Accelerate Innovation with Automated Security

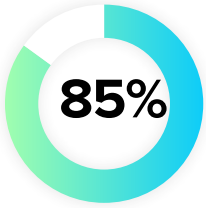
Enforce Open Source Policies with the Nexus Platform

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:

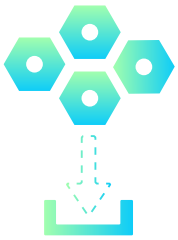
- Open source components are not created equal. Some are vulnerable from the start, while others go bad over time.
- Usage has become more complex. With tens of billions of downloads, it's increasingly difficult to manage libraries and direct dependencies.
- Transitive dependencies: if you are using 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 most modern applications are comprised of open source components.

300,000+
open source components are downloaded annually by the average company.



500 billion
download requests of Java, npm, PyPi, and RubyGems were recorded in 2018.

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 DecSecOps Community Survey:

1 in 10
open source component downloads contain a known security vulnerability.

71%
increase in verified or suspected breaches between 2014 and 2019.

1 in 4
organizations experienced at least one open source breach in the last 12 months.

38%
of organizations have no open source governance policy or ignore it.

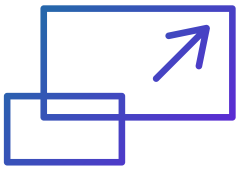
Accelerate DevSecOps early, everywhere, at scale with the Nexus platform.

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.

