




Software Composition Analysis

How to Choose the Right Solution



Contents

What Is SCA and Why Is It Important?	3
Governance SCA Solutions & Developers Sca Tools.....	3
How Does SCA Support Devsecops in Your Organization?	4
Breaking Down SCA: 4 Essential Capabilities.....	4
Empowering Open Source Automation With Usage Analysis	9
The Mend Edge.....	10



WHAT IS SCA AND WHY IS IT IMPORTANT?

Open source components have become an integral part of today's software development processes. Open source enables companies to build better products, faster.

After all why should you re-invent the wheel when you can just download it from GitHub?

However, it's still your responsibility to ensure that all of the components in your products are secure and compliant with your company's policies.

The problem is that verifying that each and every open source component used is secure and complies with your company's policies has become increasingly complex. That's because information about open source components is scattered across hundreds of sources



with varied levels of credibility, and most databases are not easily searchable.

So how can you get the control you need over your open source usage? Through automation! And this is where Software Composition Analysis (SCA) tools come in.

GOVERNANCE SCA SOLUTIONS & DEVELOPERS SCA TOOLS

SCA tools automatically detect the open source components in your applications and help you manage the different aspects related to your open source usage. Most SCA tools fall into one of the two following categories: governance tools which enforce policies in real time and generate reports, or developers' tools which alert developers on issues within their development environment and provide remediation guidance.

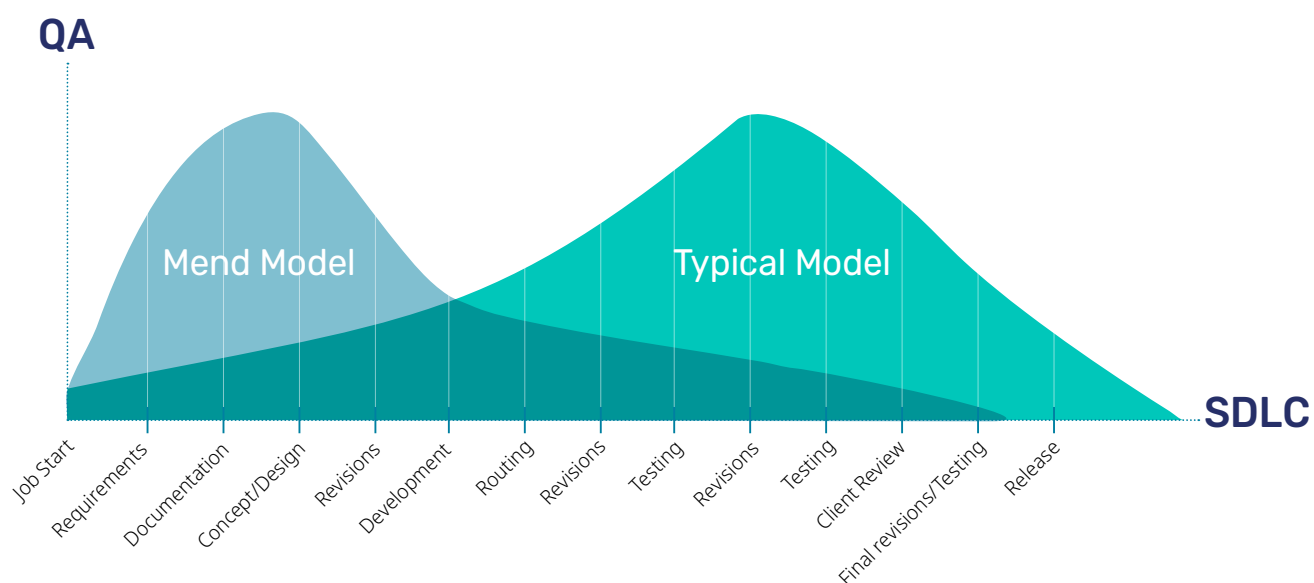
Each category has important benefits, but is strongly focused on its target audience. Only combining both types of tools can provide a solution that addresses the needs of the entire organization. Security, DevOps and legal teams get the visibility and control that they need, while developers get the tools that they need in order to prevent and fix open source security and compliance issues.

