Sonatype

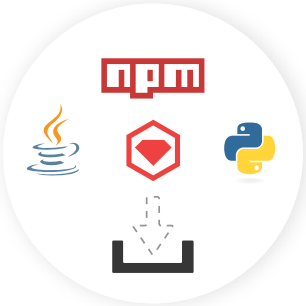
ACCELERATE DEVOPS

Early, Everywhere, at Scale

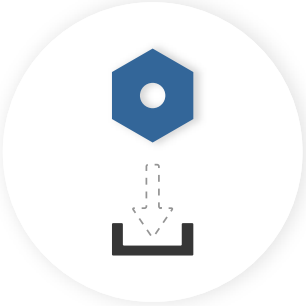
WIN THE INNOVATION BATTLE

Software developers use open source and third party components to be more competitive and speed time to innovation. Because of this, open source usage is massive and it's growing. Over 7,000 new projects and 70,000 open source components (versions) are released each week and in 2016 alone, there were over 100 billion download requests for Java, npm, PyPI, and RubyGem components from public repositories. In fact, 80% of a typical application is comprised of open source components.

Sounds great, right? Well not everything is perfect. Many of the components being downloaded have known security vulnerabilities, 1 in 16 to be exact. So, how do you ensure that you are taking advantage of all the good that open source has to offer but none of the bad?



Over 100 billion download
requets of Java, npm, PyPI, and RubyGems in 2016

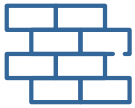


200,000+
components downloaded by an average company annually

1 in 16
open source component downloads contain a known security vulnerability

SECURE OPEN SOURCE COMPONENTS

According to a recent DevSecOps survey:



50% increase in verified or suspected breaches related to open source components from 2014-2017

Only 57% of organizations have open source governance policies in place to keep bad components out of their software supply chains

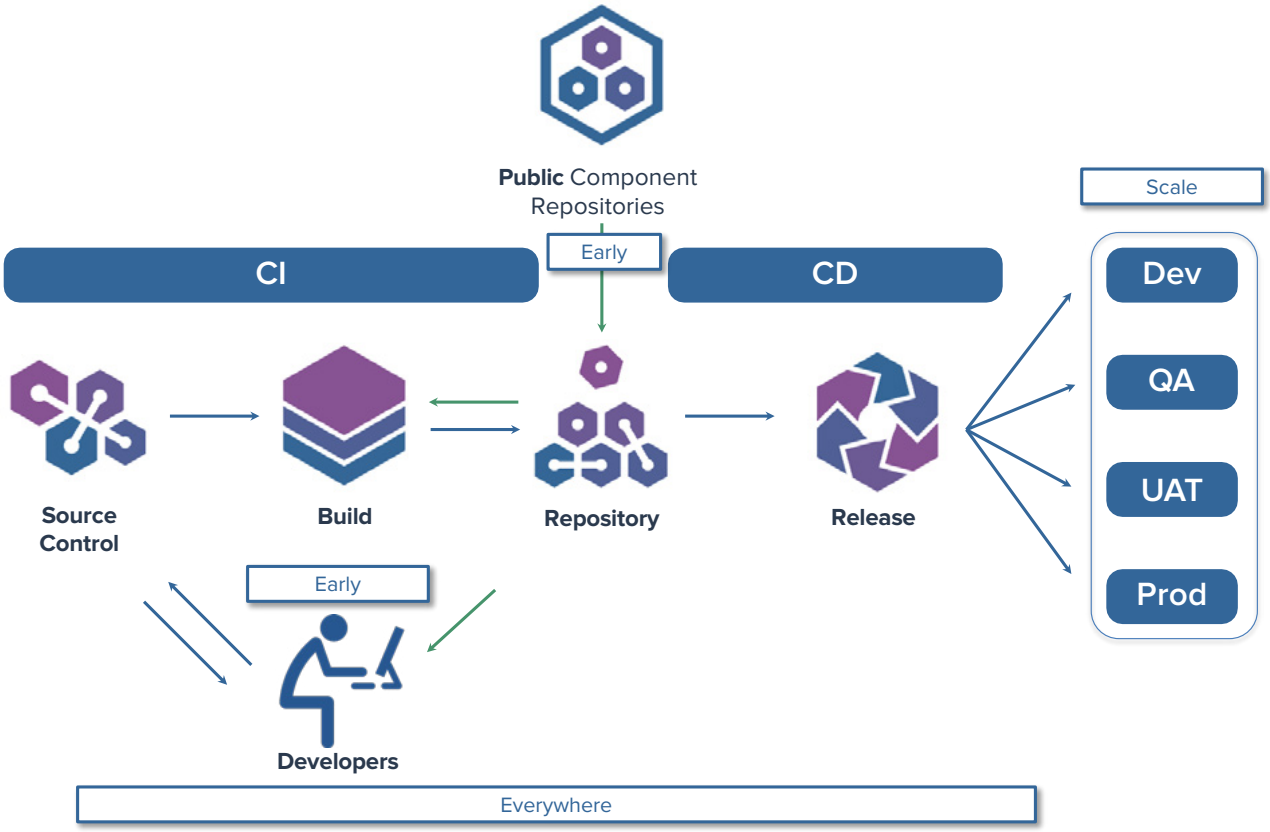
88% of organizations are worried about container security but only 47% have implemented security products to identify vulnerabilities in containers