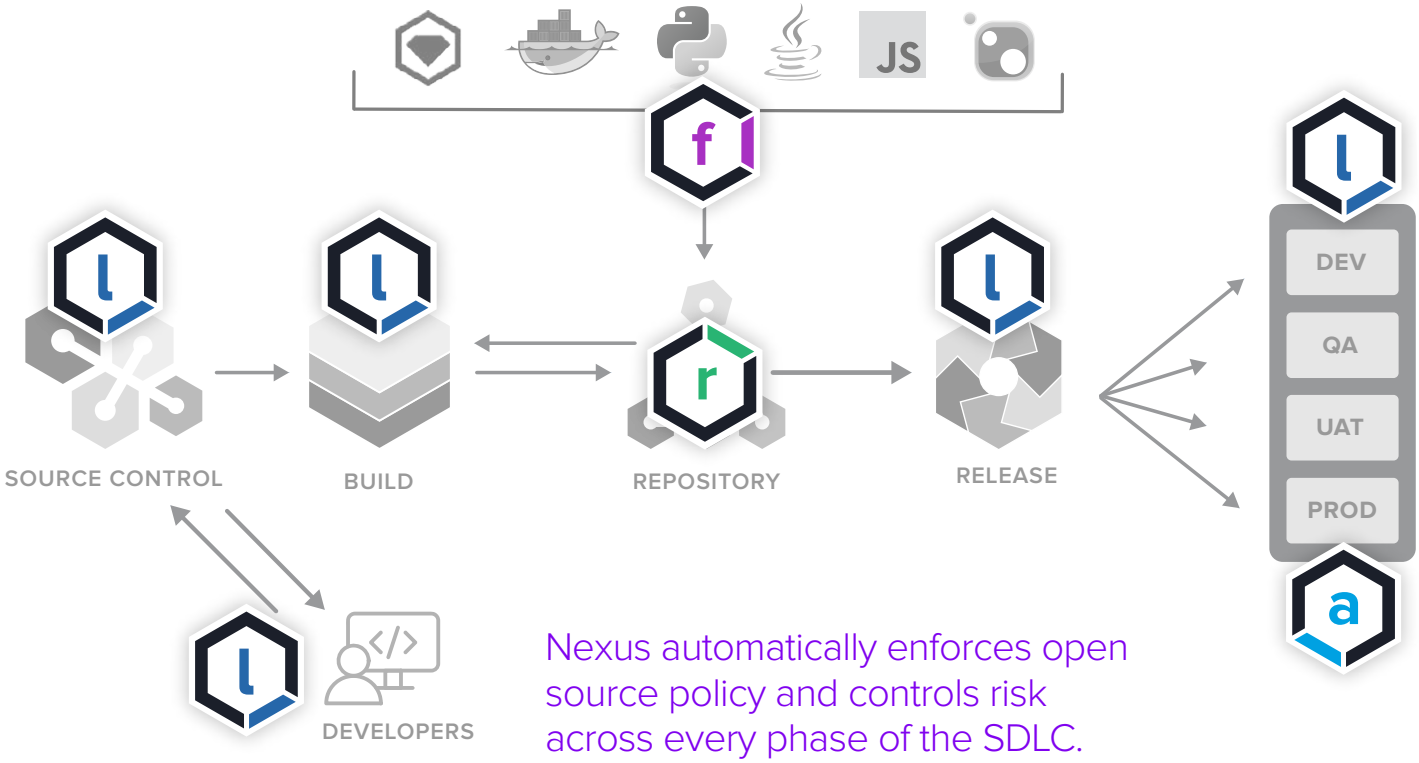
nexus repository

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

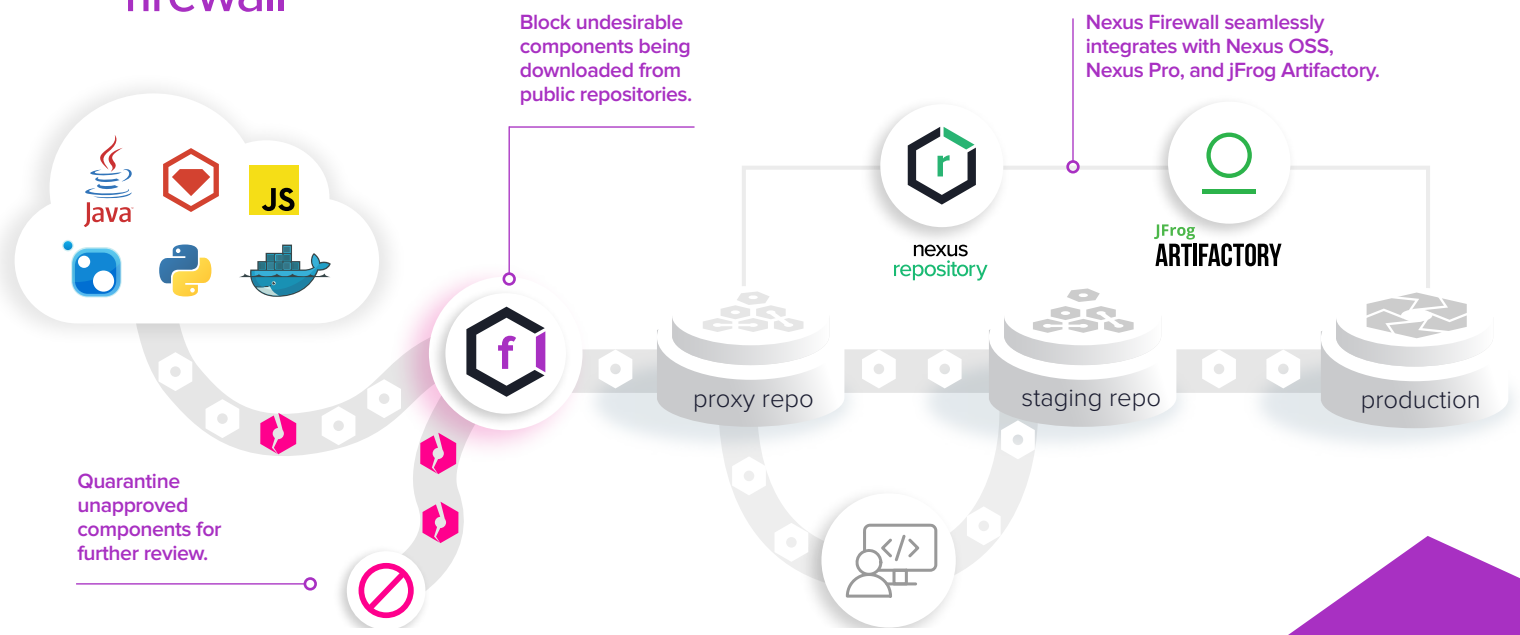


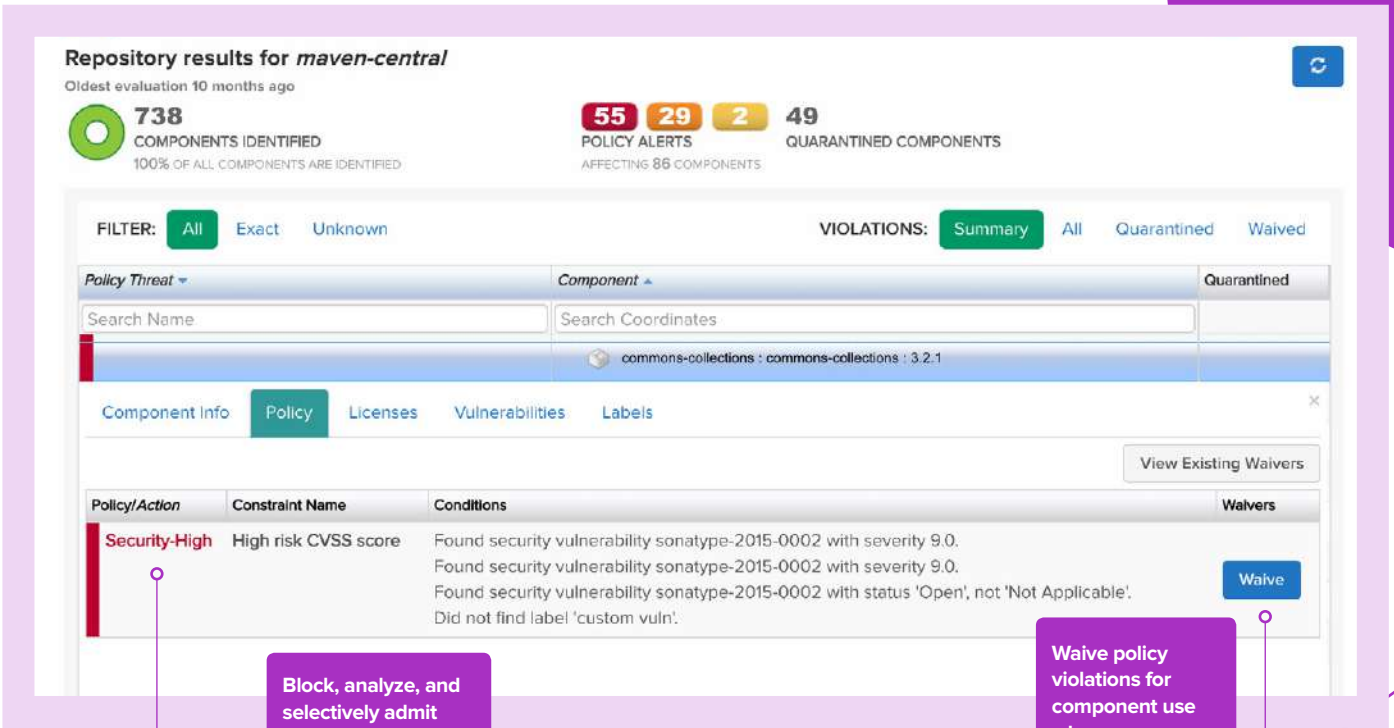
Nexus automatically enforces open source policy and controls risk across every phase of the SDLC.

nexus
firewall

THE EARLIER, THE BETTER

Block bad components at the door.





