carahsoft.

Accelerate Innovation with Automated Security

Enforce Open Source Policies with the Nexus Platform

Thank you for downloading this report. Carahsoft represents proven DevSecOps solutions, delivering agencies the innovative solutions needed for every phase of the DevOps and DevSecOps lifecycles and with security built-in every step of the way. These solutions provide support for collaborative planning, rapid code builds, iterative testing, rapid release, optimized deployment and ongoing monitoring that continuously feeds into the next wave of planning.

Carahsoft combines extensive knowledge of the technologies we provide with a thorough understanding of the government procurement process to analyze needs, provide configuration support, simplify the ordering process, and offer special government pricing. Speak to a Carahsoft representative today about achieving your DevSecOps objectives.

For more information, contact Carahsoft or our reseller partners:
carah.io/solve/devsecops |devsecops@carahsoft.com | (703) 871-8570

sonatype

A Better Way to Build.

Accelerate Innovation with Automated Security

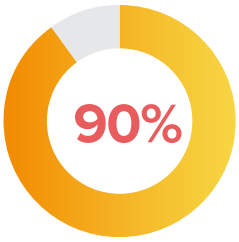
Enforce Open Source Policies with the Nexus Platform

It's no secret... developers use open source software.

Still, there are questions around how it should be managed—and for good reason. Here's why:

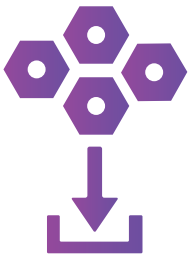
- Open source components are not created equal. Some are vulnerable from the start, while others go bad over time.
- Usage has become more complex. With tens of billions of downloads, it's increasingly difficult to manage libraries and direct dependencies.
- Transitive dependencies: if you are using dependency management tools like Maven (Java), Bower (JavaScript), Bundler (Ruby), etc., then you are automatically pulling in third party dependencies—a liability that you can't afford.

How do you manage open source risk at scale? Through an automated open source governance policy.



of the components in most modern applications are open source.

1.4 trillion
download requests of Java, npm, PyPi, and RubyGems were recorded in 2019.



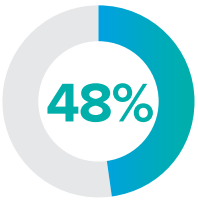
379,000+
Java components are downloaded annually by the average company.

DevSecOps: Why is open source policy critical?

As the number of breaches continue to rise, DevOps organizations are making investments to better protect themselves by doing more than just building stronger castle walls. These organizations are taking steps to integrate and automate security across the development lifecycle to build quality into their software.

According to the 2019 DevSecOps Community Survey:

1 in 10
Java component downloads are vulnerable.



of organizations have no open source governance policy or ignore it.

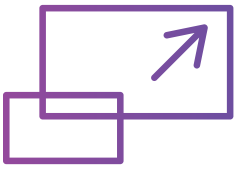
There has been a
71% increase
in open source related breaches over the past five years.

1 in 5
organizations experienced at least one open source breach in the last 12 months.

Accelerate DevSecOps early, everywhere, at scale with the Nexus Platform.

Early
Nexus delivers intelligence within existing developer workflows and vetted components can be automatically quarantined based on policy.

Everywhere
Nexus accelerates DevOps by integrating with the most widely used tools at every stage of the development pipeline.



At Scale
Automate security in a DevOps pipeline with precise component intelligence.

"Integrating security into DevOps **to deliver 'DevSecOps' requires changing mindsets, processes and technology.** Security and risk management leaders must adhere to the collaborative, agile nature of DevOps to be seamless and transparent in the development process, making the Sec in DevSecOps silent."

Gartner

"The reason **we picked Lifecycle over the other products** is, while the other products were flagging stuff too, they were flagging things that were incorrect."

— E. KWAN (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

But first, our data.

Our data quality is the lifeblood that powers our entire platform.

97% of Nexus Intelligence is exclusive to Sonatype.

The bulk of our data is collected from verified online advisories and our in-house team of 65 security researchers. In fact, Sonatype's team has uniquely discovered 1.4 million vulnerable component versions, providing more data than just what's in the National Vulnerability Database.

No false positives and no false negatives.

Through both automation and careful human curation, Nexus Intelligence is designed to give you results you can count on, saving you an average of $14,000 in time per developer per year.

When it comes to security, speed matters.

We implement a 12-hour fast track for critical and time-sensitive vulnerabilities. You'll experience a **20% reduction in probability** of a breach when using the Nexus platform.

Better together.

The Nexus Platform protects your entire software development lifecycle.

nexus firewall

Vet parts early and automatically stop defective components from entering your DevOps pipeline.

nexus lifecycle

Empower teams with precise component intelligence that enforces policy and continuously eliminates risk.

