

Control open source risk across your SDLC.

Contextual Software Composition Analysis with Sonatype Lifecycle.

The SDLC stages of design, coding, testing, and deployment all pose unique challenges that impact developer efficiency. Sonatype Lifecycle's tools and features offer visibility into application security posture while addressing pressing challenges, enabling secure and productive development workflows.



Volume of security threats and alerts

Addressing vulnerabilities while working on multiple projects strains teams, risking project timelines and extra costs due to prioritization challenges

Establish open source security policies to **automatically detect gaps**, forecast vulnerabilities, and expedite remediation processes.



Balancing speed and security

Management prioritizes Deployment Frequency and Time to Release, while AppSec teams aim to maintain application security and support business goals

Integrate security and compliance testing into the SDLC, enabling developers to select the safest open source components and offering security teams actionable intelligence and guidance.



Increasing Security and Regulatory Requirements

Teams face growing regulatory compliance, evolving security frameworks, and shifting security best-practices.

Meet open source licensing requirements, **report software contents accurately** with standardized SBOMs, and utilize automatic license compliance.



Lack of visibility into attack surfaces and vulnerabilities

Security teams need continuous detection to auto-block exploits, maximizing speed and uptime while minimizing risk

Accurately identify open source libraries, vulnerabilities, and their dependencies, reducing false positives/negatives and narrowing the exploitability window.



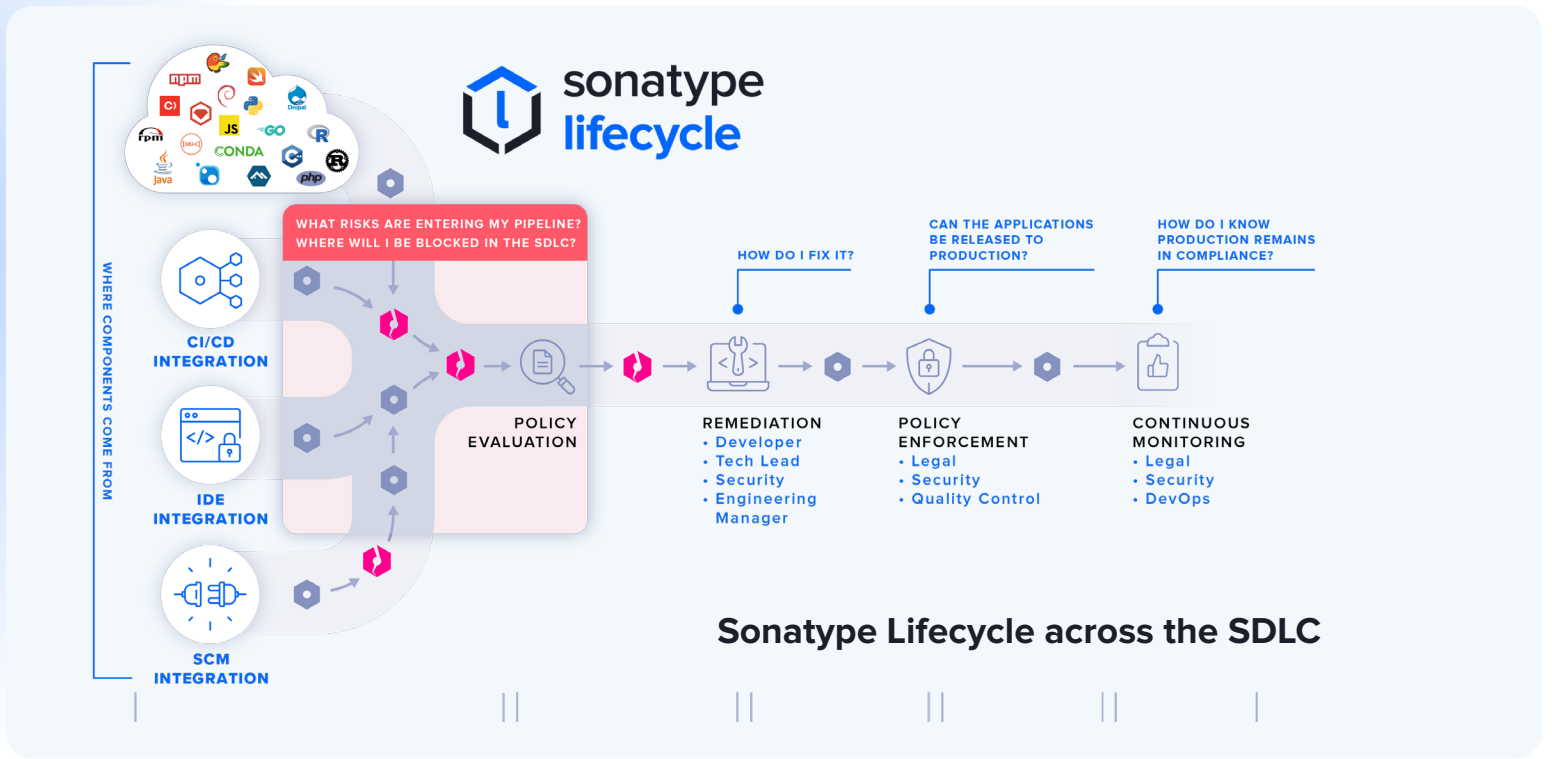
Lack of DevOps workflow integration

Teams want to control open source risk using preferred tools, avoiding the need to learn new systems.