nexus repository

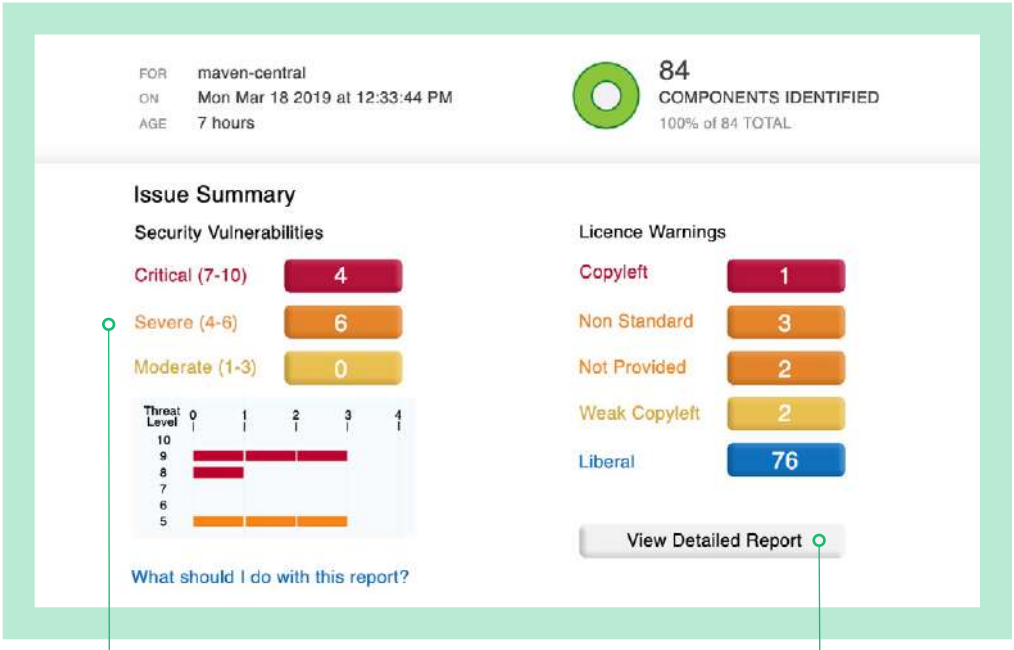
PREVENTION IS BETTER THAN A CURE.

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 often a component is being downloaded and view trending information over time.

Quickly learn the best way to remediate a vulnerable component, i.e, replace it or update it with a new version.



Understand the overall vulnerability of your repository at quick glance.

View criticality of the vulnerable components and trending information for how often that component has been downloaded.

"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

EMPOWER DEVELOPERS

Help them make better, safer component choices early in development.

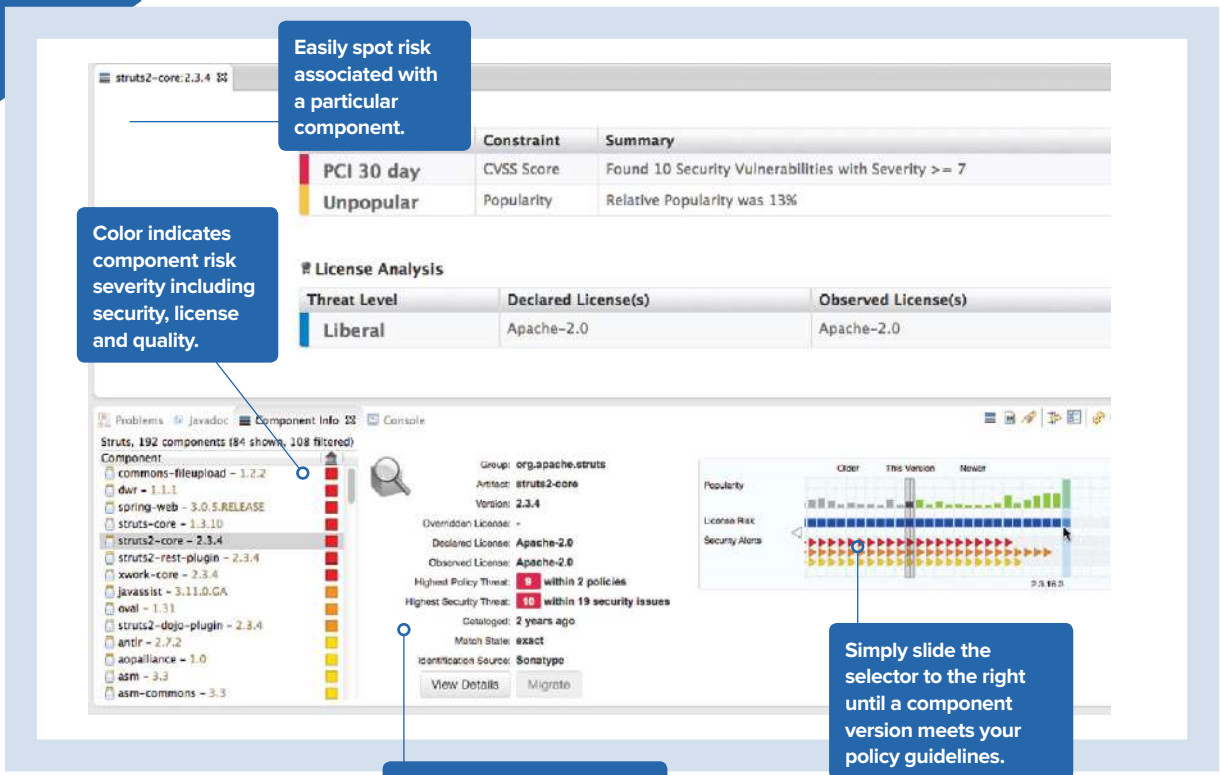
Deliver component intelligence to developers in the tools they use every day.