nexus repository

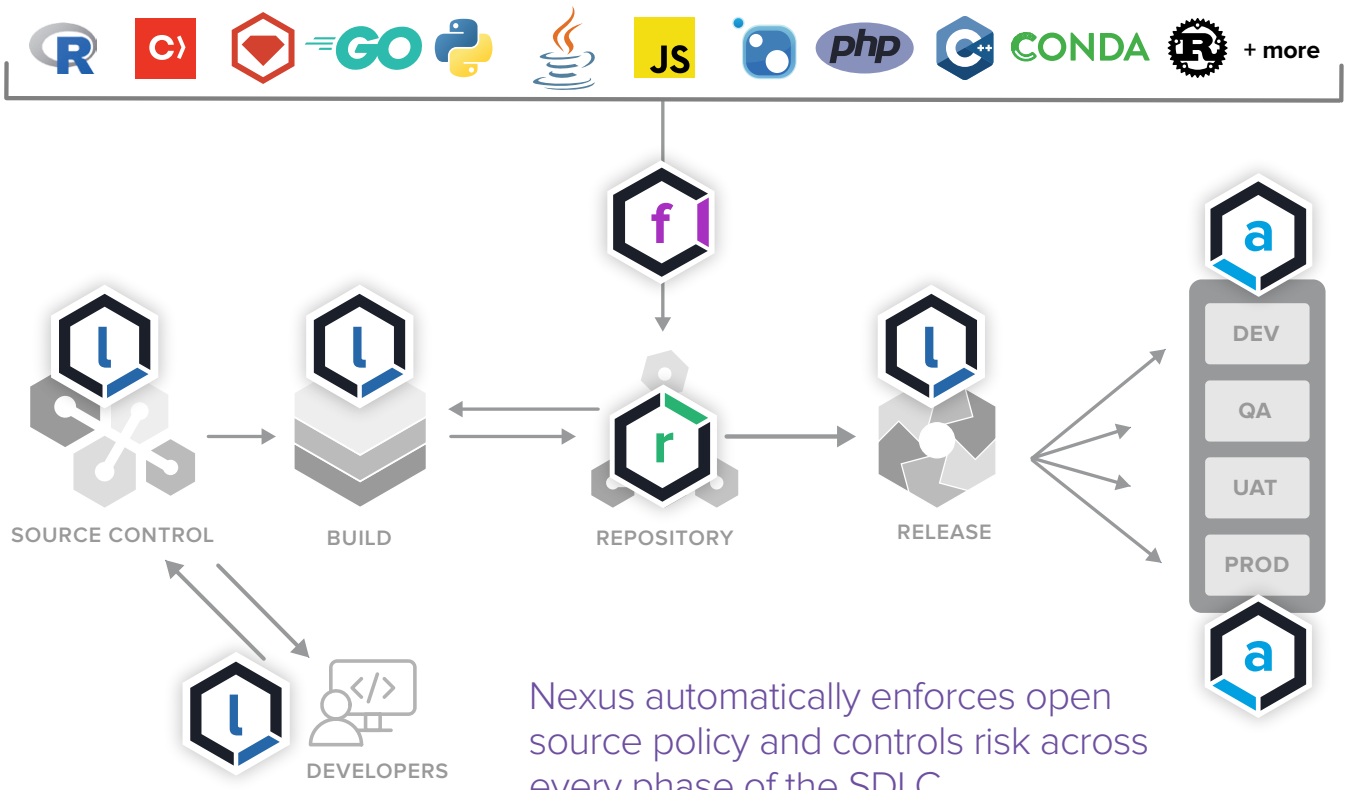
Manage libraries and store parts in a universal repository and share them across the DevOps pipeline.

nexus auditor

Examine OSS components within production apps.

"[Nexus] has helped developer productivity. **It's like working in the dark and all of a sudden you've got visibility.** You can see exactly what you're using and you have suggestions so that, if you can't use something, you've got alternatives. That is huge."