Integrate seamlessly with current tools to get contextual component suggestions, eliminate vulnerabilities at code creation, and address security needs without hindering productivity.

“We evaluated Black Duck, Veracode and Sonatype Lifecycle. My colleagues and I chose Lifecycle because it is the best user interface for what we are trying to do: remove all critical findings before they reach production.”

—Lars Brössler, Senior Software Developer, Endress+Hauser



INTELLIGENT RISK MANAGEMENT

Secure your software supply chain

✔ Control open source risk with your favorite tools

We integrate with the most popular pipeline and development tools, languages and packages you're already using, so you do what you do best - innovate and code new products - and not waste your time adapting to new tools or processes.

✔ Enforce policies automatically

Automatically enforce policies early, everywhere and contextually across the SDLC. That way, you are able to manage and mitigate a range of risks that can be exploited to do harm to your organization, such as security risks, license risks, and quality risks.

✔ Easily evaluate application security posture

Get timely visibility into new security threats with Sonatype's world class security data. Advanced AI/ML capabilities provide actionable, data-driven insight to ensure sufficient protection across all the stages of the SDLC.

pom.xml

```

16 16 - <jackson.version>2.9.9.3</jackson.version>
17 17 + <jackson.version>2.9.9.3</jackson.version>

```

19 + <jackson.version>2.9.9.3</jackson.version>

eduard 4 minutes ago Author

Sonatype IQ found policy violations introduced by:

- 10 com.fasterxml.jackson.core:jackson-databind:2.9.9.3

Bumping to version 2.10.0 will resolve these violations (as of Oct 14, 2022)

| Threat | Policy | Violation Details |
|--------|-------------------|---|
| 10 | Security-Critical | Critical risk CVSS score: • Found security vulnerabilities: CVE-2021-14893, CVE-2020-24540, CVE-2019-13592, CVE-2019-17267 |
| 9 | Security-High | High risk CVSS score: • Found security vulnerabilities: sonatype-2021-0371 |

“A bill of materials, whether it’s of open source components or in house components, is a key part of the overall strategy on ensuring large software projects have trusted, secure components.”

—Andrew Wild, Chief Security Officer, Qualys

“SHIFT-LEFT” WITH CONTEXT-AWARE SCA

Manage open source vulnerabilities



✔ Remediate vulnerabilities fast

View any concerns from a central dashboard. Prioritize remediation and development work based on detailed intelligence and vulnerability-specific remediation guidance.

✔ Generate a Software Bill of Materials (SBOM)

Identify precisely what's in your apps and containers with detailed SBOM reporting in minutes. Know your open source components, along with their dependencies.

✔ Monitor continuously for new defects

Establish an automated early warning system to identify newly discovered defects and receive detailed intelligence on them, including precise root cause to reduce risk exposure.

AUTOMATE OPEN SOURCE GOVERNANCE

Quality code. Where and when you need it.

✔ Select the best open source components

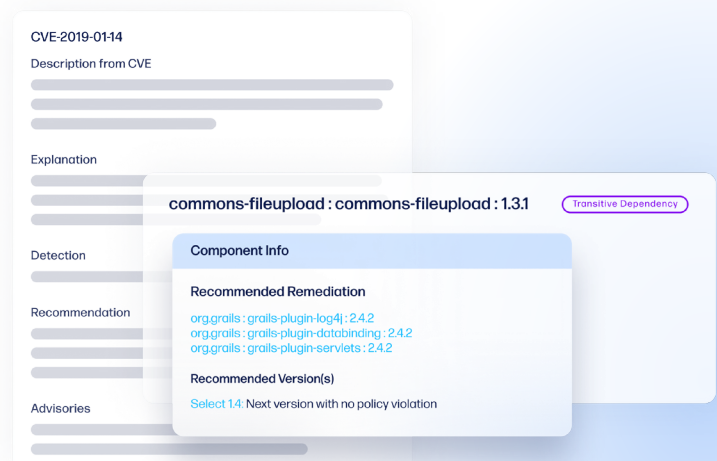
Receive detailed intelligence for healthier component choice early in development, directly in your IDE and source control.

✔ Avoid false positives and negatives

Reduce developer noise with insights you can count on. Access data compiled from automation and careful human curation for quality your team can confidently act on right away.

✔ Code with confidence

Streamline dependency management with the most precise inventory of software dependencies used in your applications and deploy without unnecessary delays.



Sonatype is the software supply chain management company. We enable organizations to innovate faster in a highly competitive market. Our industry-leading platform empowers engineers to develop software fearlessly and focus on building products that power businesses. Sonatype researchers have analyzed more than 120 million open source components – 40x more than its competitors – and the Sonatype platform has automatically blocked over 115,000 malicious components from attacking software development pipelines. Enabling high-quality, secure software helps organizations meet their business needs and those of their customers and partners. More than 2,000 organizations, including 70% of the Fortune 100 and 15 million software developers, rely on our tools and guidance to be ambitious, move fast and do it securely. To learn more about Sonatype, please visit www.sonatype.com.