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.

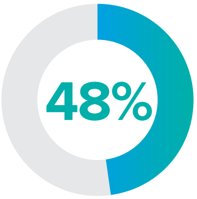
DevSecOps: Why is open source policy critical?

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**

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.

> "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

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.

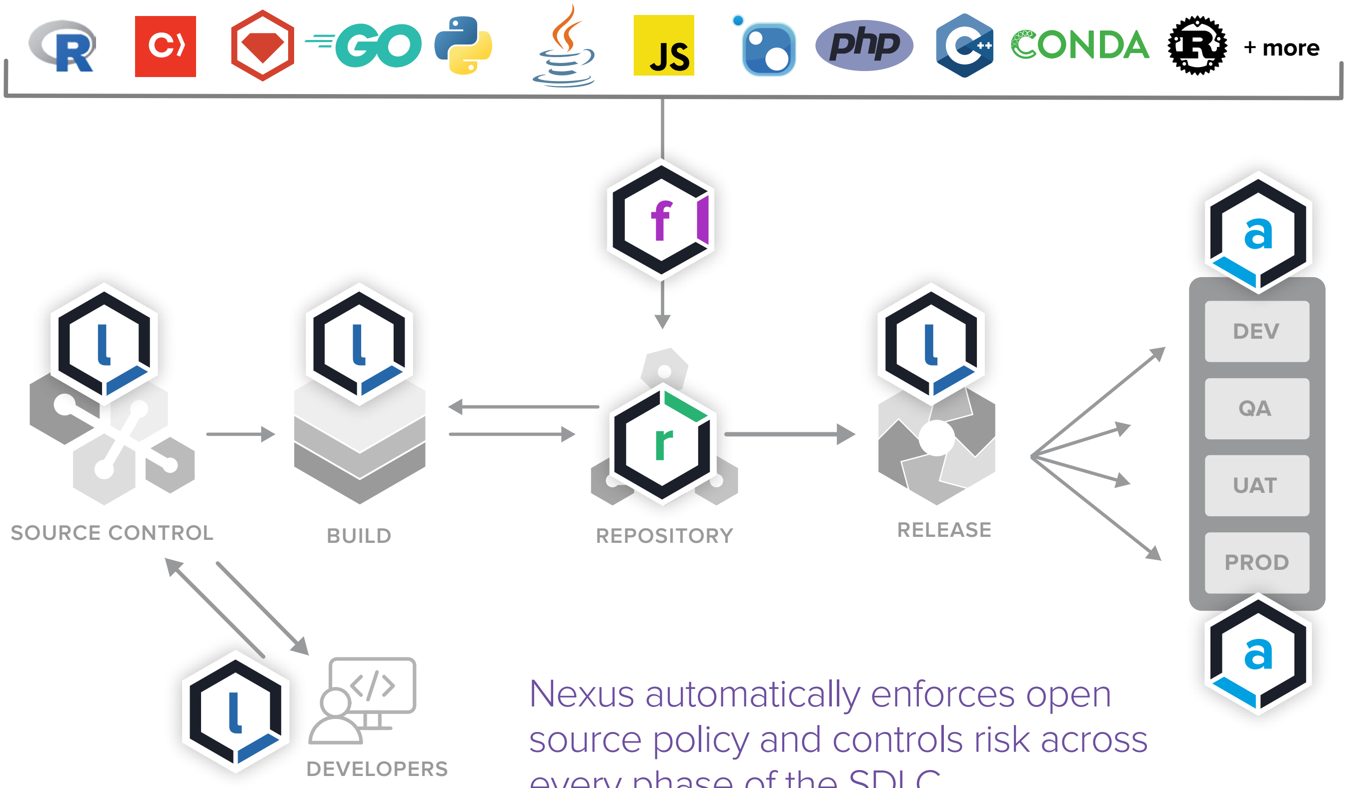
nexus repository

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

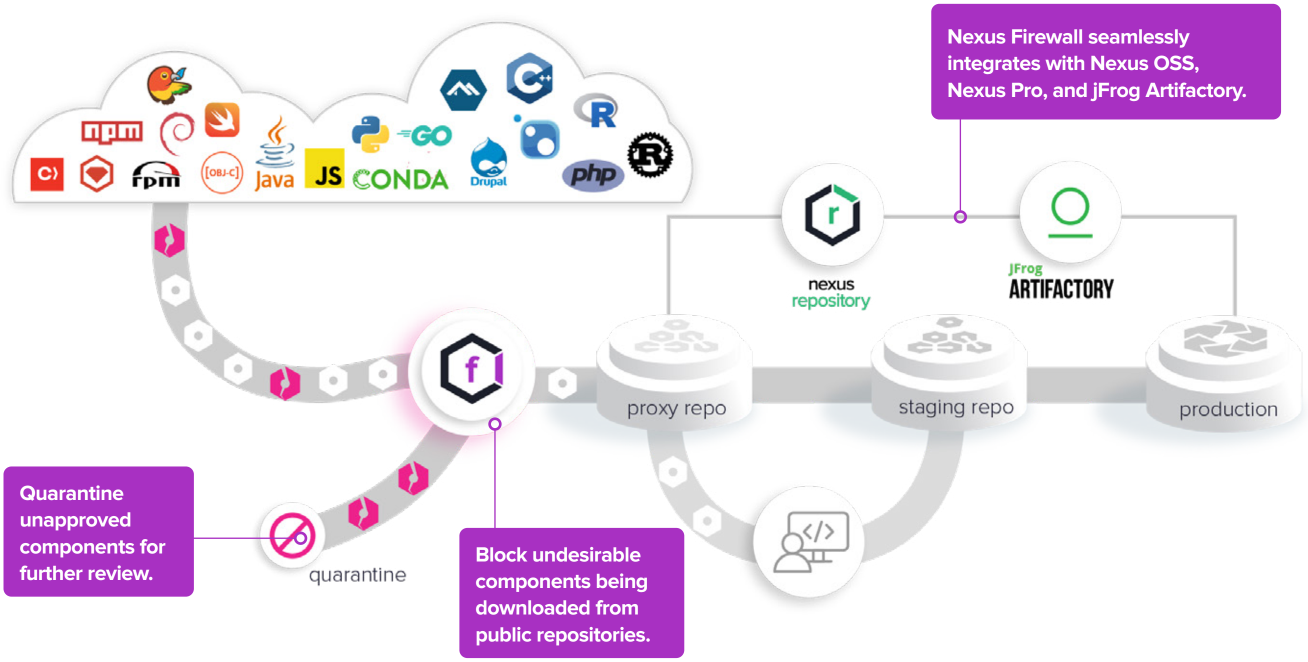


Nexus automatically enforces open source policy and controls risk across every phase of the SDLC.

nexus firewall

THE EARLIER, THE BETTER

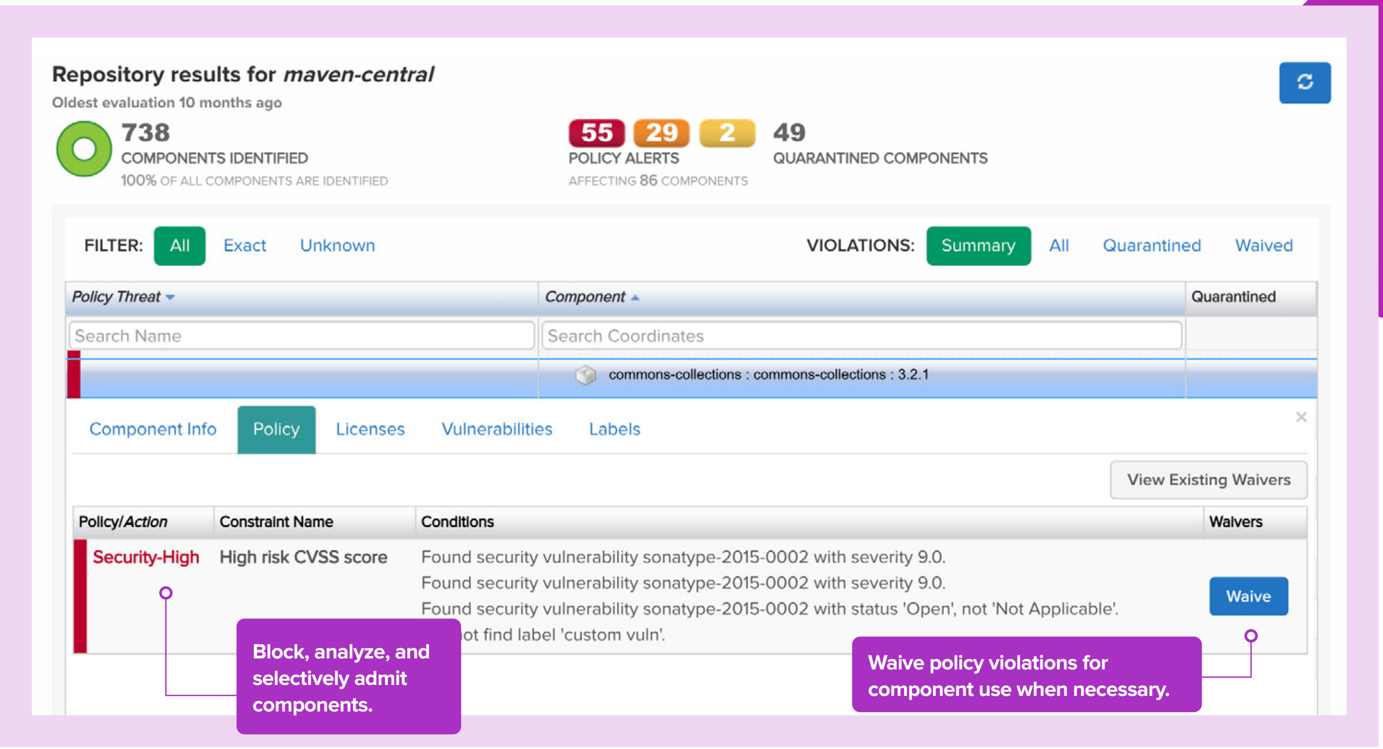
Block bad components at the door.