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

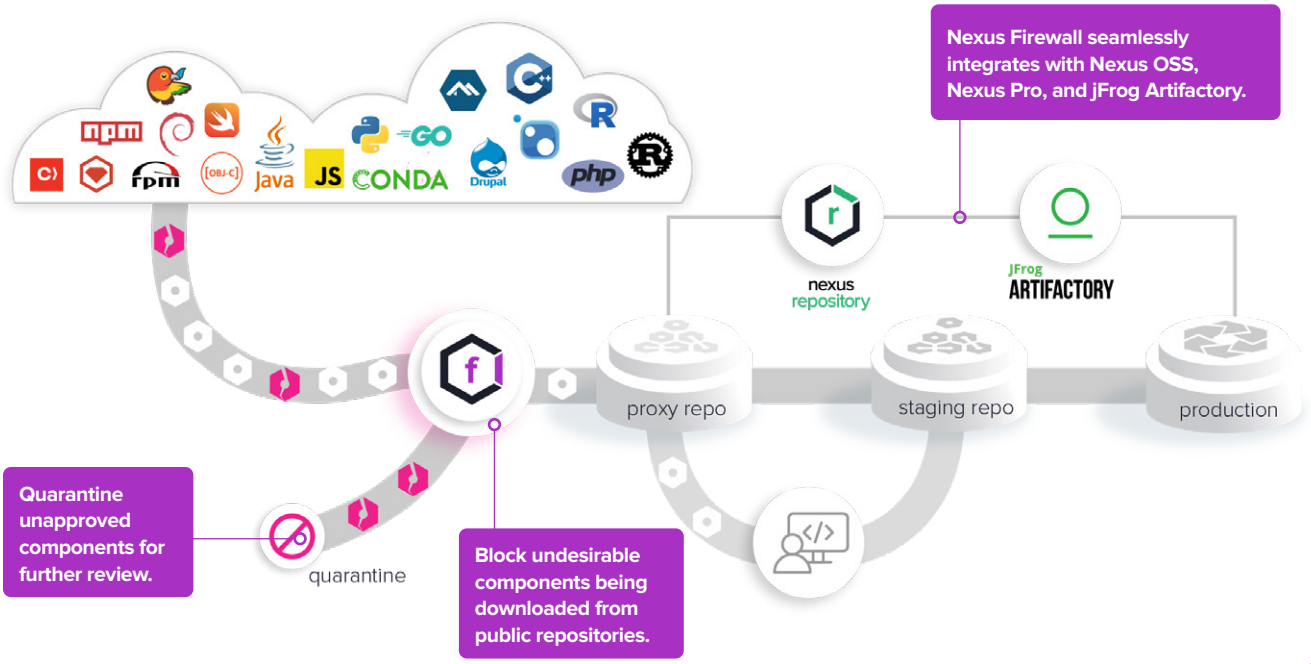


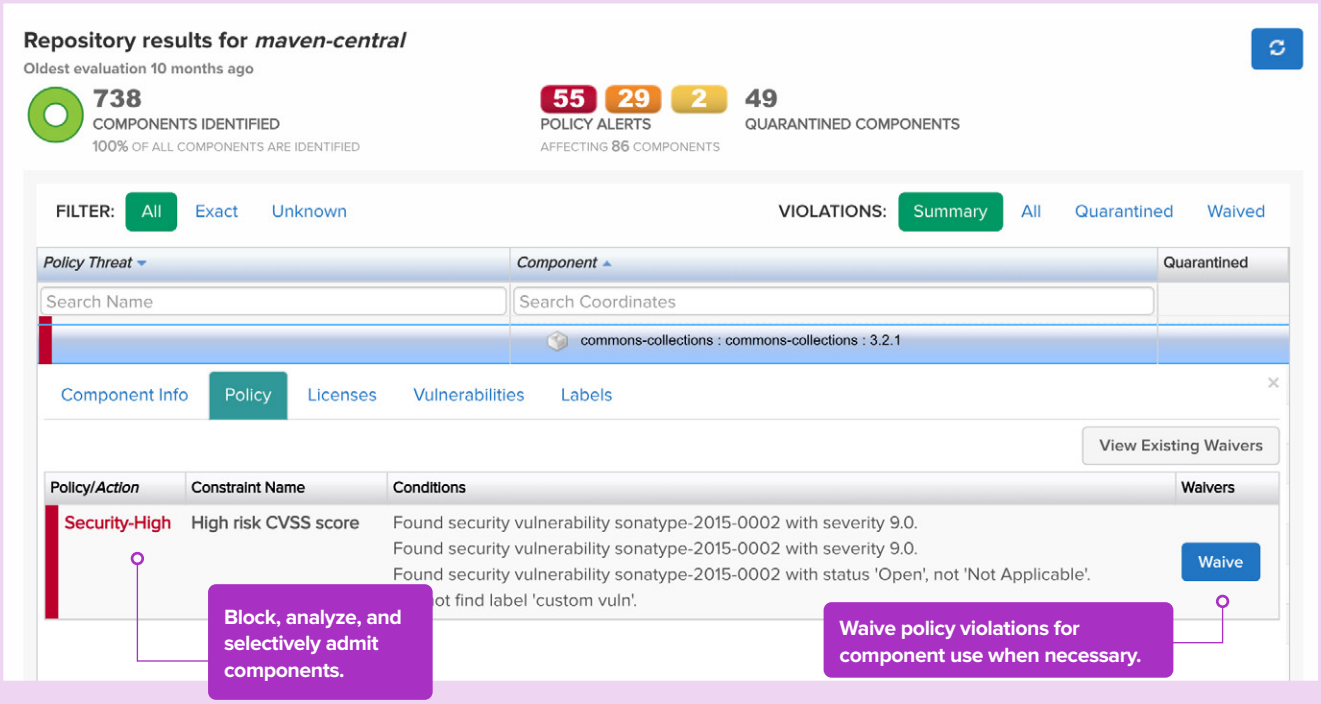
Nexus automatically enforces open source policy and controls risk across every phase of the SDLC.

nexus firewall

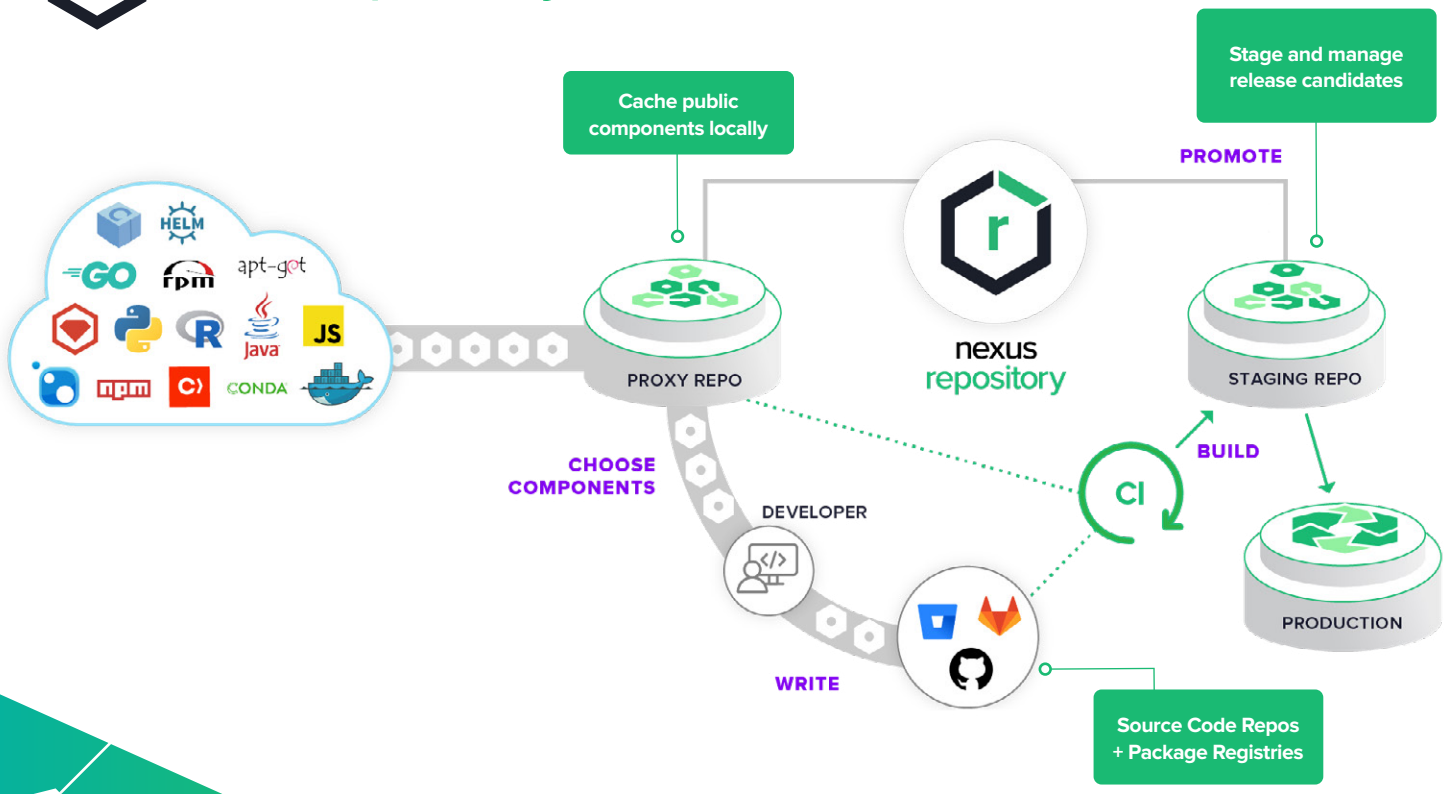
THE EARLIER, THE BETTER

Block bad components at the door.





nexus repository



A CENTRAL SOURCE OF CONTROL

Universally manage all of your components, binaries, and build artifacts.

Store and distribute all popular formats with Proxy, Hosted, and Group repositories for enterprise-ready flexibility.

Improve speed-to-market, reduce build times, and streamline developer productivity across the entire SDLC.

Scale and deploy enterprise reliability in multi-site, highly available configurations on premises or in the cloud.

"Nexus Repository Manager provides a central platform for storing build artifacts, saving us significant maintenance and hardware costs. I haven't had any negative impact, so **I am very confident using Nexus in terms of its reliability.**"

— HAGEN RAHN, SR. SOFTWARE ENGINEER, SYSTEMA, IT CENTRAL STATION REVIEW

PREVENTION IS BETTER THAN A CURE

Maintain a trusted repository with Repository Health Check.

