

## NEXUS

"**Nexus** is a **repository** manager. It allows you to proxy, collect, and manage your dependencies so that you are not constantly juggling a collection of JARs. It makes it easy to distribute your software. Internally, you configure your build to publish **artifacts** to **Nexus** and they then become available to other developers.

Sonatype Nexus and Apache Maven are two pieces of software that often work together but they do very different parts of the job. Nexus provides a repository while Maven uses a repository to **build** software.

Java-based (JDBC) data connectivity to SaaS, NoSQL, and Big Data. Download Now. My goal is to compare Sonatype **Nexus** and JFrog **Artifactory**, the two leading open source Maven repository managers. ... A customer of mine is considering using a repository manager for Maven artifacts management.

The importance of **artifact repository** and **repository management** have been continuously increasing. **Artifact repository** is a collection of binary software **artifacts** and metadata stored in a defined directory structure which is used by clients such as Maven, Mercury, or Ivy to retrieve binaries during a build process.

**Nexus**, also known as sufficient physical presence, is the determining factor of whether an out-of-state business selling products into a state is liable for collecting sales or use tax on sales into the state. **Nexus** is required before a taxing jurisdiction can impose its taxes on an entity.

Server ID is a unique ID which is used to reference the Repository Manager in Build Pipeline scripts, it should be alphanumeric without spaces. The **Nexus Jenkins** Plugin uses **Jenkins** credentials provider to manage server credentials.

**JFROG ARTIFACTORY OPEN SOURCE** FOR ARTIFACT LIFE-CYCLE MANAGEMENT. JFrog's **Artifactory open source** project was created to speed up development cycles using binary repositories. It's the world's most advanced repository manager, creating a single place for teams to manage all their binary artifacts efficiently.

In the case of the **Maven repository**, the primary type of binary **artifact** is a JAR file containing Java bytecode, but there is no limit to what type of **artifact** can be stored in a **Maven repository**. ... In **Maven**, every software **artifact** is described by an XML document called a Project Object Model (POM).

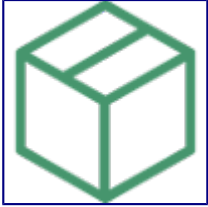
An **artifact** is one of many kinds of tangible by-products produced during the development of software. Some **artifacts** (e.g., use cases, class diagrams, and other Unified Modeling Language (UML) models, requirements and design documents) help describe the function, architecture, and design of software.

**Nexus Lifecycle**. Website. **Nexus Lifecycle** gives you full control over your software supply chain and allows you to define rules, actions, and policies that work best for your organization and teams.

# Nexus Repository

Expert flow control for binaries, build artifacts, and release candidates.

**A single source of truth for ALL your software parts.**



## Universal

Support all popular component formats.



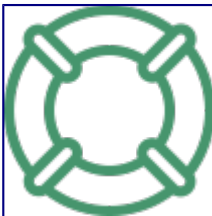
## Intelligent

Automatically identify unhealthy parts.



## High Availability

Always-on for continuous delivery and deployment.