Nexus Firewall seamlessly integrates with Nexus OSS, Nexus Pro, and jFrog Artifactory.

Quarantine unapproved components for further review.

Block undesirable components being downloaded from public repositories.



Repository results for *maven-central*

Oldest evaluation 10 months ago

738 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE IDENTIFIED

55 29 2 POLICY ALERTS
AFFECTING 86 COMPONENTS

49 QUARANTINED COMPONENTS

FILTER: All Exact Unknown

VIOLATIONS: Summary All Quarantined Waived

Policy Threat ▾	*Component* ▴	Quarantined
Search Name	Search Coordinates	
	commons-collections : commons-collections : 3.2.1	

Component Info | Policy | Licenses | Vulnerabilities | Labels

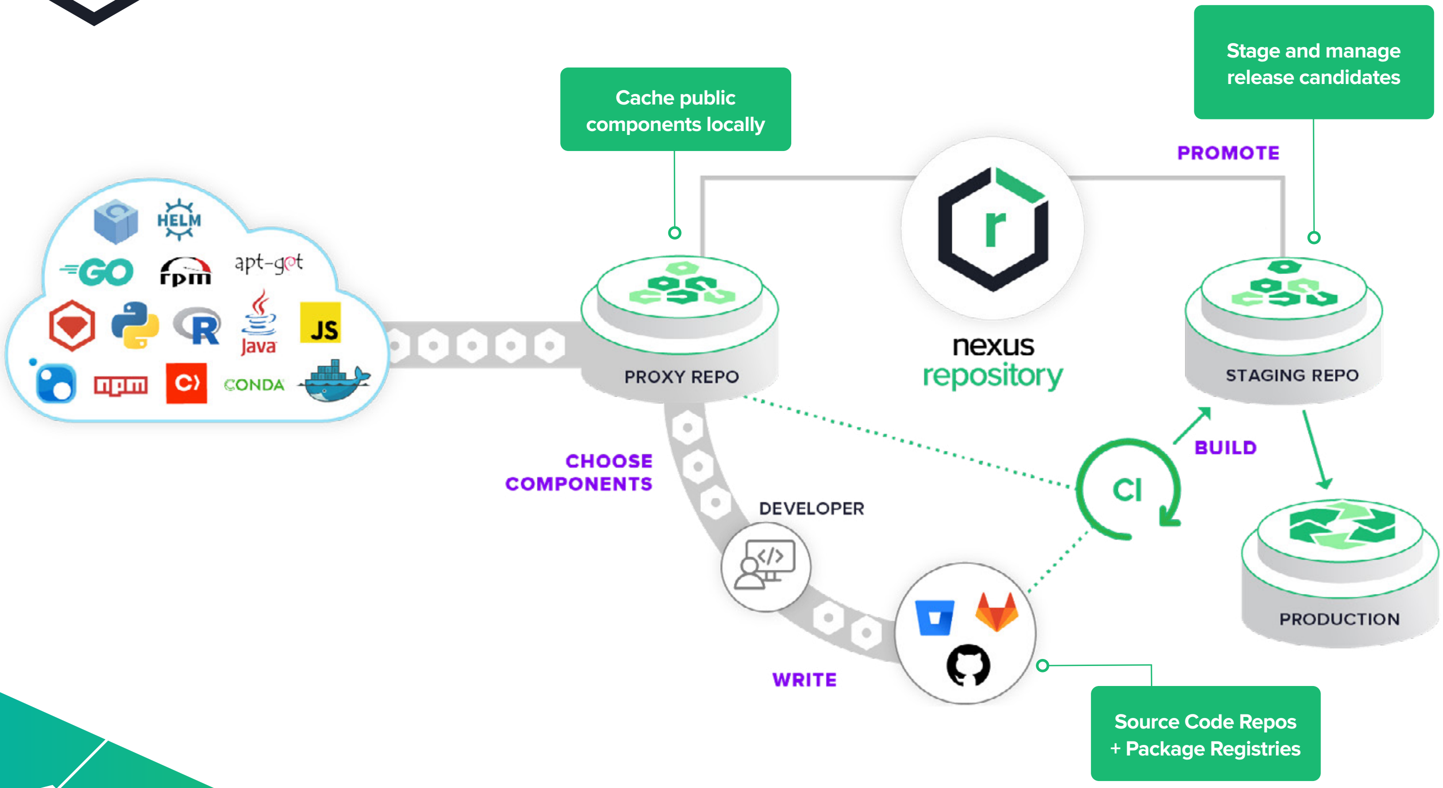
View Existing Waivers

Policy/*Action*	Constraint Name	Conditions	Waivers
Security-High	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with status 'Open', not 'Not Applicable'. ot find label 'custom vuln'.	Waive

Block, analyze, and selectively admit components.

Waive policy violations for component use when necessary.

nexus repository



> "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

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.