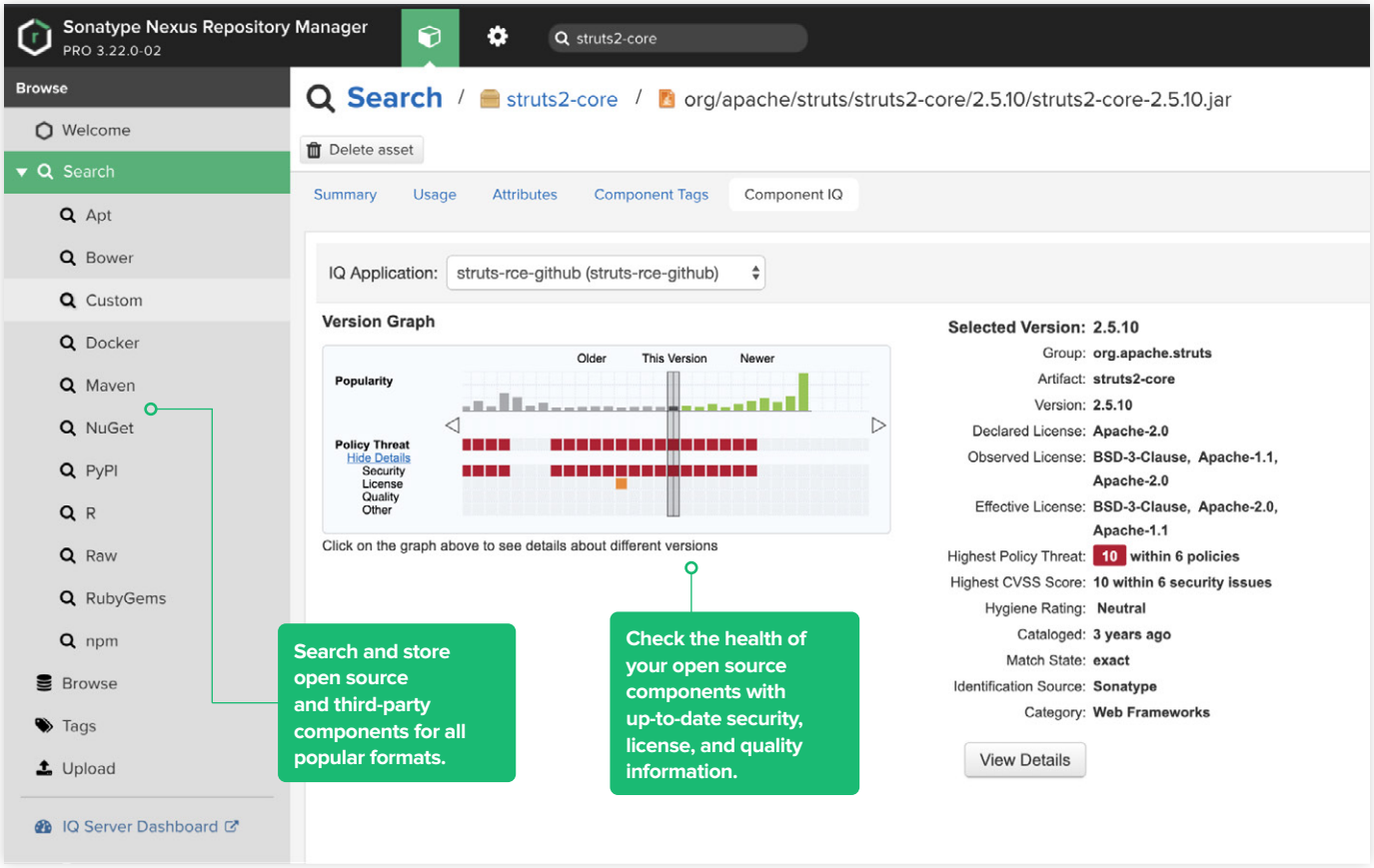
Repository Health Check (RHC) provides up-to-date component intelligence, so your teams make informed decisions early on.

Learn how many OSS components are in your repositories and the severity of any existing vulnerabilities.

Understand your open source risk exposure at a glance with known security issues.

"It ensures our developers are utilizing safe, open-source components. Through the use of Nexus software, we know when they were downloaded and where they're being used. **It has helped us increase the security of our applications."**

— A. EVANS (GOVERNMENT), IT CENTRAL STATION REVIEW



nexus lifecycle

Precise intelligence for healthier component choice early in development.

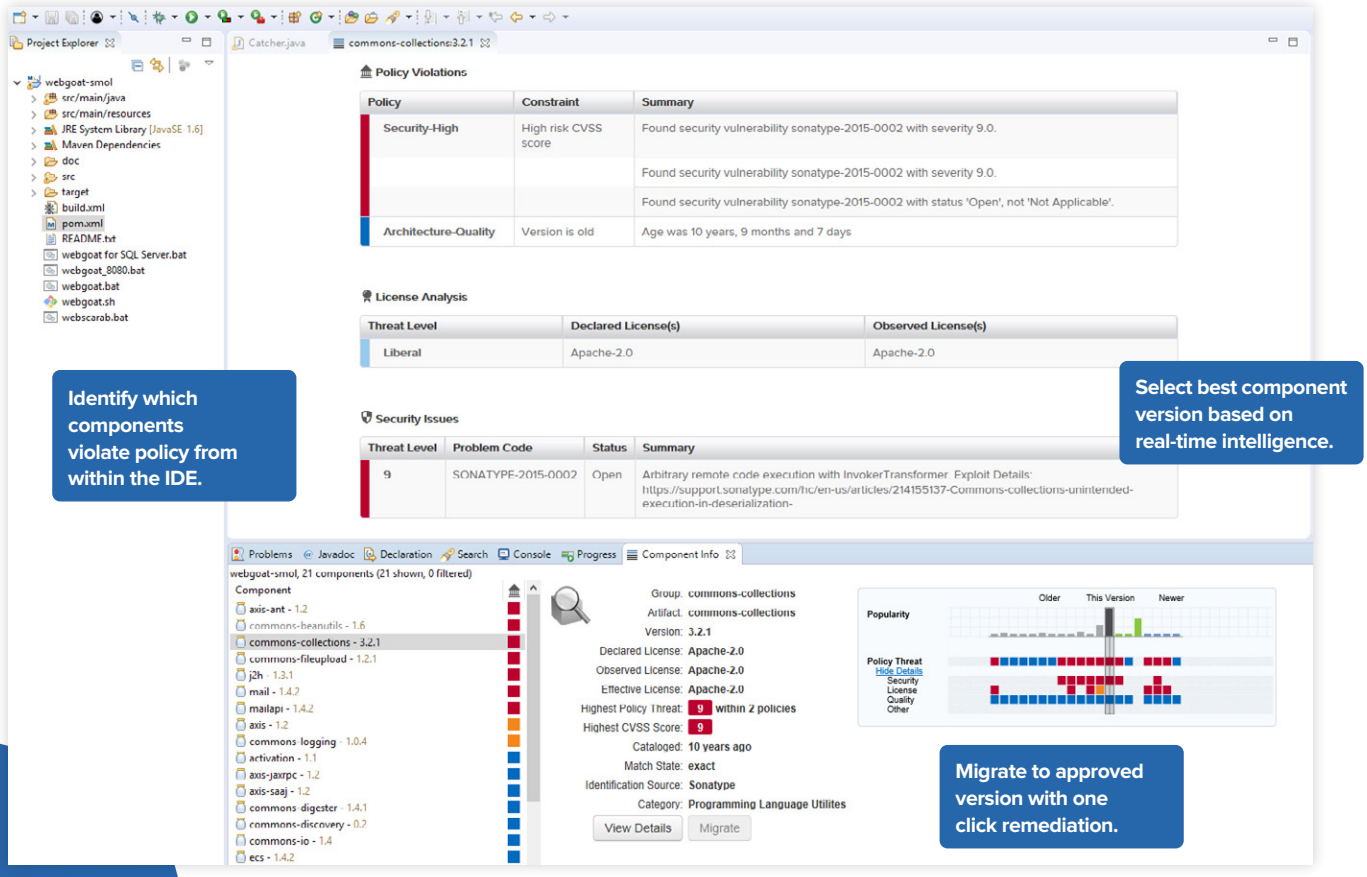
Choosing a safe component is as easy as using spell check.