## Support

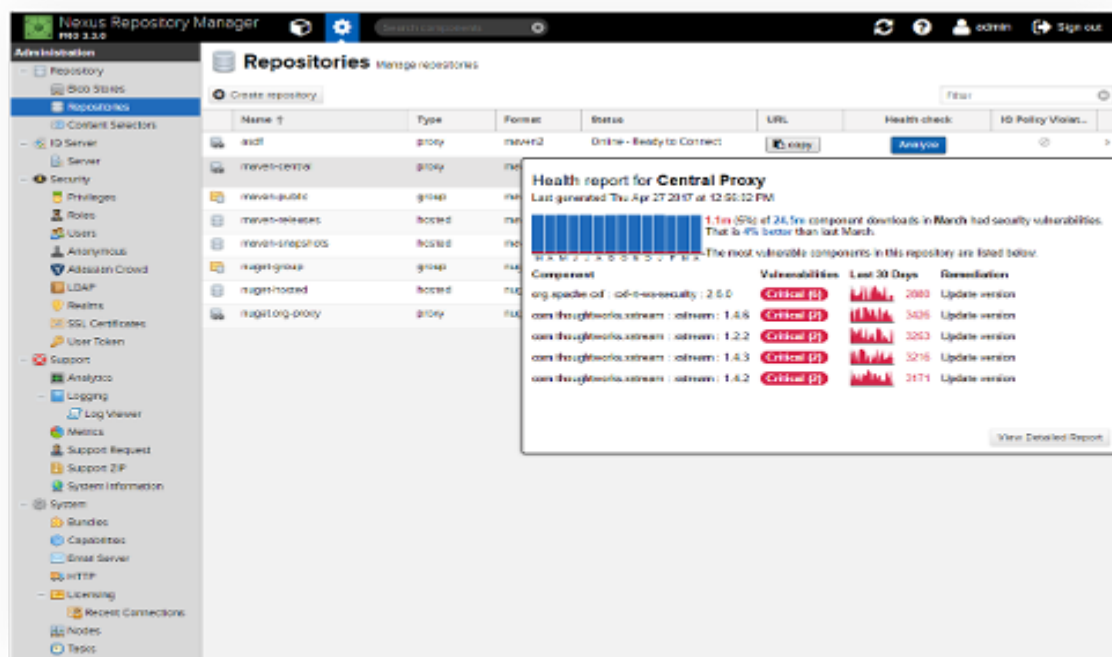
Rest comfortably with care from world-class experts.

**The perfect system of record for all your software parts.**

- Manage components, build artifacts, and release candidates in one central location.
- Understand component security, license, and quality issues.
- Modernize software development with intelligent staging and release functionality.
- Scale DevOps delivery with high availability and active/active clustering.
- Sleep comfortably with world-class support and training.

## Universal support for all your favorite formats and tools.

- Store and distribute Maven/Java, npm, NuGet, RubyGems, Docker, P2, OBR, APT and YUM and more.
- Manage components from dev through delivery: binaries, containers, assemblies, and finished goods.
- Awesome support for the Java Virtual Machine (JVM) ecosystem, including Gradle, Ant, Maven, and Ivy.
- Integrated with popular tools like Eclipse, IntelliJ, Hudson, Jenkins, Puppet, Chef, Docker, and more.



## Why Nexus Repository is the Best



### High Availability

High-availability that is uniquely affordable, rapidly configured, and easily managed.



### Universal Format Support

Universal support for popular component formats including Java, npm, Bower, NuGet, Docker, PyPI and RubyGems.



### Advanced Intelligence

Evaluate open source and third-party components for license types, security vulnerabilities, popularity and age.