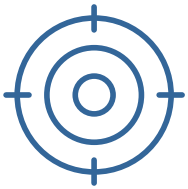
---

Gartner

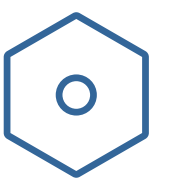
"By 2019, more than 70% of enterprise DevOps initiatives will have incorporated automated security vulnerability and configuration scanning for open source components."

The Nexus Platform helps you accelerate DevOps early, everywhere, at scale with precise component intelligence.





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



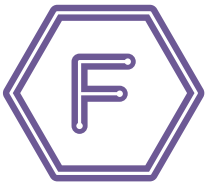
Everywhere
Nexus accelerates DevOps by integrating with the most widely used tools at every stage of the development pipeline.

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

Precise Intelligence

The Sonatype Data Research team uses a combination of automated analysis and human curation to identify vulnerabilities associated with open source software. Combined with patented identification algorithms, Nexus is architected to produce no false positives or negatives.

NEXUS PLATFORM -
Early, Everywhere, at Scale



Nexus Firewall

Vet parts early and stop defective components from entering your DevOps supply chain

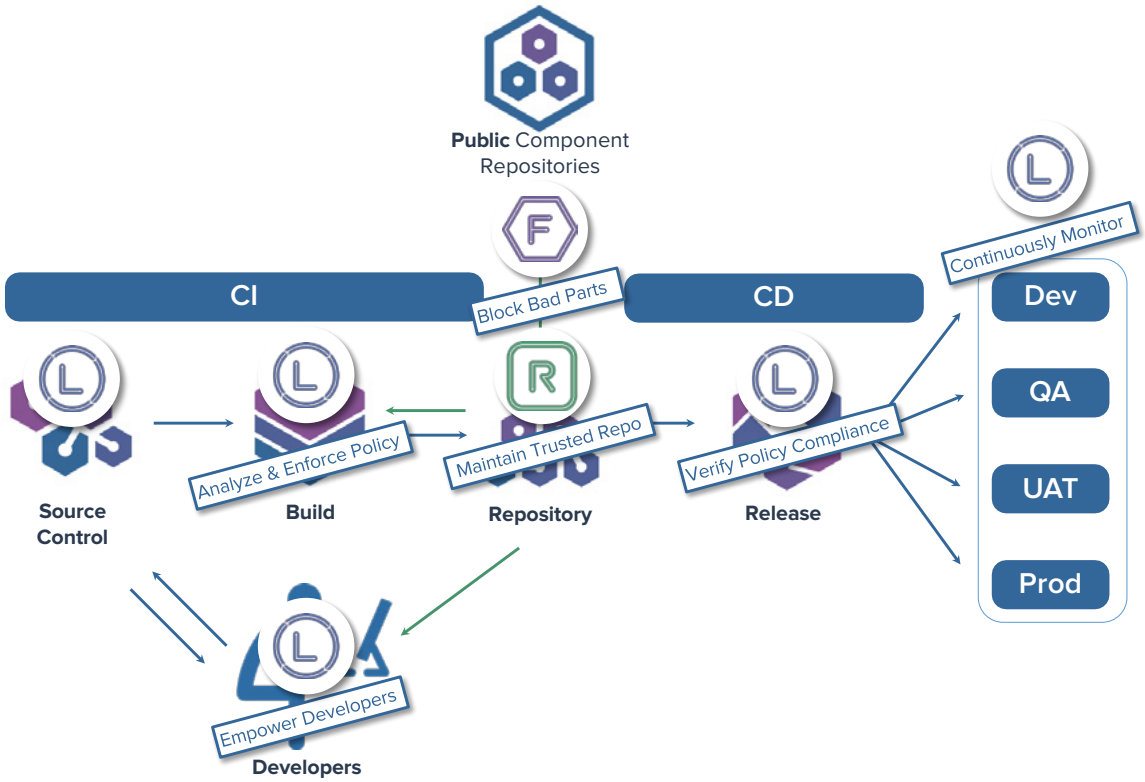
Nexus Repository

Organize and store parts in a universal repository and share them across the DevOps pipeline

Nexus Lifecycle

Empower teams and infuse every phase of your pipeline with precise component intelligence

NEXUS PROVIDES VALUE ACROSS THE ENTIRE DEVELOPMENT PIPELINE.



