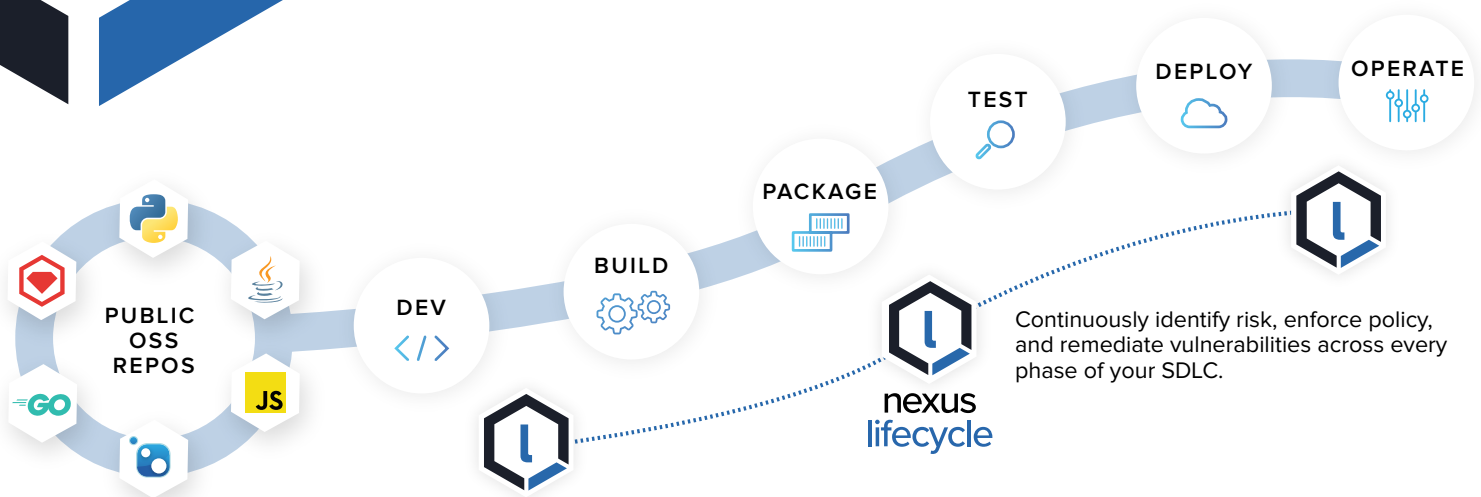


Nexus Lifecycle

Eliminate open source risk across the entire SDLC.

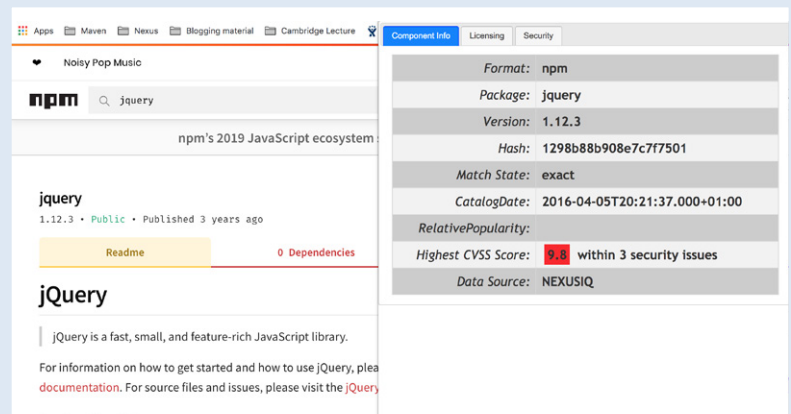
It's no secret. Developers use open source — in fact, 85% of a modern application is comprised of open source components and unfortunately *one in ten* open source component downloads contain a known security vulnerability. Given this inherent risk, how do modern software teams select the best components,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



Empower Developers to Select Safer Components

With a Chrome browser extension, developers know if an open source component is vulnerable when selecting from public repositories.



“My advice is:

do it yesterday. You'll save

yourself a lot of money. Even

during one, two, or three weeks, it's

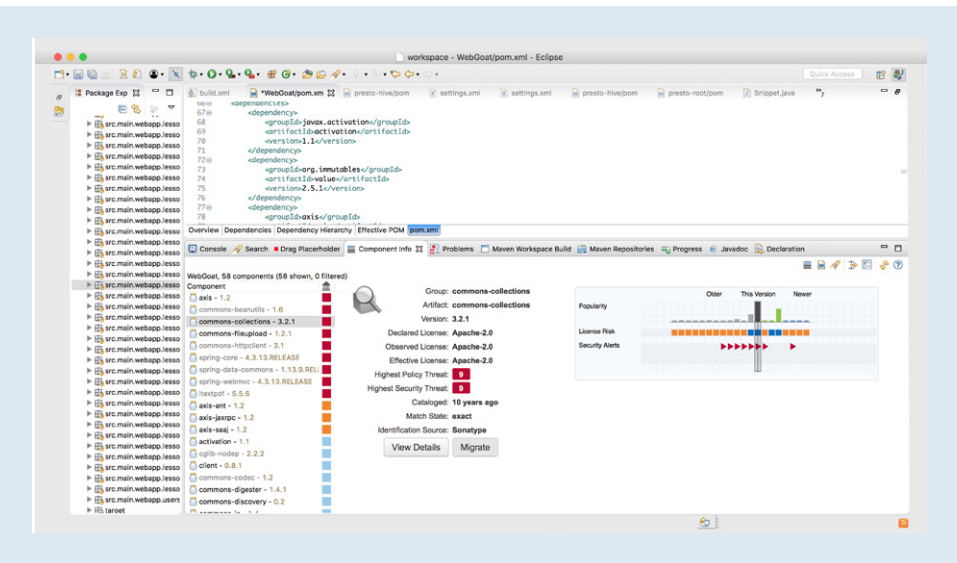
going to cost you a lot of money to fix the