#### Feature

#### Nexus Repository Pro

#### Artifactory Pro

Active/Active High Availability

#### Built In

Starts at \$1200 / year

#### Upgrade to Pro Enterprise

Starts at \$29,500 / year

#### Repository Health Check

#### Built In

Starts at \$1200 / year

#### Upgrade to Pro X + 3rd Party Tools

Starts at \$14,400 / year

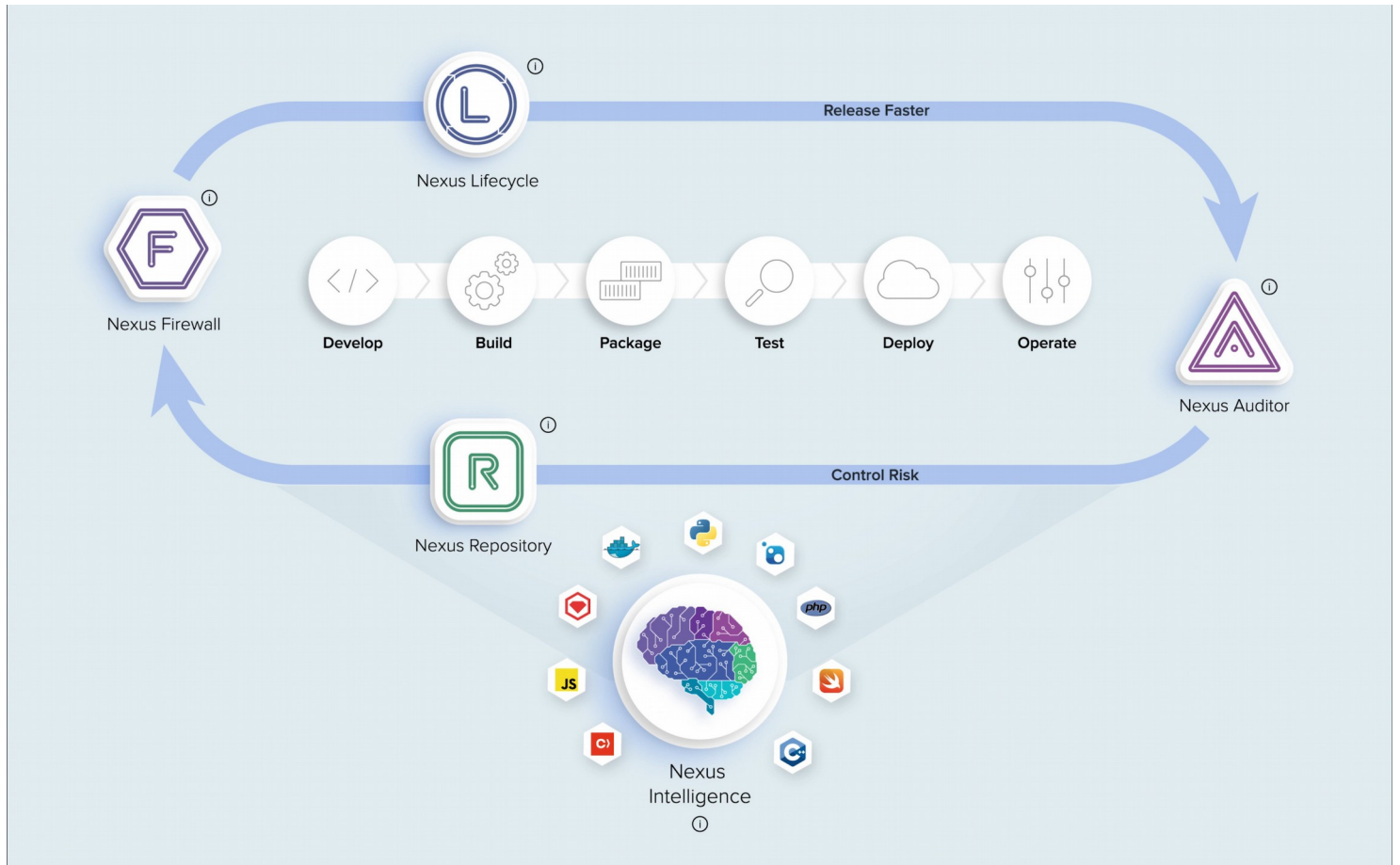
#### Universal Component Support

#### Free in OSS Version

#### Upgrade to Pro Edition

# Nexus Platform Overview

**Innovate faster and automatically control open source risk.**

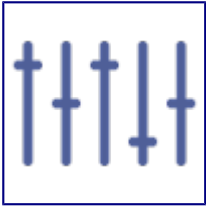


**Explore the Nexus Platform**

## Nexus Lifecycle

**Precise open source intelligence for your entire DevOps pipeline.**

**Open source governance for enterprise DevOps.**



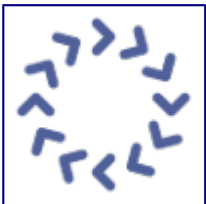
### **Control**

Define open source component policies by organization, team, and application type.



### **Integrate**

Continuously visualize component intelligence within your favorite tools (including Nexus and Artifactory).



### **Automate**

Automatically and contextually enforce policies across your entire DevOps pipeline.



### **Customize**

Pair component intelligence with in-house apps using supported REST APIs.

**Nexus knows open source.**

**Remarkably precise and accurate data.**

- 99% accuracy eliminates false positives/negatives.
- 30,000 new packages analyzed every day.
- 811,200 hours of research by security experts.
- Reduce MTTR from 6 weeks to 6 seconds.