Deliver component intelligence to developers in the tools they use every day like IDEs and source control.

Early detection and remediation prevents unplanned work, security breaches and maintainability issues.

"I would give this product a nine out of ten. I'll have a full report of artifacts—including those that are not secure—that would have been ingested into our organization. **That information is priceless."**

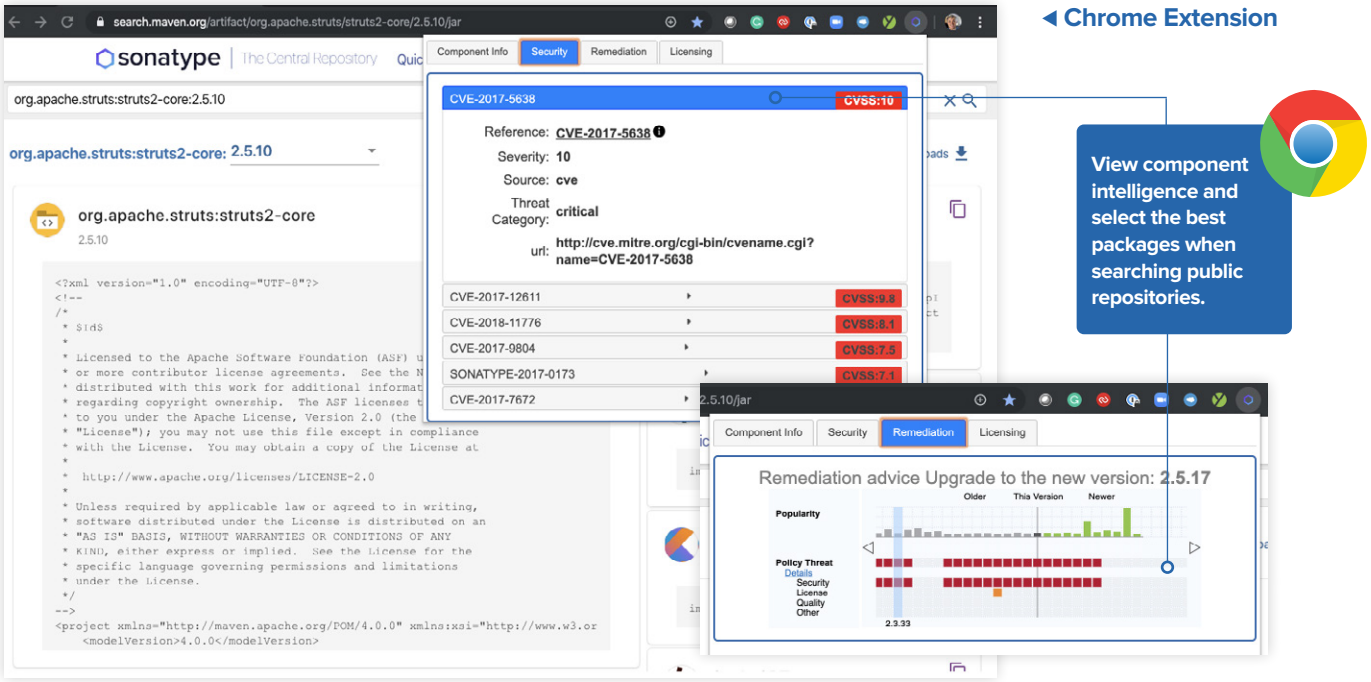
—C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW



nexus lifecycle

Instantly access Nexus Intelligence data while searching for new packages.

- **Component details:** format, package, version
- **Security info:** Severity, source, threat category, reference details
- **Licensing data:** Declared and observed
- **Remediation advice:** Version history and recommended version

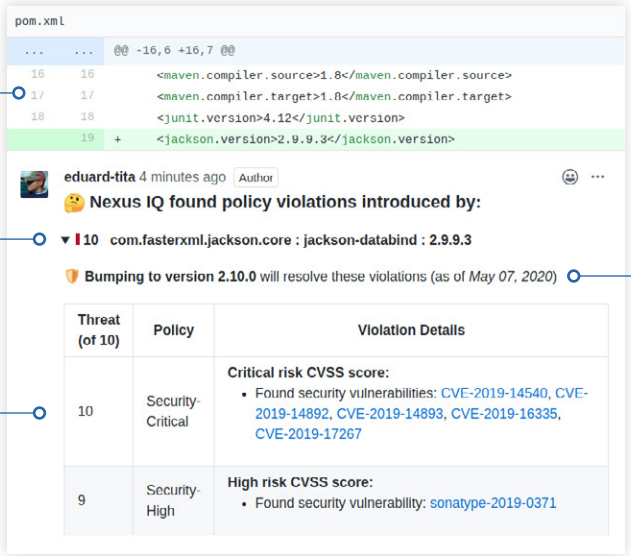


◀ Chrome Extension

View component intelligence and select the best packages when searching public repositories.