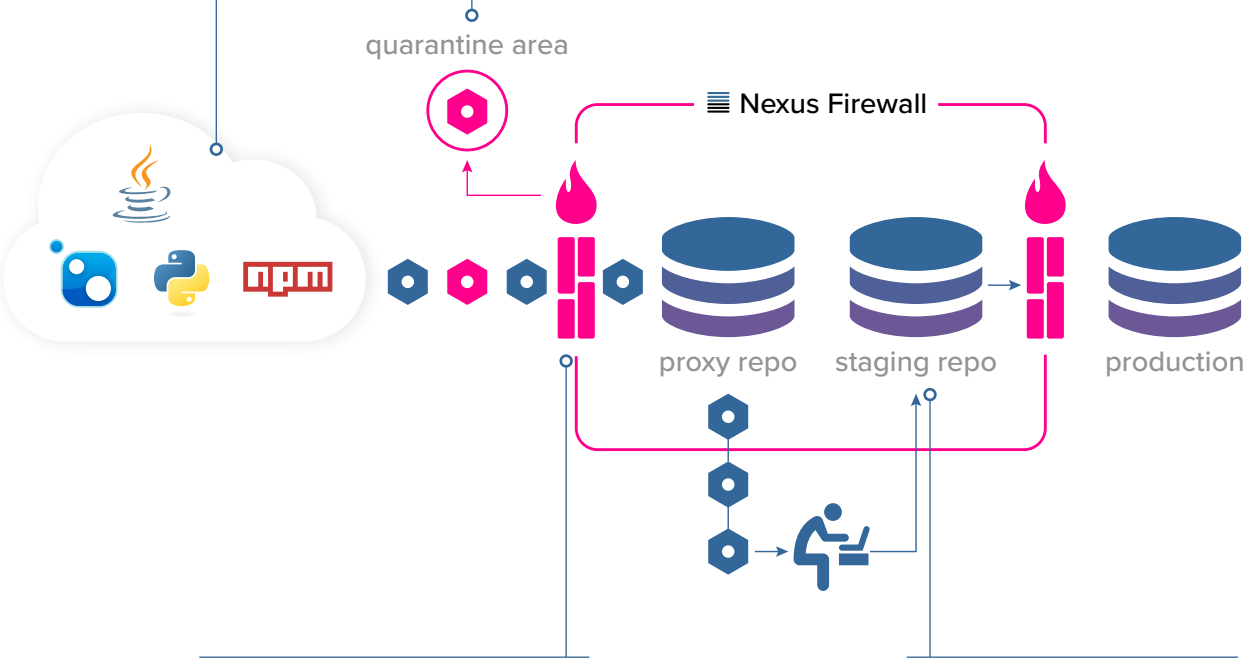
EARLY

Block bad parts at the earliest possible point.

- Shield development from easily avoidable waste and risk with a clean repository.
- Accurately and automatically check each component downloaded to your Repository Manager against your policy.
- Components age more like milk than wine, so they are rechecked against your policies across staging repositories.
- Constantly updated, privately curated component intelligence covering vulnerability, license, version and other data reduces false positives and speeds remediation.

Block undesirable components being downloaded from public repositories.

Quarantine unapproved components for further review.



Check each component download request against your policy.