**Integrated with all your favorite pipeline tools.**

- Eclipse, Visual Studio, IntelliJ IDEA, Jenkins, Hudson, Bamboo, Maven, Docker, SonarQube, and more.

**Nexus IQ Server**  
Lifecycle 4.6.0-SNAPSHOT

Filter Manage

Organizations 1 of 1  
☒ all/none  
☒ Boleh

Applications 3 of 3

Application Categories 1

Stages 4

Policy Types 1 of 4  
☐ all/none  
☒ Security  
☐ License  
☐ Quality  
☐ Other

Violation State 1 of 2  
☐ all/none  
☒ Open  
☐ Waived

Policy Threat Level 0 - 10

Apply Revert Clear

**Results** Export Components Data

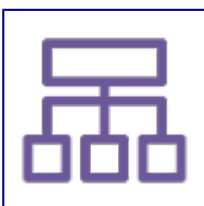
! VIOLATIONS 50 COMPONENTS 19 APPLICATIONS 3

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
org.bouncycastle : bcprov-jdk16 : 1.46	2	38	18	14	6	0
org.apache.activemq : activemq-core : 5.7.0	2	32	18	14	0	0
org.springframework : spring : 2.5.6	2	32	18	14	0	0
com.thoughtworks.xstream : xstream : 1.3.1	3	27	27	0	0	0
commons-collections : commons-collection...	3	27	27	0	0	0
commons-fileupload : commons-fileupload ...	3	27	27	0	0	0
org.apache.zookeeper : zookeeper : 3.3.6	3	27	27	0	0	0
org.webjars.bower jquery-ui 1.10.3	3	21	0	21	0	0
io.netty : netty-all : 5.0.0.Alpha1	3	21	0	21	0	0
org.scala-lang : scala-compiler : 2.11.7	3	21	0	21	0	0
angular 1.5.8	1	16	9	7	0	0
angular 1.5.8	1	16	9	7	0	0
commons-httpclient : commons-httpclient : ...	1	16	9	7	0	0

# Nexus Firewall

Stop open source risk at the front door.

Secure your DevOps perimeter.



## Manage

Define and enforce rules for component usage.





## Quarantine

Stop, analyze, and selectively admit components.



## Audit

Examine every component at the front door.



## Protect

Keep production apps safe from risky components.

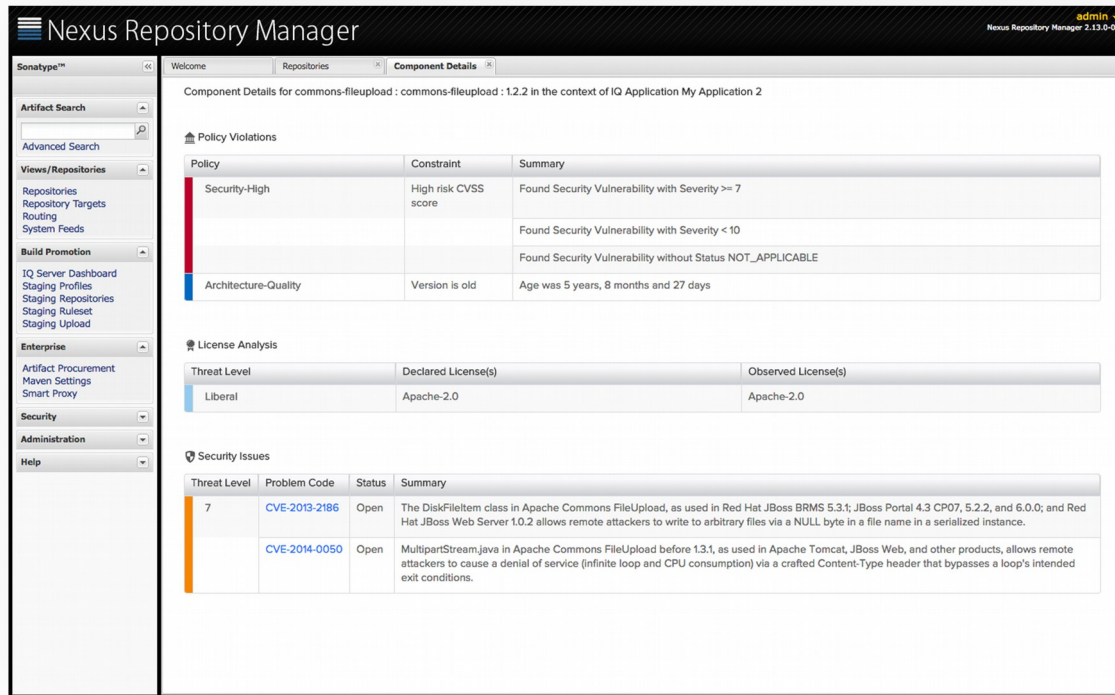
**Take the good. Leave the bad and the ugly.**