Source Control Management ▶

Highlights the specific lines of code that introduced a violation.



Shows the severity of the issue, along with the name, summary and description of the violation.

If a version is available that will fix the problem, the suggested remediation or upgrade path is also included.

nexus lifecycle

Analyze and enforce policies *automatically*.

Ensure that policies are enforced as components are consumed across a variety of development tools.

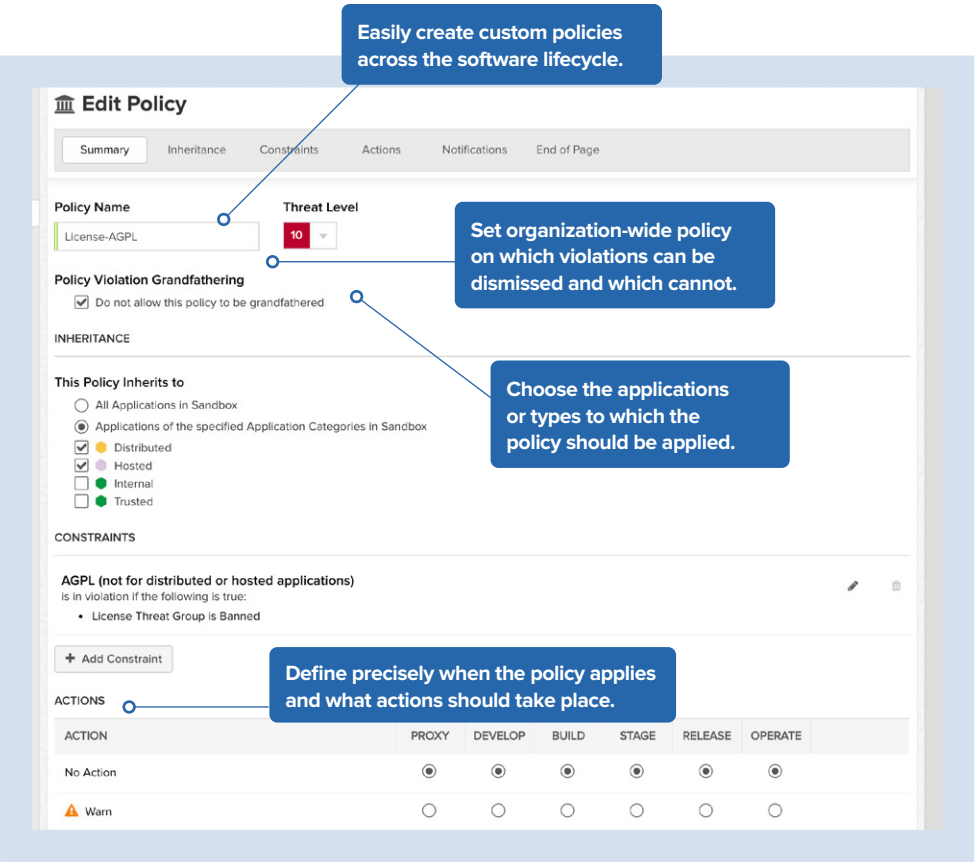
Replace inefficient work-flows and the burden of manual reviews.

Customize policies to meet specific compliance goals or mandates OR use our default policies to gain an immediate view of security, license, and quality risk.

Do it all with automation that supports agile and continuous goals!

"[Nexus Lifecycle] blocks undesirable open source components from entering our development lifecycle, based on the policies that we set. It will break the build straight away. There's no way you can ship code that introduces new vulnerabilities. We just don't allow it at all."

— E. KWAN (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW



nexus lifecycle

Verify policy compliance by knowing what components are used and where.

In just minutes, create an accurate software bill of materials for each application.

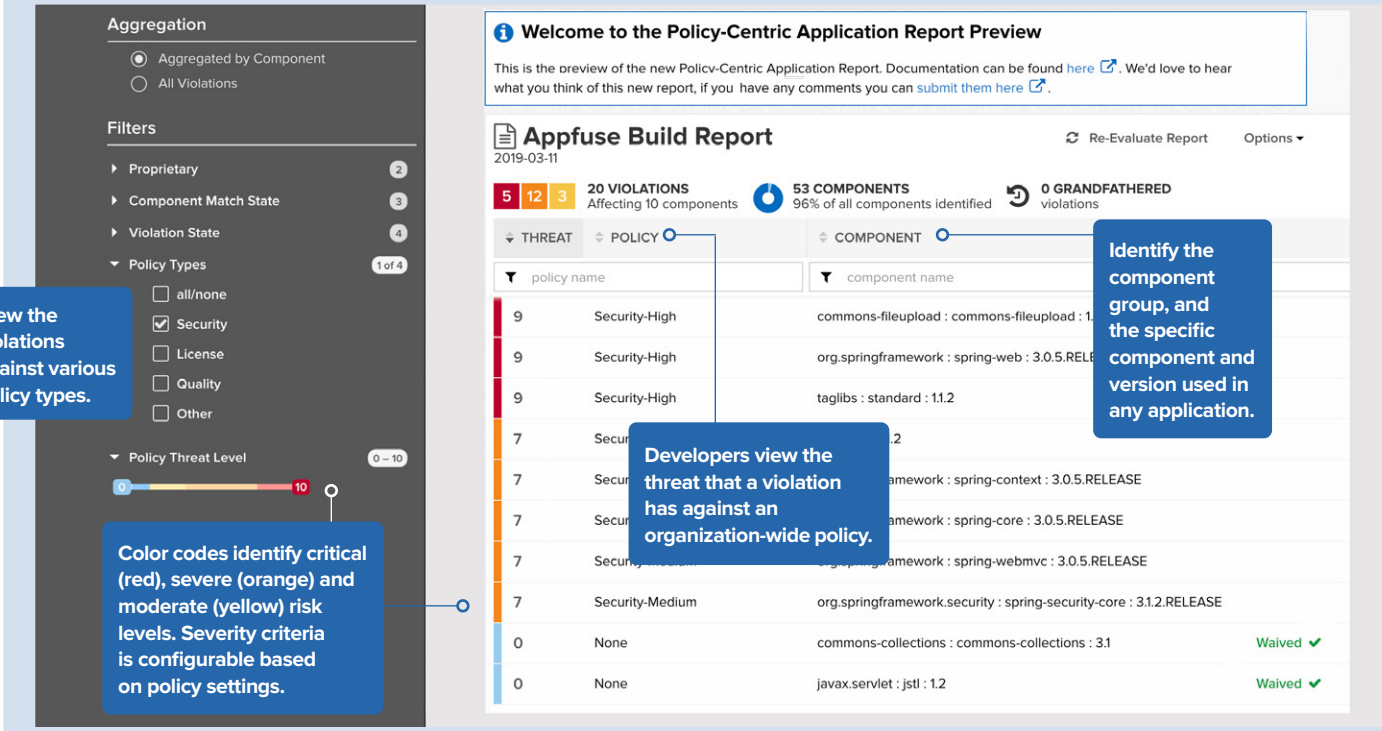
Identify specific components and their dependencies.