Choosing a safer component is as easy as using a spell checker. Just one click in your IDE or a GitHub pull request.

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

Analyze and enforce policies *automatically*.

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

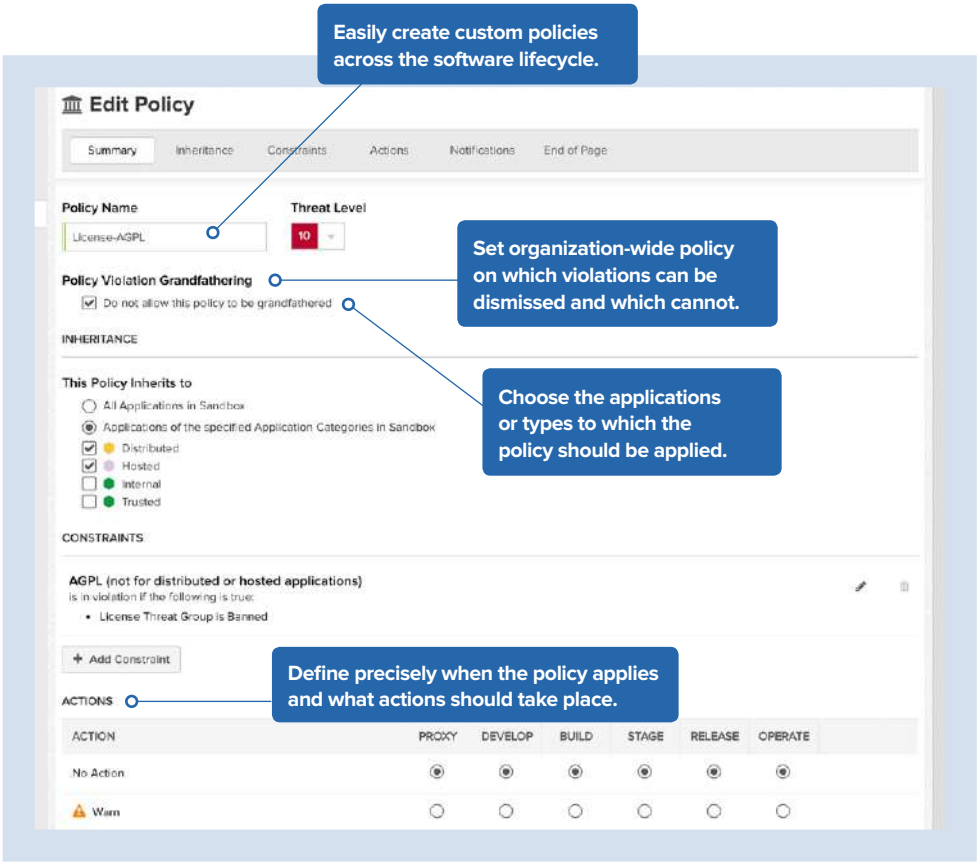
Replace inefficient workflows and the burden of manual reviews.

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.