**Automatically block vulnerable open source components.**

- Block unwanted Java, JavaScript, .Net, PyPi, RubyGems, and RPM components from entering your software supply chain.
- Improve application hygiene and protect repositories, including staging and release.
- Automatically prevent risky components from entering into your applications.

**Harness all of the good in open source, but none of the bad.**

- Know which components you should or shouldn't use, across your enterprise.
- Create policies to ensure risky components never make it into production applications.
- Identify defective components, license risk, and architectural quality.



# Nexus Auditor

Know the quality of open source inside your software.

## What's in your software?



## Evaluate

Get detailed component intelligence results, down to the transitive dependency.



## **Comply**

Create policy based on existing rules or regulations.



## **Report**

Drill into findings to discover security, license, and quality related issues.



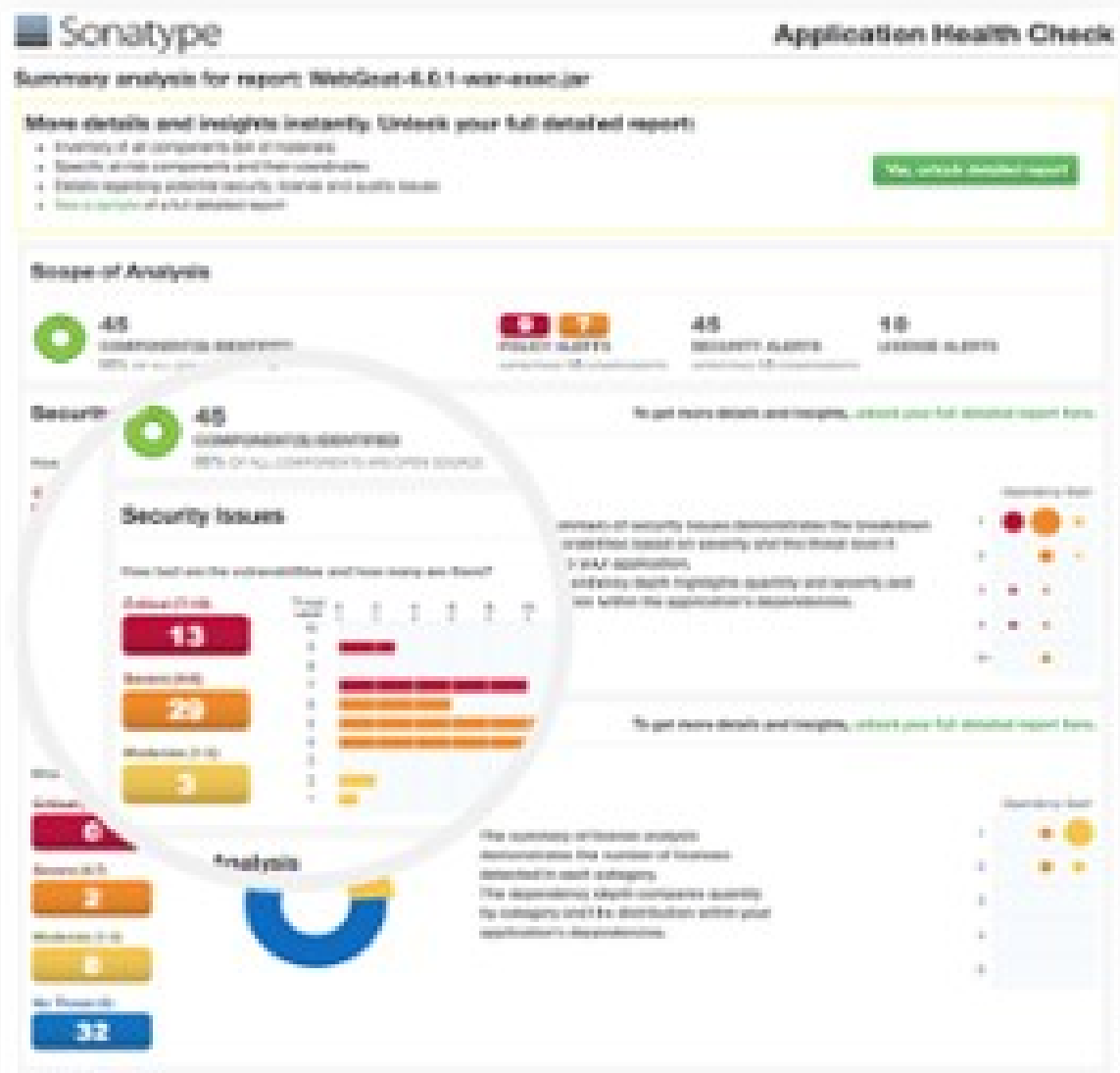
## **Maintain**

Monitor applications continuously for newly-discovered component issues.

## **Know the truth about your applications.**

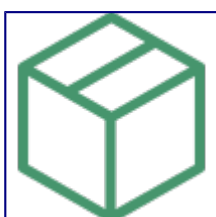
### **Determine the composition of every application, including third party apps.**

- Document the parts inside your software or COTS applications with a detailed bill of materials.
- Automatically pinpoint open source security vulnerabilities, license risk, and quality concerns.
- Remediate risk in the blink of an eye and gain first mover advantage.
- Send notifications when unwanted components are identified in evaluated applications.
- Contextually waive policy violations as appropriate.



## Nexus Repository OSS

Flow control for binaries and build artifacts.



## Store

Give your teams a single source of truth for every component they use.



## Adapt

Provide universal coverage for all major package formats and types.



## Cache

Optimize build performance and reliability by caching proxies of remote repositories.



## Scale

Install on an unlimited amount of servers for an unlimited amount of users.