Gain access to name, license, age, popularity, known security vulnera-bilities, and other metadata.

Know the exact location of any component — no more searching to see if you are impacted by a new vulnerability.

"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 were vulnerabilities, we can now remediate really quickly."

— D. DUFFY (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW



"My advice is 'do it yesterday.' You 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

nexus lifecycle

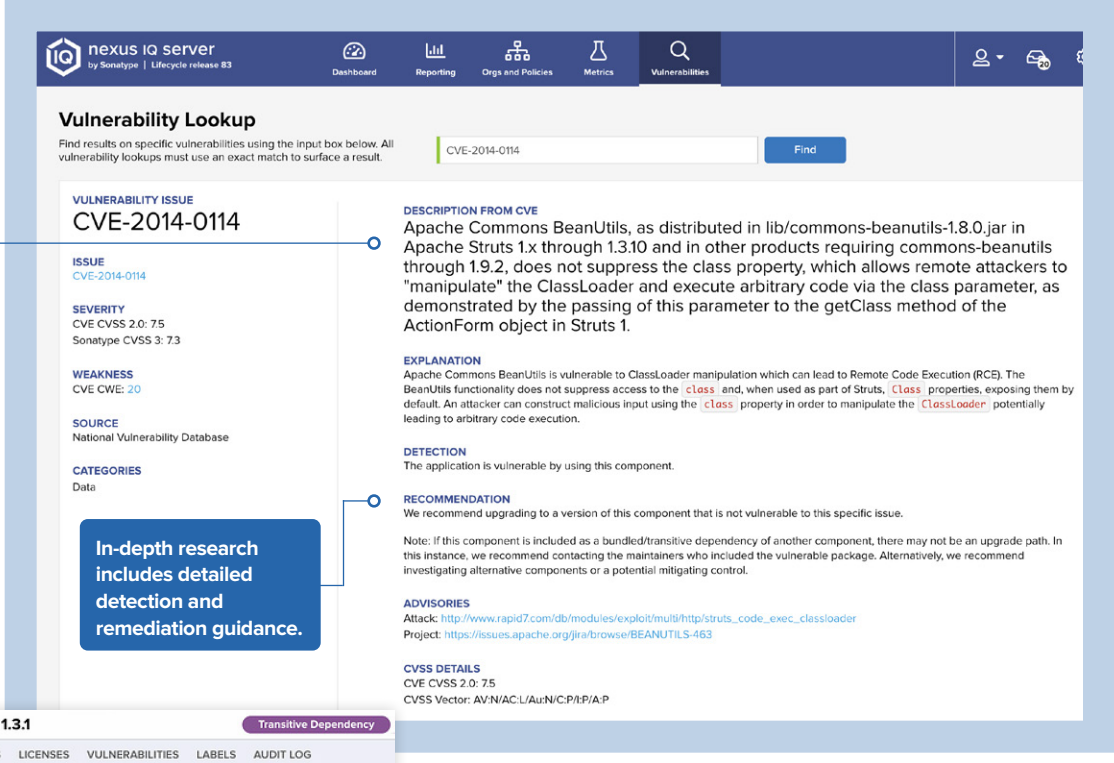
Get visibility and transparency for quick remediation.

One dashboard easily filtered to support development, operations, security, and compliance.

Prioritize remediation and development work based on detailed intelligence.

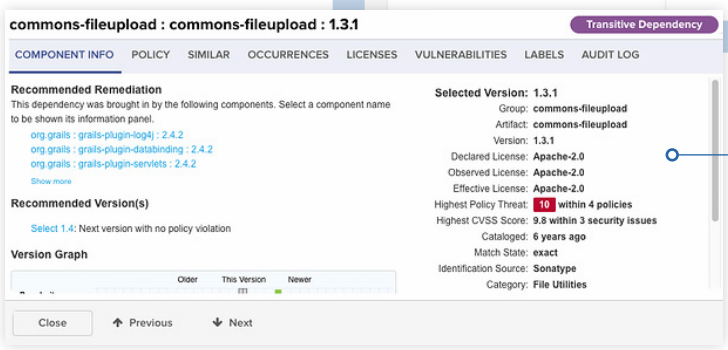
Track progress and trends for defects opened, fixed, waived, and discovered.

Reduce your technical debt and ease the maintenance burden.



Easy to understand description written for developers by developers.

In-depth research includes detailed detection and remediation guidance.



Find the best/fastest remediation path by linking to the component that brought in any transitive dependencies.

"There is a feature called Continuous Monitoring. Because of this feature, as time goes on we'll be able to know whether a platform is still secure or not. **It's integrated, it's proactive, it's exactly what you want for a security product."**

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

nexus lifecycle

Continuously monitor for new defects.

An automated early warning system to identify newly discovered defects.

Detailed intelligence on vulnerabilities including precise root cause and component dependencies.

Ongoing monitoring and alerts of new vulnerabilities based on component, risk level, or applications affected.

Improve incident response times with precise identification of components and apps to be remediated.

nexus lifecycle

Identify and fix container vulnerabilities.

View open source risk at all layers (runtime, operating system, and application levels).

Precise and accurate identification and detailed remediation guidance for application-level vulnerabilities.