	Governance Solutions 	Developers Tools 
Used by	Management, Security teams, DevOps, Legal teams	Developers
Focus	Provide visibility and control over open source risks across the software portfolio	Provide information to help developers avoid and fix vulnerabilities and noncompliant open source licenses
Features	Reports, real-time alerts, policy enforcement by blocking disallowed open source components	Integrates with native development environments and DevOps tools, provides alerts during early stages of selection and usage of open source components. Actionable insights to help developers easily fix vulnerabilities
What's missing?	It doesn't alert developers in real-time within their environments on security, quality or compliance issues and doesn't provide actionable remediation guidance for quicker resolution	It doesn't provide security and legal teams a solution to enforce policies throughout the SDLC, generate custom reports and get cross-organization visibility

HOW DOES SCA SUPPORT DEVSECOPS IN YOUR ORGANIZATION?

DevSecOps, sometimes called DevOps Security or rugged DevOps aims to integrate security into every stage of the development cycle—from planning and design to development, testing, deployment, production, and maintenance. SCA tools can help to enable a DevSecOps culture by helping developers, IT, security and legal teams share responsibility over open source risks.

In the past, management would sometimes enforce open source security standards and block components from use, without the awareness or involvement of development teams. Other times, developers would use their own tools to detect and avoid open source vulnerabilities, with no visibility to other teams or external auditors. Adopting an SCA technology that provides both developer-focused tools and governance solutions, puts developers, IT, security, and legal on the same page.



Breaking Down SCA: 4 Essential Capabilities You Need In Order to Use Open Source Technology Effectively

Which capabilities does your organization need in order to benefit from open source usage, without being exposed to open source security vulnerabilities and legal risk? Below are four essential capabilities, and associated challenges you may run into as you try to implement them.



Vulnerability
Detection



Vulnerability
Remediation



Inventory
Management



Open Source
License Compliance

VULNERABILITY DETECTION



You must be able to discover open source components with known vulnerabilities as early as possible, when remediation is easiest. Once a vulnerability is publicly disclosed, you are in a race against hackers to fix it. If you don't know that you are using a vulnerable open source component, you can't win this race.

The Challenge

It's difficult to gather information about open source vulnerabilities

Knowledge about open source vulnerabilities is scattered across multiple sources, many of them are under-the-radar, with different levels of credibility. You need access to all available information to address known vulnerabilities.

False positives

Many SCA tools frequently raise false alarms, making it more difficult to act on the data.

Detection is crucial in every stage of the SDLC

It's not enough to check at the gate. New components are introduced at every stage of the SDLC.

New vulnerabilities are constantly discovered

New vulnerabilities can be discovered in components that were previously thought to be secure.

Mend Offering - Identifying Vulnerable Components: Essential Features

Identifying Vulnerabilities	Aggregates dozens of sources: NVD, security advisories, open source project issue trackers. Rapid assessment of reported vulnerabilities to validate the information
Accuracy and False Positives	Guarantees zero false positives. The patent-pending algorithm matches vulnerabilities with the specific components that they impact, ensuring relevance.
Real Time Alerts	The components and vulnerabilities DBs are updated multiple times a day. Immediately provides comprehensive information to prioritize and fix vulnerabilities.
Reporting and Auditing	Offers pre-built reports for all use cases. Supports R&D management, security, legal, management, compliance, due diligence.

VULNERABILITY REMEDIATION



In order to mitigate open source risks, it's essential to remediate open source vulnerabilities as soon as they are discovered. However, in most cases it's impractical to fix all vulnerabilities, and some require major development work. You must prioritize vulnerabilities, understand which ones represent a real risk, and provide development and IT teams with the information that they need in order to quickly fix the most critical vulnerabilities first. You must also help teams shift left and discover vulnerabilities earlier, making remediation easier.