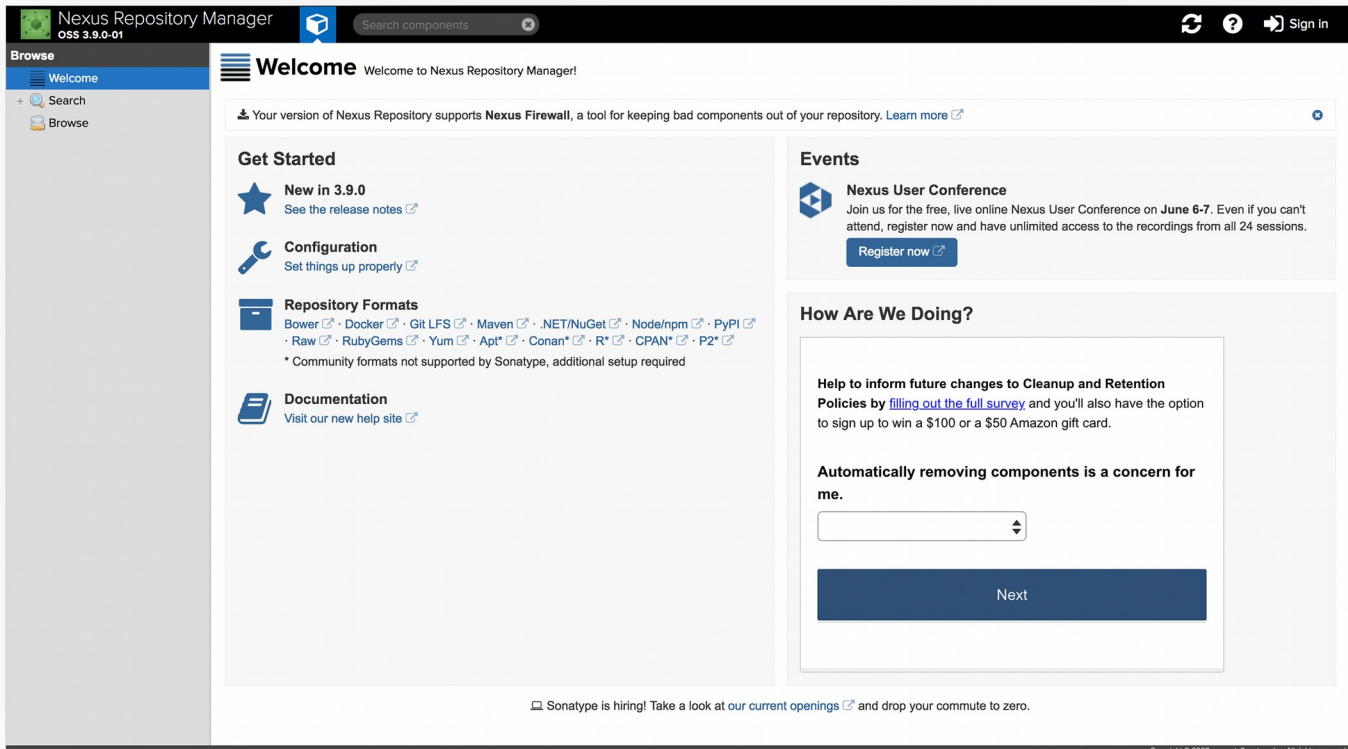
## The world's most popular repository

- Centralized repository for managing all popular component formats
- Single source of truth for all binaries and build artifacts.
- Gain insight into component security, license, and quality issues.

## Universal support for all popular formats

- Store and distribute Maven/Java, npm, NuGet, RubyGems, Docker, P2, OBR, APT and YUM and more.
- Manage components from dev through delivery: binaries, containers, assemblies, and finished goods.

- Awesome support for the Java Virtual Machine (JVM) ecosystem, including Gradle, Ant, Maven, and Ivy.
- Compatible with popular tools like Eclipse, IntelliJ, Hudson, Jenkins, Puppet, Chef, Docker, and more.



## NEXUS INTELLIGENCE

### Everything you need to know about Open Source

#### Component Identification

**Nexus Intelligence:** Advanced Binary Fingerprinting (ABF) precisely identifies components via cryptographic hash, structural similarity, derived coordinate, and file name.

**Competitors:** Identify components using file name and/or package manifest which contributes to false positives / negatives.

#### Component Data

**Nexus Intelligence:** Operates at enormous scale with highly curated intelligence on:

- 2M Unique Projects
- 31M Components
- 8B Files
- 97% of GitHub Commits
- All Major Ecosystems