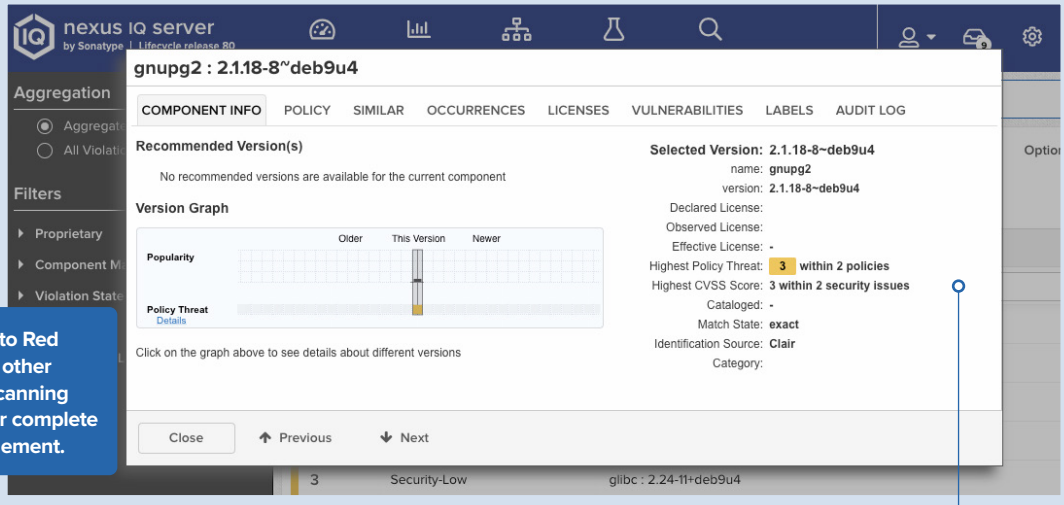
Single view into all open source risk with native Lifecycle dashboards and reports.

"Nexus has improved the time it takes us to release secure apps to market by saving us weeks of rework."

— SR. LEAD SOLUTION SERVICES (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

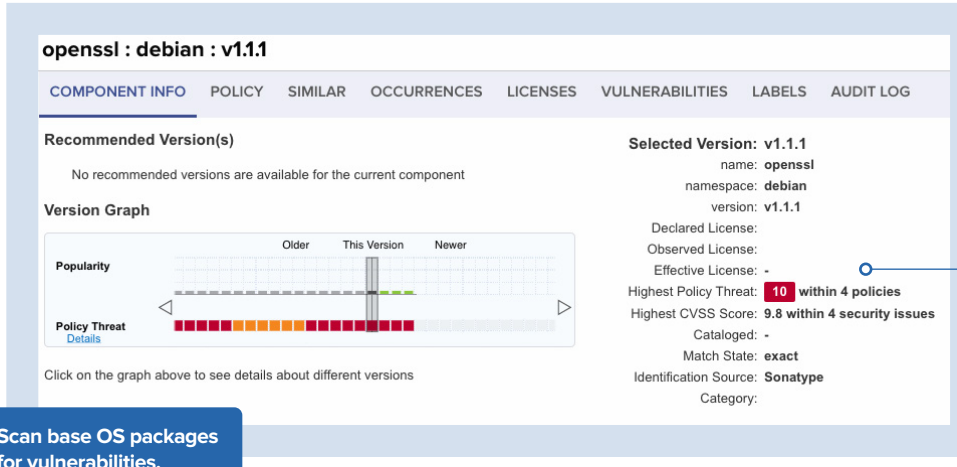
Red Hat Clair ▶

clair



Integration to Red Hat Clair or other container scanning solutions for complete vuln management.

One flexible policy engine to govern OSS risk in the entire container.

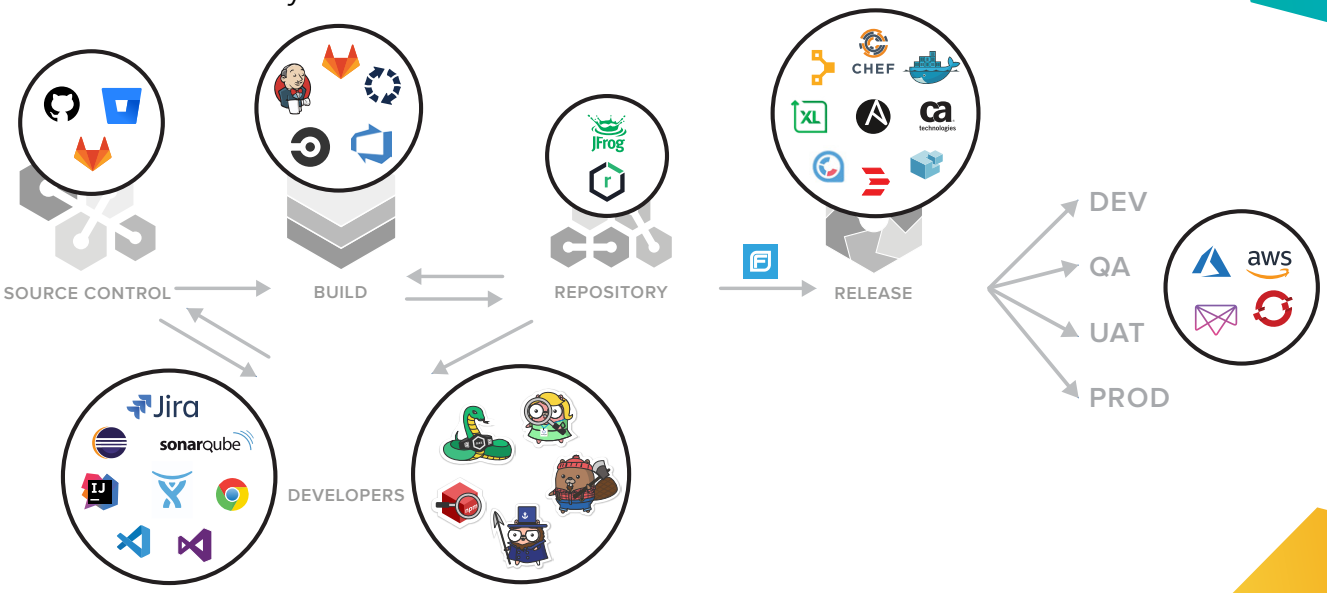


Scan base OS packages for vulnerabilities.

◀ Sonatype Ahab

Integrations? You better believe it.

We work where you work.



Better or the best? You decide.

Test drive the power of Nexus Intelligence in five minutes.

Run a free Nexus Vulnerability Scan to learn about vulnerabilities in an app (yours or one of ours). **Try it free at www.sonatype.com/appscan.**

sonatype.com/get-nexus

GET STARTED TODAY!

sonatype

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**.

Headquarters
8161 Maple Lawn Blvd.
Suite 250
Fulton, MD 20759
United States
1.877.866.2836

Virginia Office
8281 Greensboro Dr.
Suite 630
McLean, VA 22102

European Office
168 Shoreditch
High St., 5th Floor
London E1 6JE
United Kingdom

APAC Office
5 Martin Place
Level 14
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com