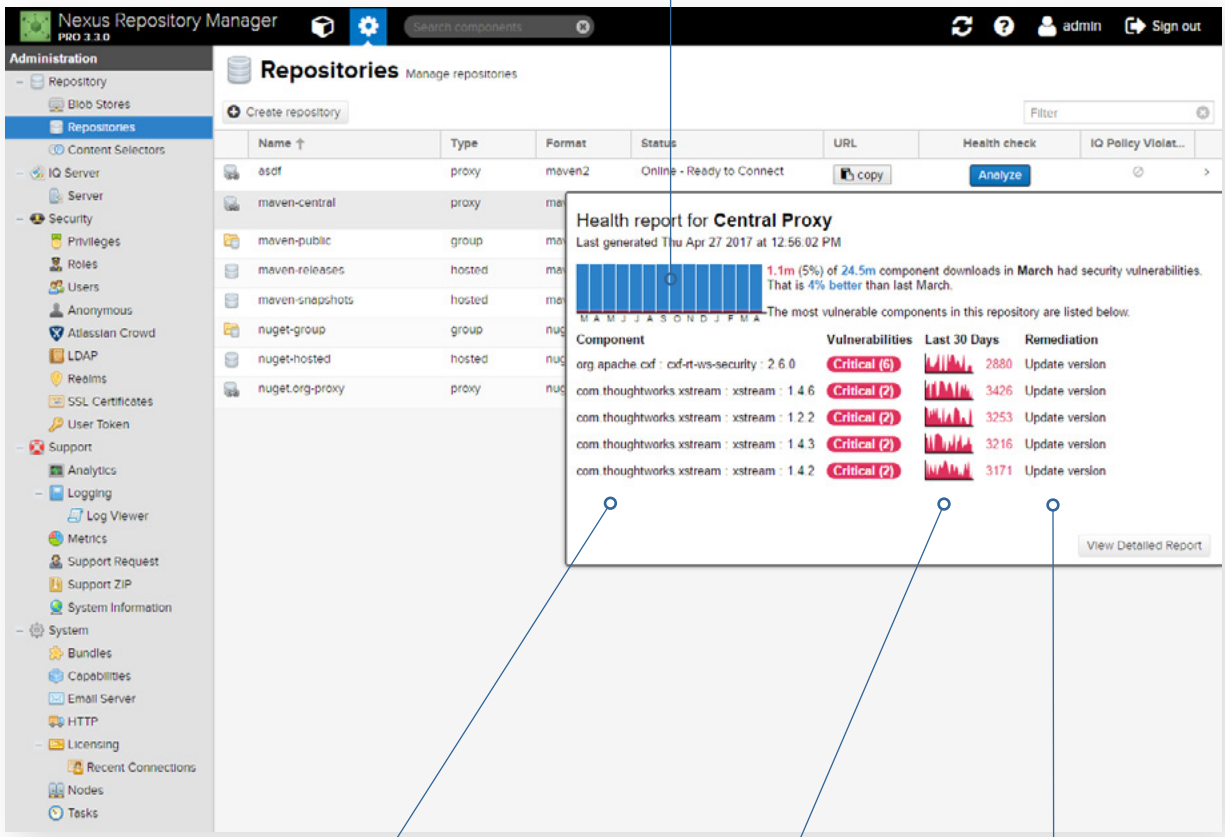
Policy enforcement continues across staging repositories.

EARLY

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.
- View the top five components in need of remediation, prioritized by the severity and impact of the vulnerability.
- 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.
- Easily avoid known security and license issues for Maven/Java, npm, NuGet, and PyPI components before they are used in your applications.

Number of downloads by month and the percentage that are vulnerable. See comparison to same month, previous year.



Top 5 most vulnerable components in your repository.

View criticality of the vulnerable components and trending information for how often that component has been downloaded in the last 30 days.

Information on how best to remediate the vulnerable component.