PREVENTION IS BETTER THAN A CURE

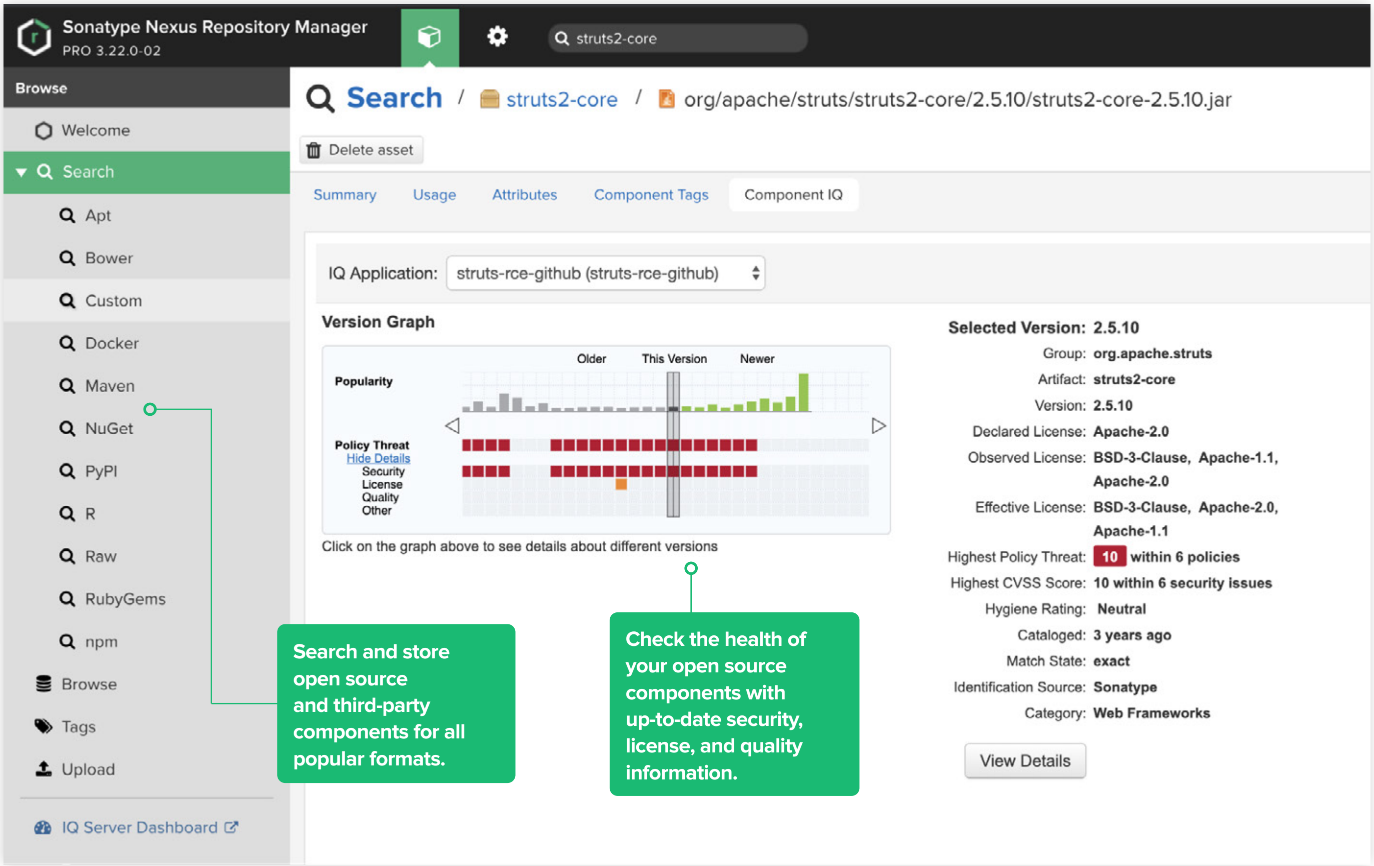
Maintain a trusted repository with Repository Health Check.

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



IQ Application: struts-rce-github (struts-rce-github)

Click on the graph above to see details about different versions

Selected Version:	2.5.10
Group:	org.apache.struts
Artifact:	struts2-core
Version:	2.5.10
Declared License:	Apache-2.0
Observed License:	BSD-3-Clause, Apache-1.1, Apache-2.0
Effective License:	BSD-3-Clause, Apache-2.0, Apache-1.1
Highest Policy Threat:	10 within 6 policies
Highest CVSS Score:	10 within 6 security issues
Hygiene Rating:	Neutral
Cataloged:	3 years ago
Match State:	exact
Identification Source:	Sonatype
Category:	Web Frameworks

Search and store open source and third-party components for all popular formats.