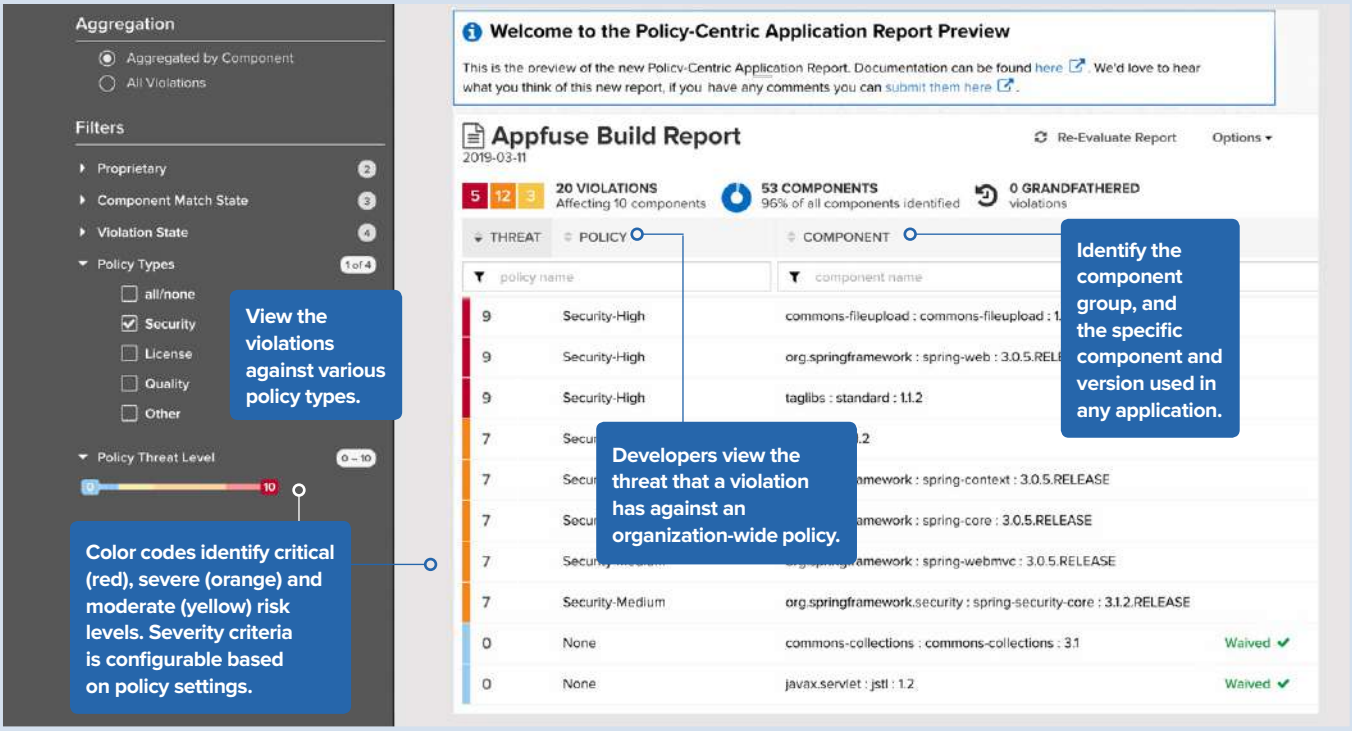
In just minutes, create an accurate software bill of materials for each application.

Identify specific components and their dependencies.

Gain access to name, license, age, popularity, known security vulnerabilities, 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



NEXUS LIFECYCLE

Get visibility and transparency for quick remediation.

"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."