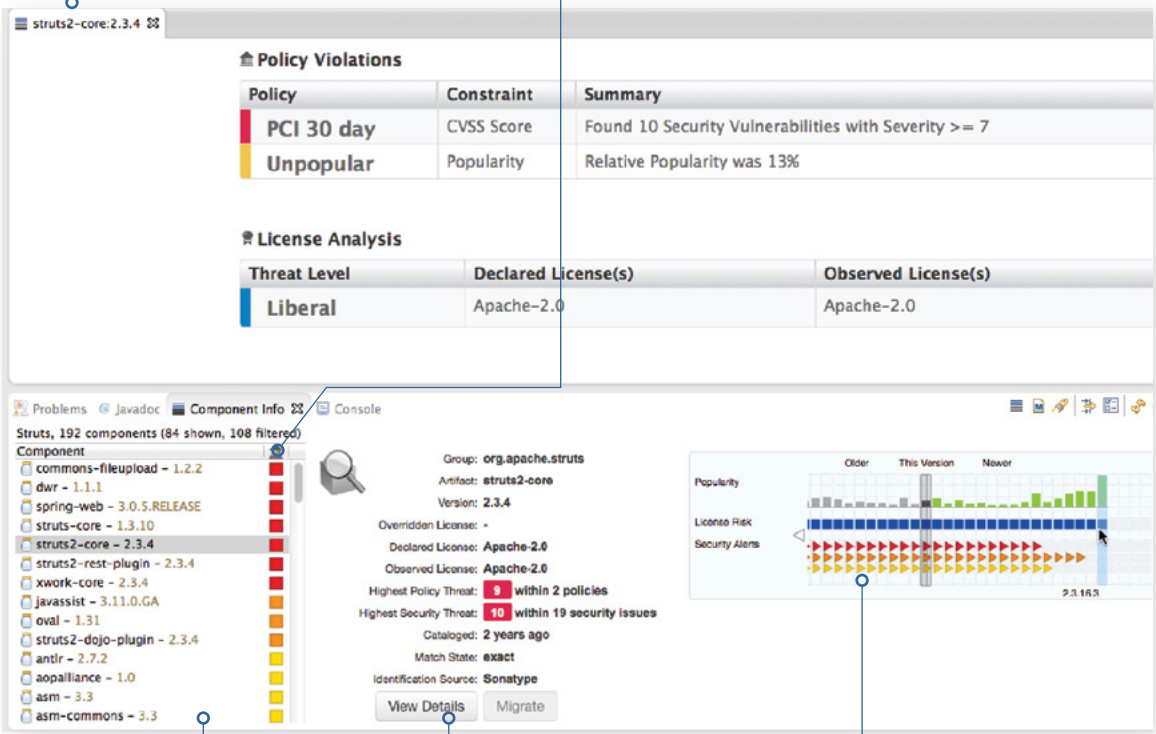
EARLY

Empower developers to choose the best, safest components.

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

Easily spot risk associated with a particular component.

Color indicates component risk severity including security, license and quality.



Define precisely when the policy applies and what actions should take place.

Details are easy to see and understand at-aglance.

Simply slide the selector to the right until a component version meets your policy guidelines.