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

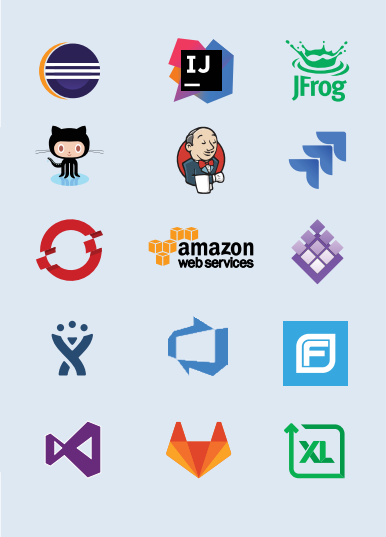
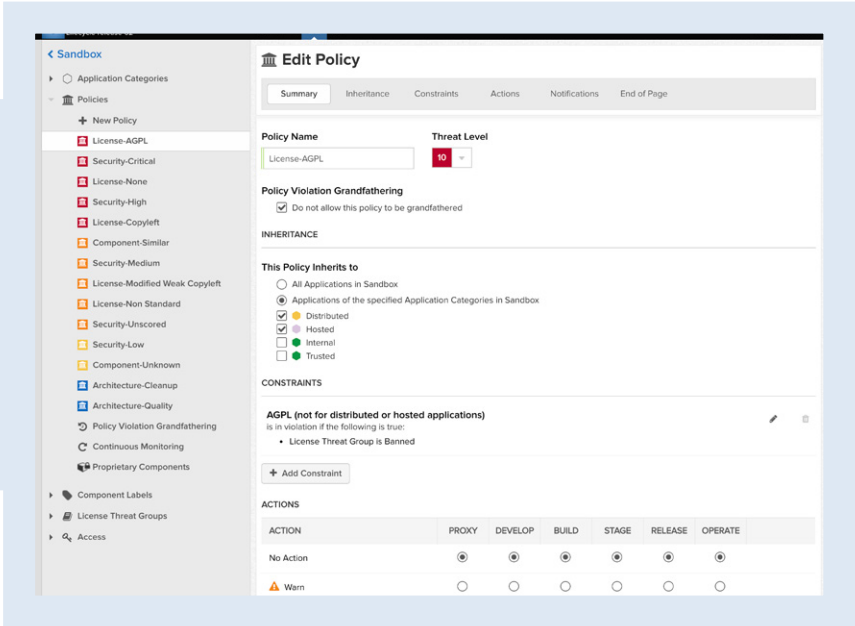


Remediate Known Issues Within the IDE

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.

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.



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.

“We’re no longer building blindly with vulnerable components. We have awareness, we’re pushing that awareness to developers, and we feel we have a better idea of what the threat landscape looks like. Things that we weren’t even aware of that were bugs or vulnerabilities, we are now aware of them and we can remediate really quickly.”

— D. DUFFY (Financial Services), IT Central Station Review

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient: commons-httpclient: 3.1	8	200	81	113	6	0
org.apache.struts: struts2-assembly: zip: all: 2.3.14	4	169	99	48	6	0
org.apache.struts: struts2-blank: war: 2.3.14	4	130	76	48	6	0
org.apache.struts: struts2-showcase: war: 2.3.14	4	130	76	48	6	0
org.apache.struts: struts2-portlet: war: 2.3.14	4	109	70	48	6	0
org.apache.struts: struts2-rest-showcase: war: 2.3.14	4	130	76	48	6	0
axis: axis: 1.2	6	126	54	72	0	0
org.apache.struts: struts2-mailreader: war: 2.3.14	4	125	76	43	6	0
commons-collections: commons-collections: 3.1	10	122	94	24	0	0
org.apache.struts: struts2-core: 2.3.14	4	122	76	43	3	0
commons-collections: commons-collections: 3.2.1	5	99	81	18	0	0
org.apache.struts: struts2-core: 2.3.14	4	99	66	33	0	0
org.springframework: spring-context: 2.5.6.SEC03	6	94	36	58	0	0
org.apache.httpcomponents: httpclient: 4.2.5	6	94	36	58	0	0
org.springframework: spring-web: 2.5.6.SEC03	6	94	36	52	6	0
org.apache.jackrabbit: jackrabbit-webdav: 2.5.2	6	87	36	51	0	0
org.springframework: spring-web: 3.0.5.RELEASE	4	86	36	47	3	0
org.apache.struts: struts2-rest-plugin: 2.3.14	4	81	54	22	3	0
commons-fileupload: commons-fileupload: 1.2.1	6	78	54	12	12	0

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.

gnupg2 : 2.1.18-8~deb9u4

Recommended Version(s)
No recommended versions are available for the current component

Selected Version: 2.1.18-8~deb9u4
name: gnupg2
version: 2.1.18-8~deb9u4
Declared License:
Observed License:
Effective License: -
Highest Policy Threat: 3 within 2 policies
Highest CVSS Score: 3 within 2 security issues
Cataloged: -
Match State: exact
Identification Source: Clair
Category:

Version Graph
Popularity
Order: Older | This Version | Newer

Policy Threat
Click on the graph above to see details about different versions

Close | Previous | Next

3	Security-Low	glibc : 2.24-11~deb9u4
3	Security-Low	gnupg2 : 2.1.18-8~deb9u4

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](https://www.sonatype.com), or connect with us on [Facebook](https://www.facebook.com/sonatype), [Twitter](https://twitter.com/sonatype), or [LinkedIn](https://www.linkedin.com/company/sonatype).