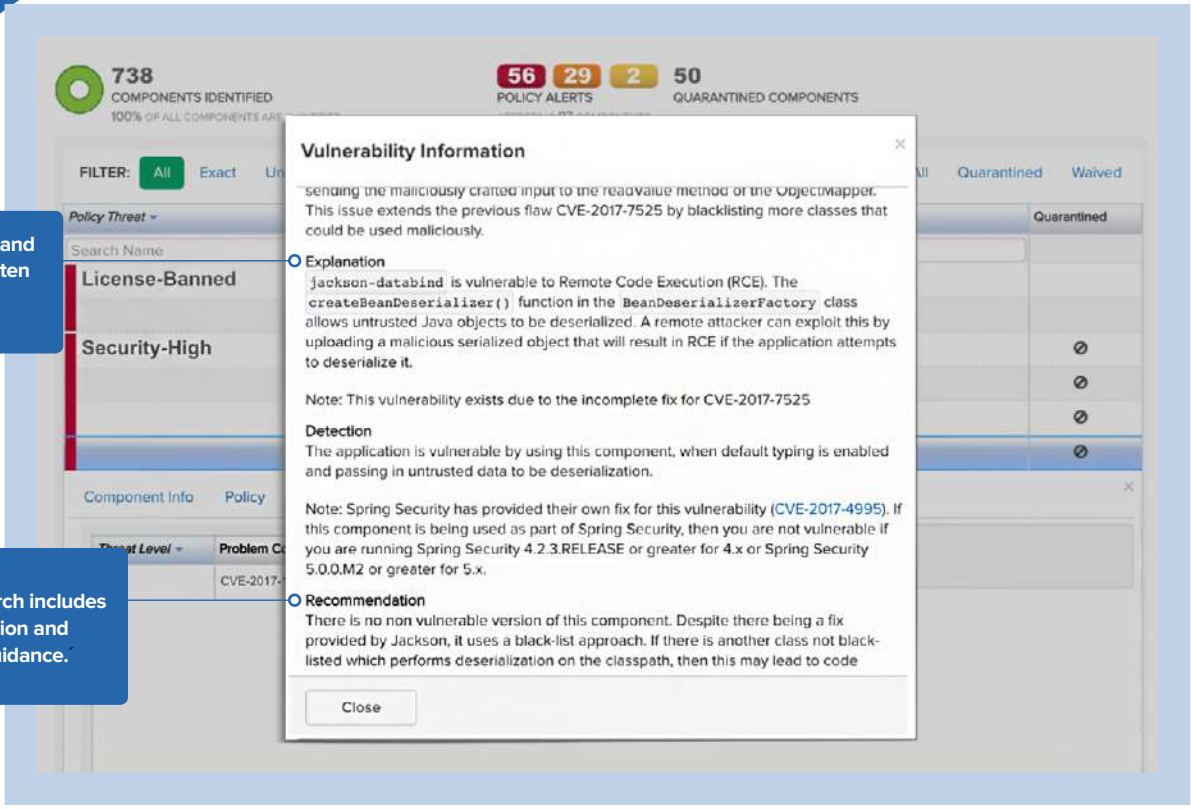
— C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

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.



"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

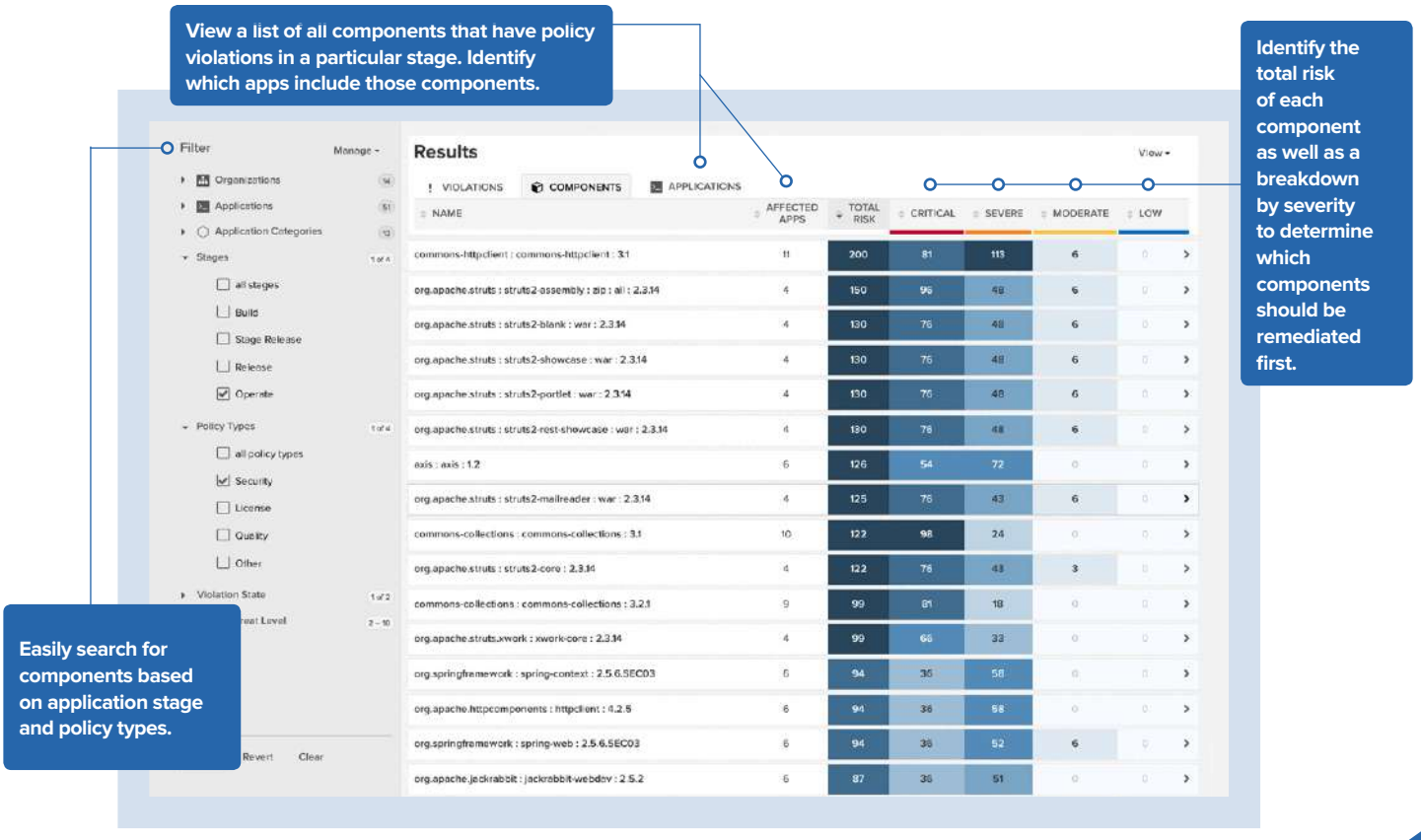
Continuously monitor for new defects.