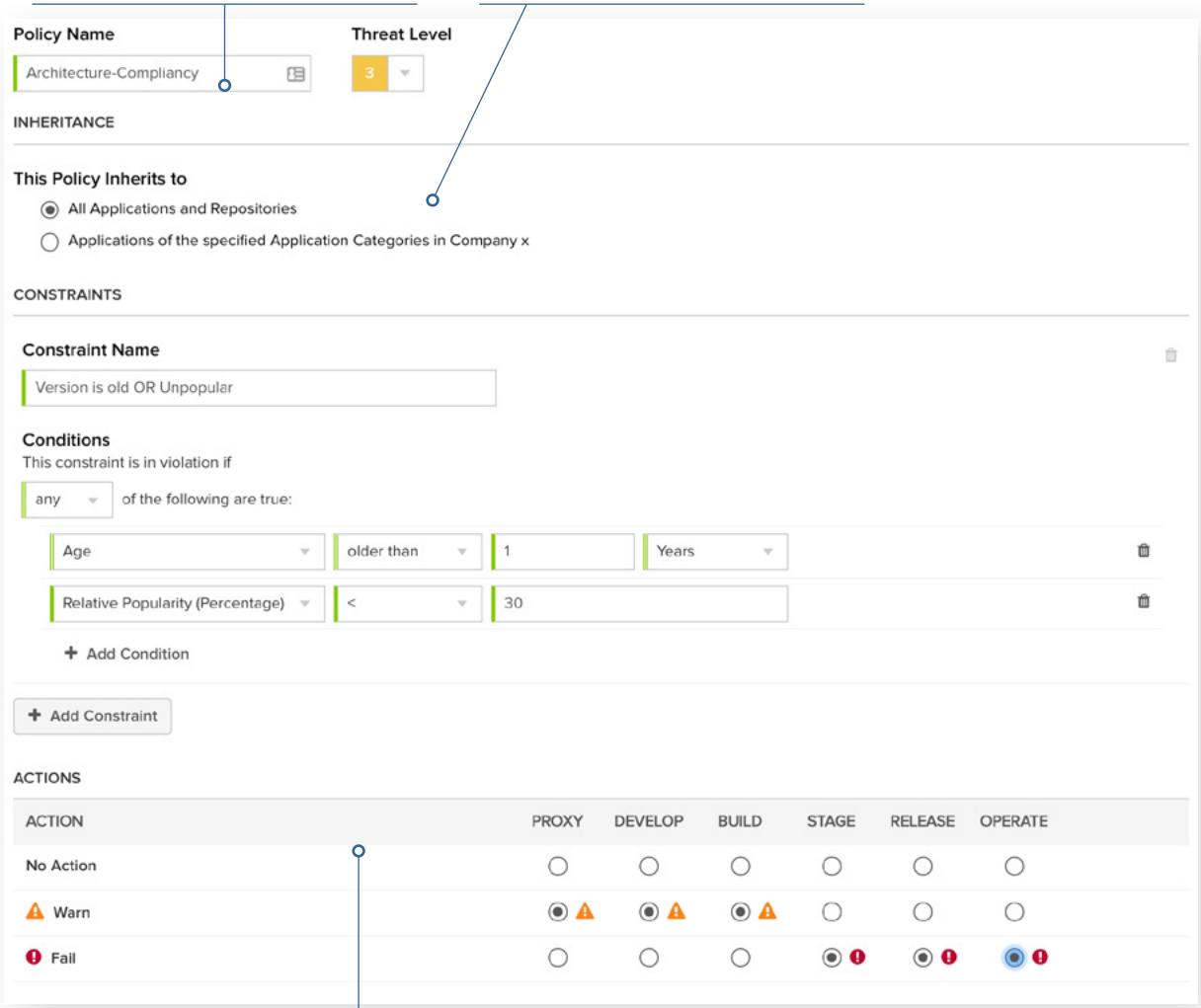
EVERYWHERE

Analyze and enforce policy automatically.

- Ensure that policies are enforced as components are consumed across a variety of development tools, like Nexus Repository, Eclipse, Jenkins, Hudson, Bamboo, Maven, SonarQube, GitHub, Chef, Puppet, Xebia Labs and more.
- Replace inefficient workflows and the burden of manual reviews.
- Utilize ‘out-of-the-box’ policies to gain an immediate view of security, license and quality risk.
- Customize policies to meet specific compliance goals or mandates.
- And do it all with automation that supports agile and continuous goals!

Easily create custom policies across the software life cycle.

Choose the applications or types to which the policy should be applied.



Define precisely when the policy applies and what actions should take place.

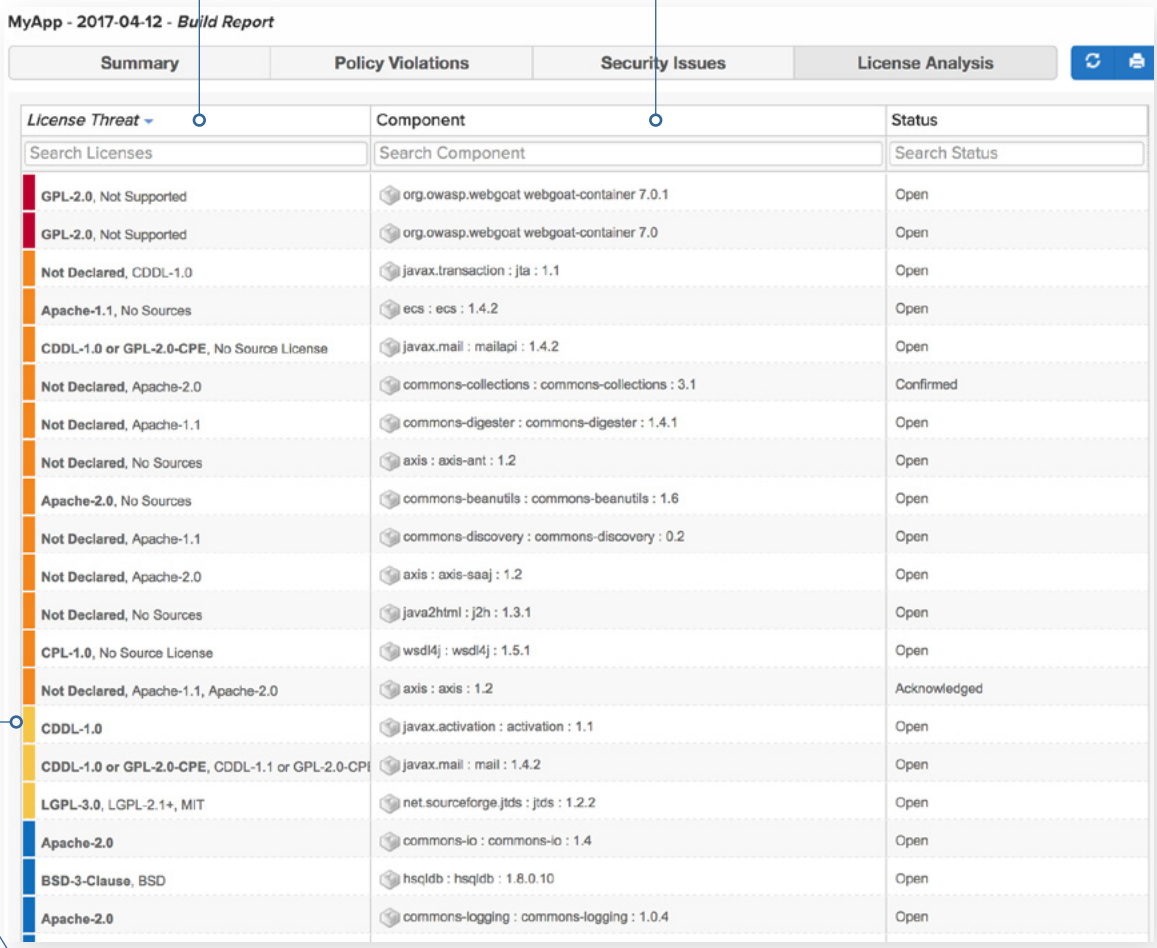
EVERYWHERE

Verify policy compliance by knowing what components are in use 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.