Check the health of your open source components with up-to-date security, license, and quality information.

nexus lifecycle

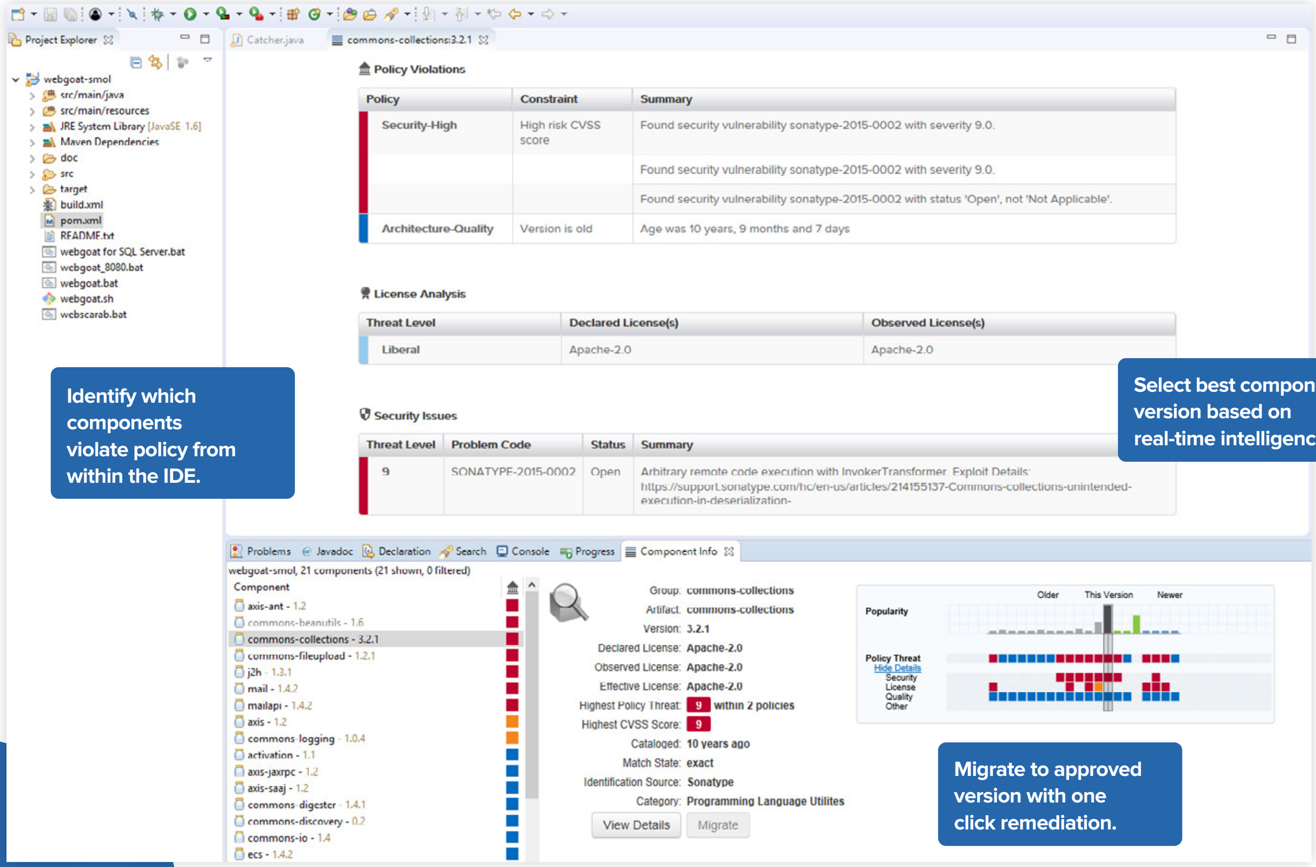
Precise intelligence for healthier component choice early in development.

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



Policy Violations

Policy	Constraint	Summary
Security-High	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with severity 9.0.
		Found security vulnerability sonatype-2015-0002 with status 'Open', not 'Not Applicable'.
Architecture-Quality	Version is old	Age was 10 years, 9 months and 7 days

License Analysis

Threat Level	Declared License(s)	Observed License(s)
Liberal	Apache-2.0	Apache-2.0

Security Issues

Threat Level	Problem Code	Status	Summary
9	SONATYPE-2015-0002	Open	Arbitrary remote code execution with InvokerTransformer. Exploit Details: https://support.sonatype.com/hc/en-us/articles/214155137-Commons-collections-unintended-execution-in-deserialization-

webgoat-smol, 21 components (21 shown, 0 filtered)

Component	
axis-ant - 1.2	🟥
commons-beanutils - 1.6	🟥
commons-collections - 3.2.1	🟥
commons-fileupload - 1.2.1	🟥
j2h - 1.3.1	🟥
mail - 1.4.2	🟥
mailapi - 1.4.2	🟥
axis - 1.2	🟧
commons-logging - 1.0.4	🟧
activation - 1.1	🟦
axis-jaxrpc - 1.2	🟦
axis-saaj - 1.2	🟦
commons-digester - 1.4.1	🟦
commons-discovery - 0.2	🟦
commons-io - 1.4	🟦
ecs - 1.4.2	🟦

Group: commons-collections
Artifact: commons-collections
Version: 3.2.1
Declared License: Apache-2.0
Observed License: Apache-2.0
Effective License: Apache-2.0
Highest Policy Threat: 9 within 2 policies
Highest CVSS Score: 9
Cataloged: 10 years ago
Match State: exact
Identification Source: Sonatype
Category: Programming Language Utilites

Identify which components violate policy from within the IDE.