The Challenge

Fast response is critical

When a new vulnerability is discovered, you must fix it fast before hackers exploit it. However, many remediations require major development work.

Prioritization

In order to make remediation efficient, you must be able to quickly prioritize vulnerabilities that matter.

Open source component selection

The best remediation is avoiding insecure components when they are initially selected for a project. This requires integrating security at early stages of development.

Locating vulnerabilities in the code

Once a vulnerability is discovered, it's difficult to pinpoint where it is referenced in the code

Mend Offering - Vulnerability Remediation: Essential Features

Prioritization	Analyzes how affected libraries are actually used in your code. Eliminates 70-80% of vulnerability alerts which have no impact on the current project.
Pinpointing Vulnerabilities in Code	Provides a complete trace analysis for each vulnerability. Shows which part of your code touches the vulnerable functionality, down to the line number.
Shift Left	Scans popular repos, including GitHub repos using its GitHub integration Browser extension gives developers information about components as they browse the web
Shift Right	Tracks the "Bill of Materials" of the latest build of every version you deploy. Alerts teams in real-time if new vulnerabilities are reported, with remediation guidance.
Vulnerability Remediation	Sources patches and suggested fixes from hundreds of trusted open source communities. Offers developers multiple remediation options, with scoring.
Automated Policy Enforcement	Enables granular policies per the project, product, app type, or organization. Allows you to set policies for each stage of the SDLC: planning, development, deployment, production. Policies can be conditional on security parameters such as severity or a specific CVE.

INVENTORY MANAGEMENT



It's crucial to identify which open source components are in use in your software. To fully manage open source security, licensing, and compliance issues, you must gain visibility into open source code usage across all stages of the SDLC—from the selection stage to development, deployment and production stages.

The Challenge

Manual inventory management is extremely time consuming

Developers spend precious time checking licenses and security and requesting approval. These processes can be automated.

Support for multiple languages and frameworks

Automated tools must support all of the languages and frameworks used in your organization to accurately track open source components.

It's difficult to gather information about open source components

Information about open source components, versions and licenses is spread across hundreds of sources. Tracking it manually is extremely complex.

Detecting transitive dependencies

Most open source components are dependant on other open source components, creating complex dependency trees.

Mend Offering - Inventory Management: Essential Features

Languages and frameworks coverage	Supports over 200 languages, frameworks and development environments
Integrations with DevOps tools	Integrates with IDEs, package managers, repos, build tools, CI servers and AST tools. Alerts about problems and guides teams as they select and download components.
Open Source Components Database	Doesn't rely on proprietary data—aggregates information about open source components from hundreds of sources, multiple times a day.
Dependency Detection	Detects open source components based on SHA file signatures. Fully resolves dependency tree and manifest files, including undeclared dependencies.
Automated Policy Enforcement	Automates selection, approval, and tracking of open source components. Policies defined per SDLC stage, product, and organization.
Reporting	Provides built-in reports at the project, product or organization level. Open source Bill of Materials, due diligence report, risk and attribution reports.

*An attribution report tells you which components require you to publish attributions, crediting the project creators

OPEN SOURCE LICENSE COMPLIANCE



You must establish an open source usage policy, and block inappropriate or overly restrictive open source licenses. You must also ensure that you are meeting license requirements for all of the open source components used in your software. Management, security, legal teams, and third parties such as investors conducting due diligence need complete visibility over open source licensing.

The Challenge

Manual license management is extremely time consuming

Applications use thousands of open source components. Managing their licenses manually creates overhead and slows down development.

Expert review is required in some cases

Even when using automated tools, there must be a way to perform a review for some types of licenses.

Inaccurate detection

Less advanced automated SCA tools do not always accurately detect licenses. Associating libraries and licenses is not trivial. Missing problematic licenses can incur major costs later on.

False positives

Some SCA tools raise false alarms, placing a burden on teams, or miss problematic licenses leading to liability.