**Competitors:** Operate at smaller scale with partially curated intelligence.

### **Remediation Data**

**Nexus Intelligence:** Our Automated Vulnerability Detection (AVD) engine runs 24x7x365 and combines with 65 human security experts to monitor public, private, and crowd data for new open source vulns. New critical vulns are itemized, associated to component versions, and published with dev-friendly and actionable remediation guidance within 6 hours.

**Competitors:** Monitor public data sources for new vulns and only identify a portion of risk as it emerges. Resource constrained teams perform limited research on new vulns leading to inadequate remediation guidance.

### **Security Data**

**Nexus Intelligence:** Premier source of open source risk and developer-friendly remediation guidance consists of:

- 4M Unique vulns
- 1.4M Sonatype identified
- 3% Public data (ex. NVD)
- 97% Proprietary data

**Competitors:** Commodity sources of open source risk with limited remediation guidance.

### **Architecture Data**

**Nexus Intelligence:** Offers empirical perspective on open source project hygiene and architectural concerns, including:

- Popularity
- Age
- Release history
- Usage patterns

**Competitors:** Offer limited to no insight.

**License Data**

**Nexus Intelligence:** Deep licensing visibility including:

- 211K Weak-Copyleft
- 859K Copy-left
- 177K Banned
- 1.6M Non-Standard
- 42K Commercial
- 17M Liberal

**Competitors:** Adequate licensing visibility.




























**Crowd Data**

**Nexus Intelligence:** Informed by opt-in and anonymized data aggregated from 1.5m developers and 180,000 instances of Nexus Repository Manager, generating deeper insights into developer patterns and organizational practices.