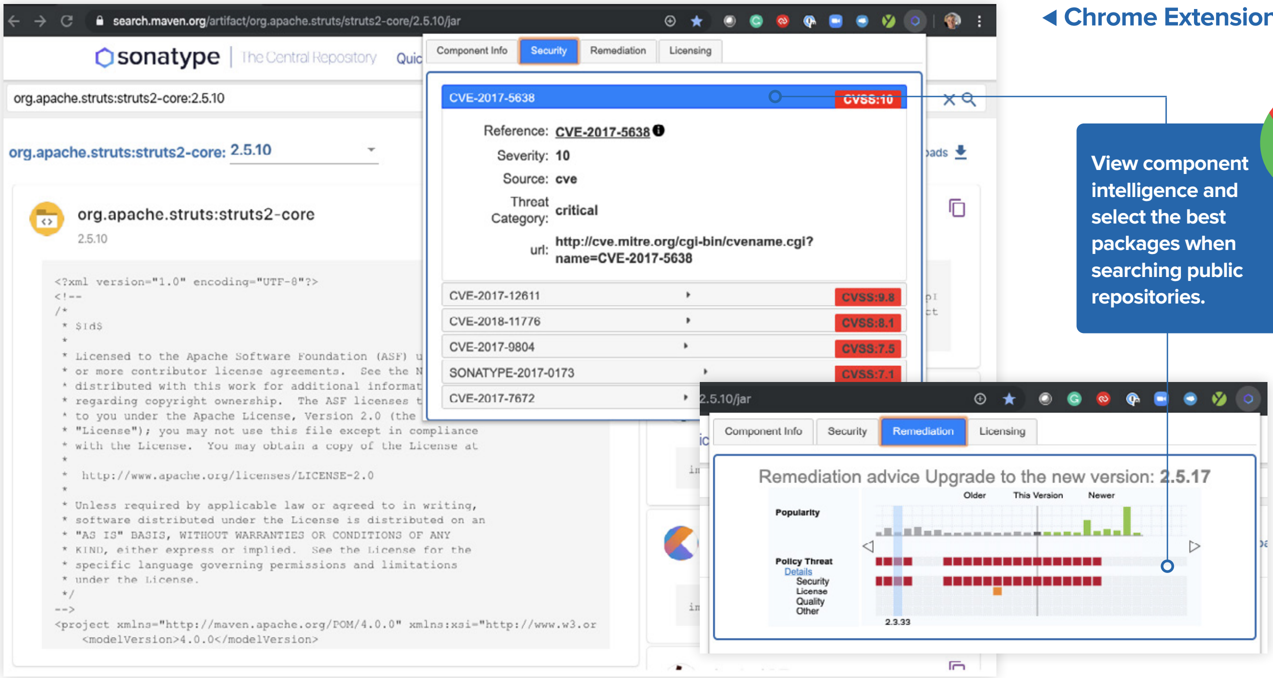
Select best component version based on real-time intelligence.

Migrate to approved version with one click remediation.

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



search.maven.org/artifact/org.apache.struts/struts2-core/2.5.10/jar

org.apache.struts:struts2-core:2.5.10

org.apache.struts:struts2-core: 2.5.10

org.apache.struts:struts2-core
2.5.10

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
/*
 * $Id$
 *
 * Licensed to the Apache Software Foundation (ASF) u
 * or more contributor license agreements.  See the N
 * distributed with this work for additional informat
 * regarding copyright ownership.  The ASF licenses t
 * to you under the Apache License, Version 2.0 (the
 * "License"); you may not use this file except in compliance
 * with the License.  You may obtain a copy of the License at
 *
 *  http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing,
 * software distributed under the License is distributed on an
 * "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
 * KIND, either express or implied.  See the License for the
 * specific language governing permissions and limitations
 * under the License.
 */
-->
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.or
    <modelVersion>4.0.0</modelVersion>
```

CVE-2017-5638 CVSS:10

Reference: CVE-2017-5638
Severity: 10
Source: cve
Threat Category: critical
url: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638

CVE-2017-12611	CVSS:9.8
CVE-2018-11776	CVSS:8.1
CVE-2017-9804	CVSS:7.5
SONATYPE-2017-0173	CVSS:7.1
CVE-2017-7672	

2.5.10/jar

Remediation advice Upgrade to the new version: 2.5.17

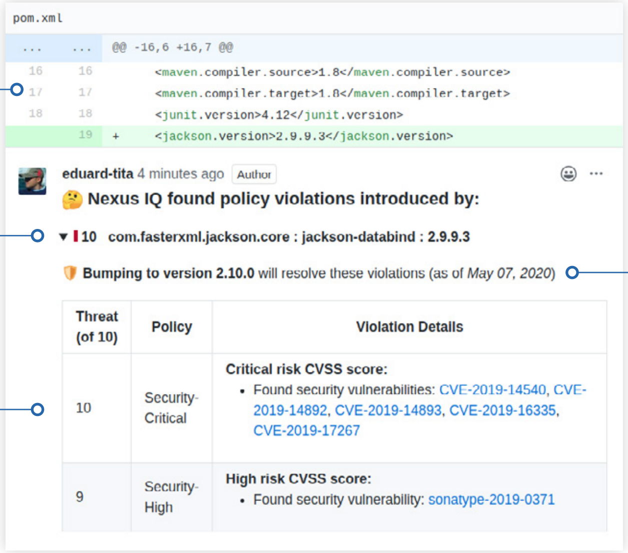
◀ **Chrome Extension**

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.



pom.xml