Mend Offering - License Compliance: Essential Features

Languages and frameworks coverage	Supports over 200 languages, frameworks and development environments
Accuracy	100% license detection accuracy unique ability to associate folders and libraries. Shows licenses for the entire dependency tree. Supports multiple licenses for one component.
Real-Time Alerts	Alerts which license types are in your software, with a full risk analysis. Offers suggestions for resolution based on organizational policies.
Shift Left	Provides a native Github integration—scans GitHub repos and discovers license information. Provides a browser plugin that helps avoid problematic licenses at the selection stage. Integrates with DevOps tools at all stages of the SDLC and alerts about license issues.
Automated Policy Enforcement	Automates the license approval process. Extends license tracking and approval to the full dependency tree of each package. Can automatically approve, reject, or initiate a manual workflow, depending on license type.
Reporting and Auditing	Offers a wide range of reports built for all relevant organizational roles. Provides visibility for internal teams—R&D or IT management, security, legal, management. Provides visibility for compliance auditors and due diligence investigators.

EMPOWERING OPEN SOURCE AUTOMATION WITH EFFECTIVE USAGE ANALYSIS

Automation of open source vulnerability management and license compliance is critical to solving the challenges we outlined above. However, automated tools have their limitations.

Previous generations of SCA tools were able to detect open source components and tell organizations they have vulnerabilities but were not able to identify the potential impact of those vulnerabilities. This required security and development teams to invest many resources in investigation and response to a large number of vulnerability reports.



**EFFECTIVE
Vs.
INEFFECTIVE**



Research has shown that of the vulnerabilities discovered, 70-85% were not really critical, because the vulnerable open source code was not actually accessed or used by the organization's proprietary code.

Mend pioneered the next generation of SCA with Effective Usage Analysis. This technology doesn't just tell you what open source components you have, but also how you use them. It lets you hone in on the 15-30% of open source vulnerabilities that are actually in active use within your product.

It also shows exactly where a vulnerable functionality is referenced within the code, making it much easier for developers to fix vulnerabilities.

Effective Usage Analysis provides automatic prioritization that can reduce remediation efforts, and help teams fix important vulnerabilities much faster.

THE MEND EDGE

We have covered numerous considerations for selecting an SCA tool for your organization. The bottom line is that you should select an SCA tool that enables you to minimize risk and reduces the effort for all of your teams—from management, legal and security through ops, developers and QA engineers.

Mend is the leading SCA platform. It helps you minimize risk with the lowest possible effort while fostering a DevSecOps mindset and cooperation across your organization:



Completeness

A one-stop-shop for all of your open source usage regardless of your languages or environments, including containers and serverless. We also support all groups in your organization: Security, Developers, DevOps.



Prioritization

Focus on what really matters. We help you to prioritize the security vulnerabilities that actually impact your products, and ensure there are no false positives.



Remediation

Alerts are great, and we also provide the fix. Automatically generate fix pull requests, get direct links to suggested fixes, optimize remediation with full trace analysis and initiate automated workflows including issue tracker integration.

Simplifying the World of Open Source Usage

We believe the only way to use open source without compromising on security or quality and without slowing down your developers — is to make this complex process of risk mitigation as simple as possible.

Using open source code should be easy. That's why we created Mend. Our technology takes care of the heavy lifting that comes with open source usage. We alert you only when something demands your attention, providing you with all the information that you need to make the right choices.

How We Bring Order to Chaos

The Mend platform continuously detects all of the open source components used in your products. It then compares these components against Mend's database. This database is built by collecting up-to-date information about open source components from numerous sources, including various vulnerability feeds and hundreds of community and developer resources. The Mend platform is designed for security and compliance professionals, to give managers everything that they need in order to control and manage the open source usage within their organization. It allows them to enforce their policies automatically throughout the SDLC, get real-time alerts on critical issues, and generate up-to-date reports.

It includes a set of tools that fit into the developers' ecosystem, empowering them to make educated choices, speed up integration, and quickly find and remediate problematic open source components. Because knowledgeable developers make better software.