An inventory of components ranked by license risk. Also available by security or quality risk.

Identify the component group, and the specific component and version used in any application.



Color codes identify critical (red), severe (orange) and moderate (yellow) risk levels. Severity criteria is configurable based on policy settings.

SCALE

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.

View a list of all components that have policy violations in a particular stage. Identify which apps include those components.

Identify the total risk of each component as well as a breakdown by severity to determine which components should be remediated first.

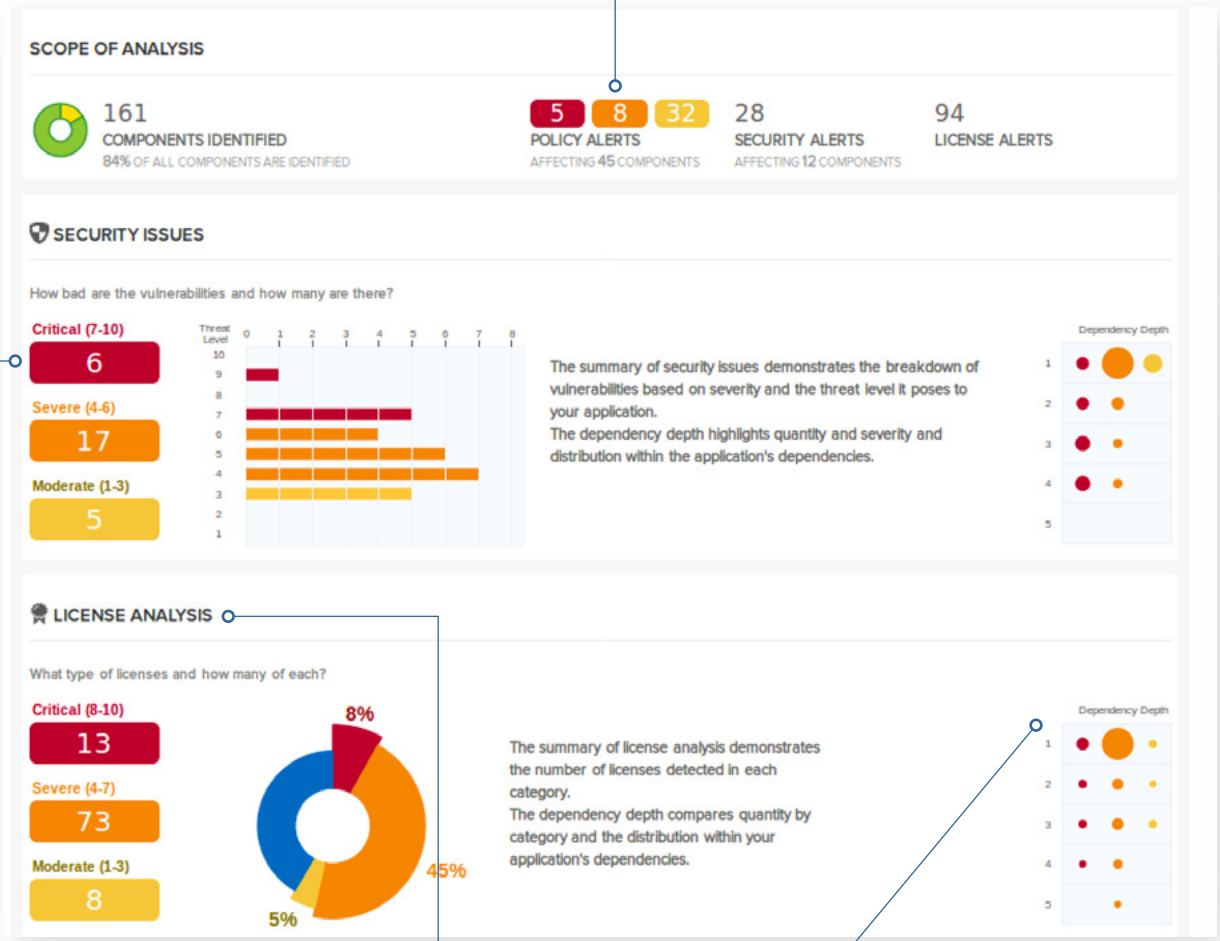
Easily search for components based on application stage and policy types.