```
@@ -16,6 +16,7 @@
      <maven.compiler.source>1.8</maven.compiler.source>
      <maven.compiler.target>1.8</maven.compiler.target>
      <junit.version>4.12</junit.version>
+     <jackson.version>2.9.9.3</jackson.version>
```

eduard-tita 4 minutes ago Author

🤔 **Nexus IQ found policy violations introduced by:**

▼ ▌**10 com.fasterxml.jackson.core : jackson-databind : 2.9.9.3**

Bumping to version 2.10.0 will resolve these violations (as of *May 07, 2020*)

Threat (of 10)	Policy	Violation Details
10	Security-Critical	**Critical risk CVSS score:** • Found security vulnerabilities: CVE-2019-14540, CVE-2019-14892, CVE-2019-14893, CVE-2019-16335, CVE-2019-17267
9	Security-High	**High risk CVSS score:** • Found security vulnerability: sonatype-2019-0371

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*.

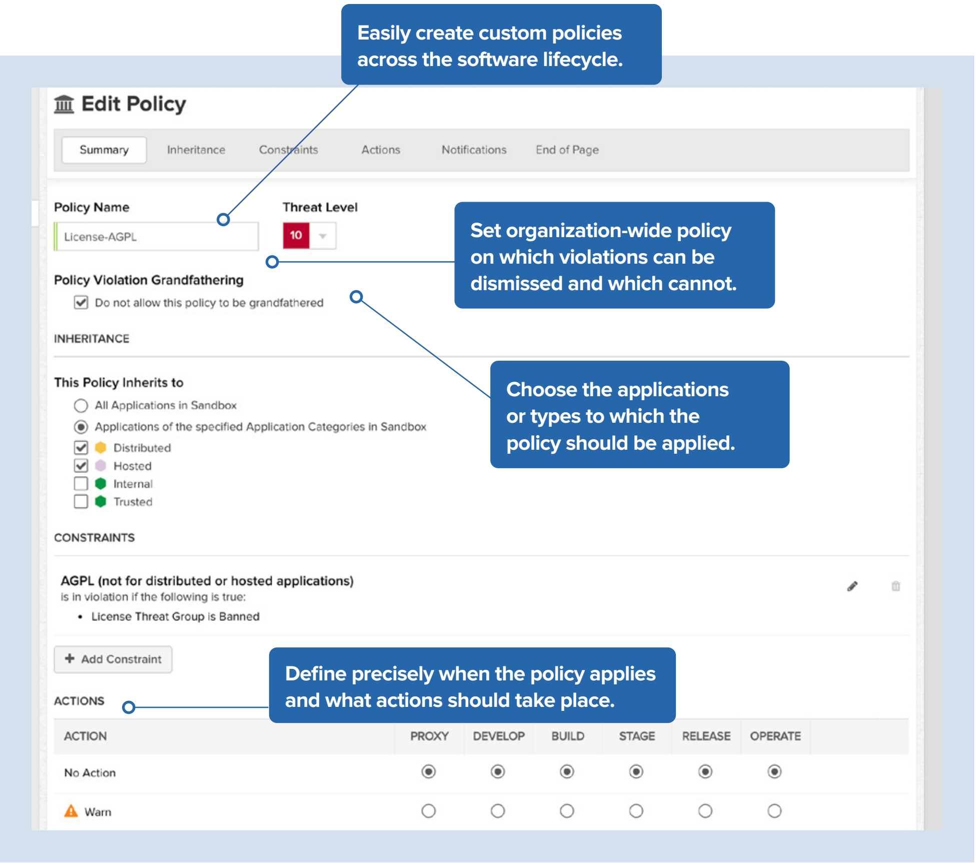
Ensure that policies are enforced as components are consumed across a variety of development tools.

Replace inefficient 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



Easily create custom policies across the software lifecycle.

Set organization-wide policy on which violations can be dismissed and which cannot.

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

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

Edit Policy

Policy Name: License-AGPL

Threat Level: 10

Policy Violation Grandfathering

☑ Do not allow this policy to be grandfathered

INHERITANCE

This Policy Inherits to

○ All Applications in Sandbox

● Applications of the specified Application Categories in Sandbox

☑ Distributed

☑ Hosted

☐ Internal

☐ Trusted

CONSTRAINTS

AGPL (not for distributed or hosted applications)
is in violation if the following is true:

- License Threat Group is Banned

ACTIONS

ACTION	PROXY	DEVELOP	BUILD	STAGE	RELEASE	OPERATE
No Action	●	●	●	●	●	●