**Competitors:** Blind



# Compare Nexus Intelligence

OSS Governance Requirements	Free Tools OWASP Dependency Check, npm	Commercial Tools Black Duck, Whitesource	Enterprise Tools Sonatype Nexus Platform
Ecosystem coverage	 Partial	 Complete	 Complete
Data sources	 Public	 Public, private	 Public, private, proprietary
Component identification	 Imprecise	 Imprecise	 Precise
Vulnerability coverage	 Partial	 Partial	 Complete - 4M Vulns (1.4M identified by Sonatype)
Remediation guidance	 Generic guidance from public sources	 Generic guidance from public sources	 Expert guidance from professional researchers
Project health assessment	 None	 Partial	 Project popularity, age, and release history
License information	 None	 Complete	 Complete
Time to vulnerability awareness	 Weeks	 Days	 Hours
Policy management and enforcement	 None	 Partially automated	 Fully automated

## The Nexus Platform *Powered by Superior Intelligence*

Automatically enforce open source policy early, everywhere, at scale. Empower your development teams to release faster and control risk.



### Firewall

Confidently quarantine bad parts from entering your software supply chain. [Learn more.](#)



## Lifecycle

Automate open source governance at scale with precise and actionable intelligence. [Learn more.](#)



## Repository

Analyze the quality of components inside your parts warehouse.

### Nexus Repository Pro features:

- Staging and release functionality
- High availability
- Advanced security options
- Component intelligence via Repository Health Check
- World class enterprise support

### Nexus Firewall features:

- Always-on component intelligence
- Custom policy creation
- Automatically manage security and license risks
- Advanced reporting capabilities
- World-class enterprise support
- Requires Nexus Repository

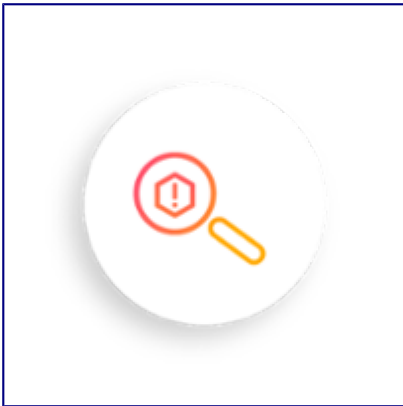
### Nexus Lifecycle features:

- Real time component intelligence integrated with existing tools
- Dashboards, detailed reporting, and tool-level interfaces
- Advanced application monitoring
- World-class enterprise support



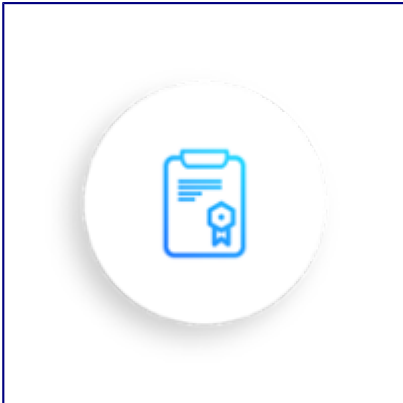
## **Component**

The average application consists of 106 open source components.



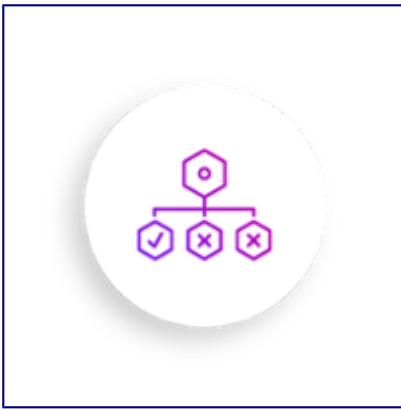
## **Vulnerability**

A typical application contains 23 known vulnerabilities.



## **License**

Most applications indicate at least 8 GPL licensed components.



## Architecture

Many components in use are old, unsupported, and unpopular.