SCALE

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.

Easily spot the risk level and policy violations.



See vulnerabilities based on severity and threat level posed.

See licenses detected.

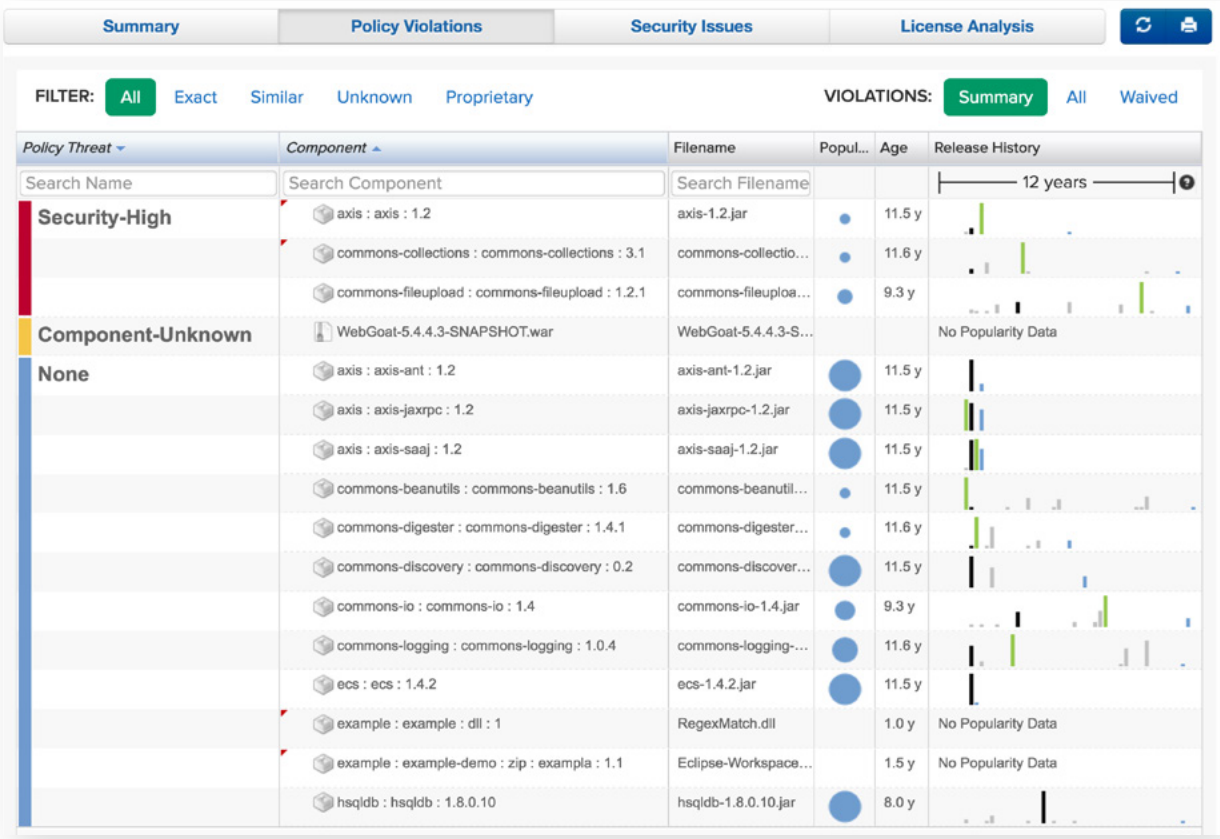
Discover how deep issues identified are in the dependency tree.

INTEGRATE AT EVERY POINT

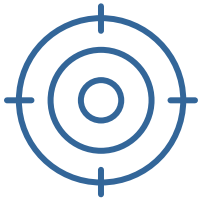
in your DevOps Toolchain

START YOUR JOURNEY

Got 5 minutes? Run a free Software Bill of Materials to understand what components are being used in your applications. www.sonatype.com/BoM



Sample Software Bill of Materials from Sonatype.



Early

Everywhere

at Scale

Sonatype

Sonatype is the leading provider of DevOps-native tools to automate modern software supply chains. As the creators of Apache Maven, the Central Repository, and Nexus Repository, Sonatype pioneered componentized software development and has a rich history of supporting open source innovation. Today, more than 120,000 organizations depend on Sonatype's Nexus platform to govern the volume, variety, and quality of open source components flowing into modern software applications. Sonatype is privately held with investments from New Enterprise Associates (NEA), Accel Partners, Hummer Winblad Venture Partners, Morgenthaler Ventures, Bay Partners and Goldman Sachs.
Learn more at **www.sonatype.com**

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

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