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.



Integrations? You better believe It.

We work where you work.

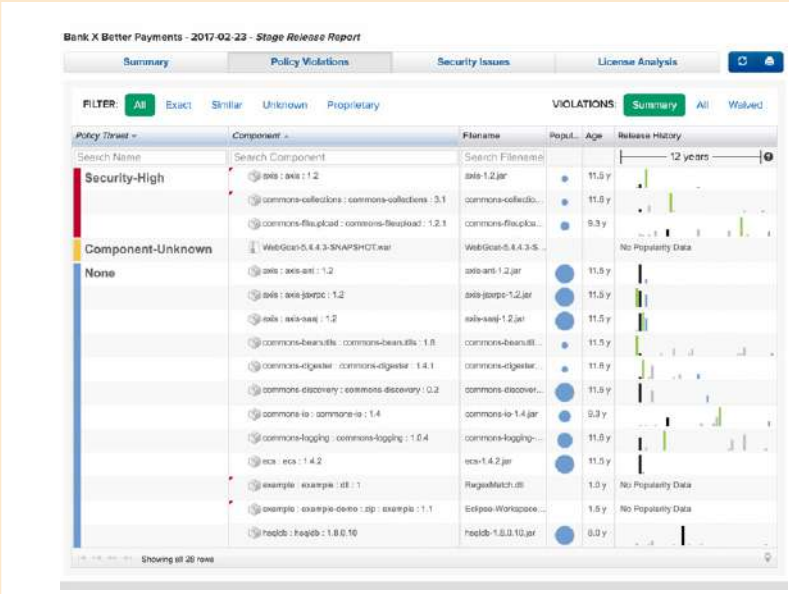
nexus vulnerability scanner

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

More than 10 million software developers rely on Sonatype to innovate faster while mitigating security risks inherent in open source. Sonatype's Nexus platform combines in-depth component intelligence with real-time remediation guidance to automate and scale open source governance across every stage of the modern DevOps pipeline.

Sonatype is privately held with investments from TPG, Goldman Sachs, Accel Partners, and Hummer Winblad Venture Partners. **Learn more at www.sonatype.com**

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
1 Primrose Street
London EC2A 2EX
United Kingdom

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

Sonatype Inc.
www.sonatype.com