST to prevent business disruption and build a transparent dialogue with their service providers. CAST is also an integral part of software delivery and maintenance at the world’s leading IT service providers and independent software vendors.

158
Customer references from happy CAST users

VIEW ALL REFERENCES

“The CAST platform can analyze all layers of complex applications; from coding best practices, to compliance with architectural standards including middleware and integration framework, identifying problems in different application layers.”

Leonardo

“CAST improves our visibility on application quality across our systems and allows us to steer our development lifecycle, while improving the alignment and satisfaction between IT and the business.”

Jörg Müller
Director of Information Technology Services, Atradius

“CAST AIP enables us to perform systematic, extensive and automated code reviews, throwing light on code quality issues before they become major production problems.”

Jürgen Bodtländer
VP of Application Development, Deutsche Bahn

“CAST enabled us to completely change what we demand from suppliers, and we now have a way of effectively reviewing their source code and receiving regular reports on their progress.”

Xavier Escudero
Head of Quality Assurance, CTTI
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.

14
Customer references from happy FOSSA users

VIEW ALL REFERENCES

“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.

“By using FOSSA and Screwdriver, Verizon Media can deploy software at scale with confidence. Continuous integration, continuous delivery, and continuous compliance are required for any product to provide value.”
Gil Yehuda
Director of Open Source, Verizon Media

“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

“Integrating FOSSA within the build process for Verizon Media mobile apps not only ensures apps are compliant with open source licenses but also generates automated credit reports that we include in each app.”
Mani Subramaniam
Software Development Engineer, Verizon Media
ABOUT PRAETORIAN

Praetorian is an information security consulting firm that provides risk assessment, penetration testing, secure software development, computer forensics, and security education services. Praetorian’s expertise and client base spans all major verticals. They regularly provide expertise to Fortune 500 companies across the financial, technology, healthcare, insurance, oil & gas, and manufacturing sectors.

“They are industry leaders in what they do. On the tabletop side, on the penetration testing side, I knew that if I brought in Praetorian I would get exactly what I was looking for and more.”

Chris Castaldo
Senior Director of CyberSecurity, 2U

“We found it to be a highly collaborative process. I highly recommend Praetorian for anyone looking for outside security expertise. They truly act as partners and their depth of expertise in unrivaled in the industry.”

Brent Stackhouse
Director of Security, WP Engine

“Praetorian’s approach was very professional, to the point and comprised of in-depth analysis of the security vulnerabilities, which was greatly beneficial to us.”

Fakhr Ul-Islam
Director Product Management IOT, Kimberly-Clark

“Praetorian had one of the best IoT domain expertise and the security expertise for various areas. What we liked was the fact that the team was very responsive, it had the relevant expertise, and more importantly, the collaborative nature of a resolving issue or improving the overall architecture. The back and forth discussions were very good.”

Vish Pai
Sr Manager, Product Management, Samsung ARTIK

31
Customer references from happy Praetorian users
VIEW ALL REFERENCES