Nexus Lifecycle
Eliminate open source risk across the entire SDLC.

It's no secret. Developers use open source — in fact, 85% of a modern application is comprised of open source components and unfortunately one in ten open source component downloads contain a known security vulnerability. Given this inherent risk, how do modern software teams select the best components, govern open source usage, and still deliver at DevOps speed? Automated open source governance.

Nexus Lifecycle empowers developers and security professionals to make safer open source choices across the SDLC, ensuring organizations continue to innovate with less risk.

“"My advice is: do it yesterday. You’ll save yourself a lot of money. Even during one, two, or three weeks, it’s going to cost you a lot of money to fix the security vulnerabilities that you are ingesting in your development lifecycle. You could be avoiding that by using a product like Lifecycle.”

— C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

www.sonatype.com
Enforce Open Source Policies Across the SDLC

Create custom security, license, and architectural policies based on application type or organization and contextually enforce those policies across every stage of the SDLC. Automatic policy enforcement can only happen with the precision and accuracy of Nexus Intelligence, eliminating false positives / negatives found in other solutions.

Remediate Known Issues Within the IDE

With integration to source repos and IDE’s, developers can select the best components based on real-time intelligence and move to an approved version with one click. Nexus Lifecycle integrates with GitHub, GitLab, BitBucket, Eclipse, IntelliJ, and Visual Studio.

We Work Where You Work

Automatically enforce policies and view expert remediation guidance in the tools you use every day. Nexus Lifecycle works with Nexus Repository, Artifactory, GitHub, GitLab, IDEs, Jira, Jenkins, Azure DevOps, Micro Focus Fortify, Xebia Labs, OpenShift, Mesosphere OS, AWS, Docker, and many more.

“For us, it’s seeing not only the licensing and security vulnerabilities but also seeing the age of the open source included within our software. That allows us to take proactive steps to make sure we’re updating the software to versions that are regularly maintained and that don’t have any vulnerabilities.”

— A. COX, CIVICA, IT CENTRAL STATION REVIEW

www.sonatype.com
Automatically Generate a Software Bill of Materials

Verify policy compliance by knowing what components are used and where. In just minutes generate a precise software BoM for each app to identify every open source component along with its dependencies.

Identify and Fix Container Vulnerabilities

With integration to Red Hat Clair, you can view open source risk at all layers of the container (runtime, operating system, and application levels) within existing dashboards and reports. Use Nexus Lifecycle’s flexible policy engine to govern open source risk within the entire container.

Key Benefits of Nexus Lifecycle

✓ Automatic enforcement of open source policies across every stage of the SDLC, powered by the most precise and accurate component intelligence.

✓ Sleep better at night knowing that your applications and containers are continuously monitored for new risk.

✓ No need to learn a new tool, Nexus Lifecycle integrates with your existing DevSecOps pipeline.

Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype’s Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit Sonatype.com, or connect with us on Facebook, Twitter, or LinkedIn.