⚠ Warn	○	○	○	○	○	○

nexus lifecycle

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

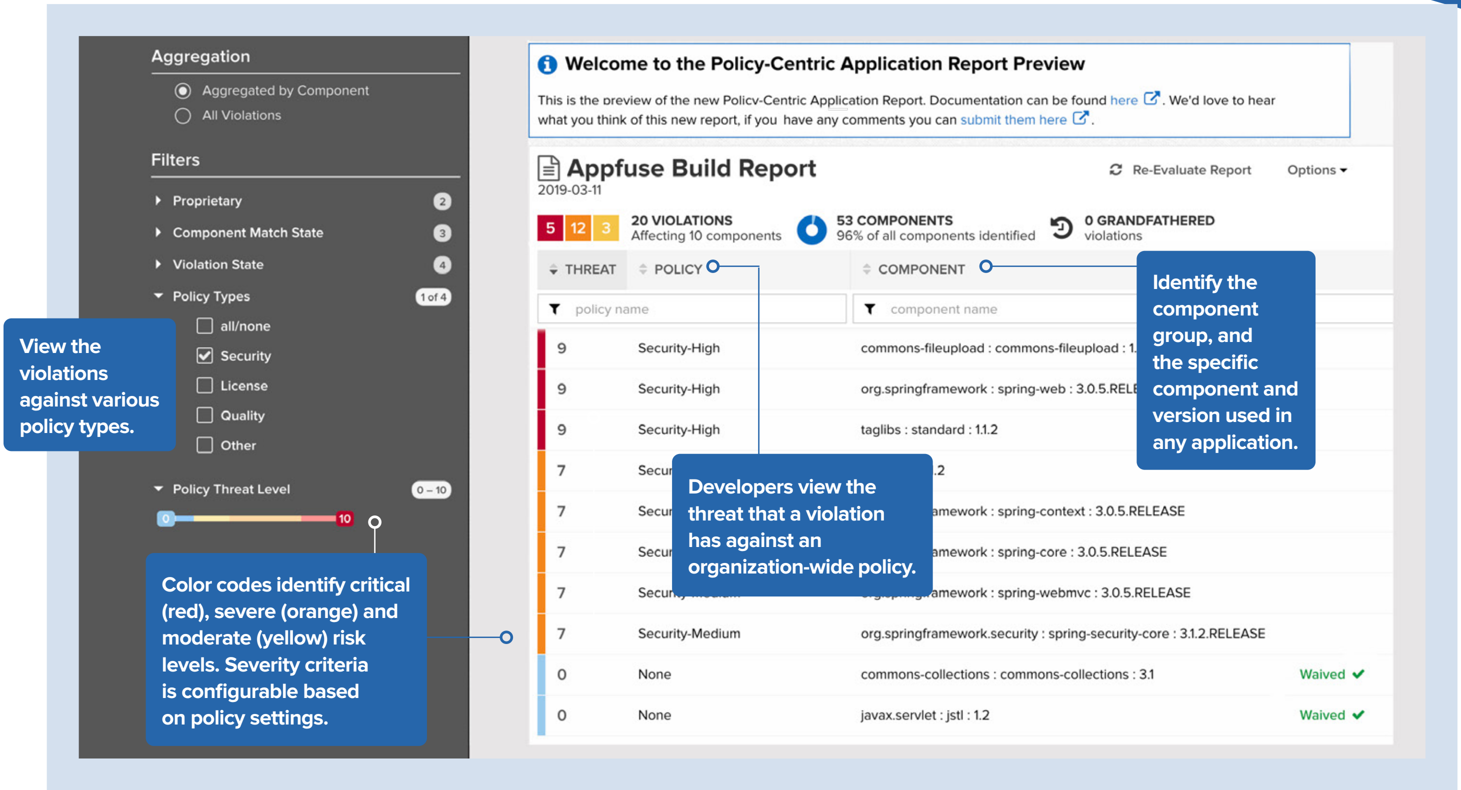
In just minutes, create an accurate software bill of materials for each application.

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



Aggregation

● Aggregated by Component
○ All Violations

Filters

- Proprietary 2
- Component Match State 3
- Violation State 4
- Policy Types 1 of 4
  - □ all/none
  - ☑ Security
  - □ License
  - □ Quality
  - □ Other
- Policy Threat Level 0 – 10

Welcome to the Policy-Centric Application Report Preview

This is the preview of the new Policy-Centric Application Report. Documentation can be found here. We'd love to hear what you think of this new report, if you have any comments you can submit them here.

Appfuse Build Report
2019-03-11

5 12 3 — 20 VIOLATIONS Affecting 10 components

53 COMPONENTS 96% of all components identified

0 GRANDFATHERED violations

THREAT	POLICY	COMPONENT	
	policy name	component name	
9	Security-High	commons-fileupload : commons-fileupload : 1.	
9	Security-High	org.springframework : spring-web : 3.0.5.RELE	
9	Security-High	taglibs : standard : 1.1.2	
7	Secur	.2	
7	Secur	amework : spring-context : 3.0.5.RELEASE	
7	Secur	amework : spring-core : 3.0.5.RELEASE	
7	Secur	amework : spring-webmvc : 3.0.5.RELEASE	
7	Security-Medium	org.springframework.security : spring-security-core : 3.1.2.RELEASE	
0	None	commons-collections : commons-collections : 3.1	Waived ✓
0	None	javax.servlet : jstl : 1.2	Waived ✓

View the violations against various policy types.

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

Developers view the threat that a violation has against an organization-wide policy.

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

> **“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

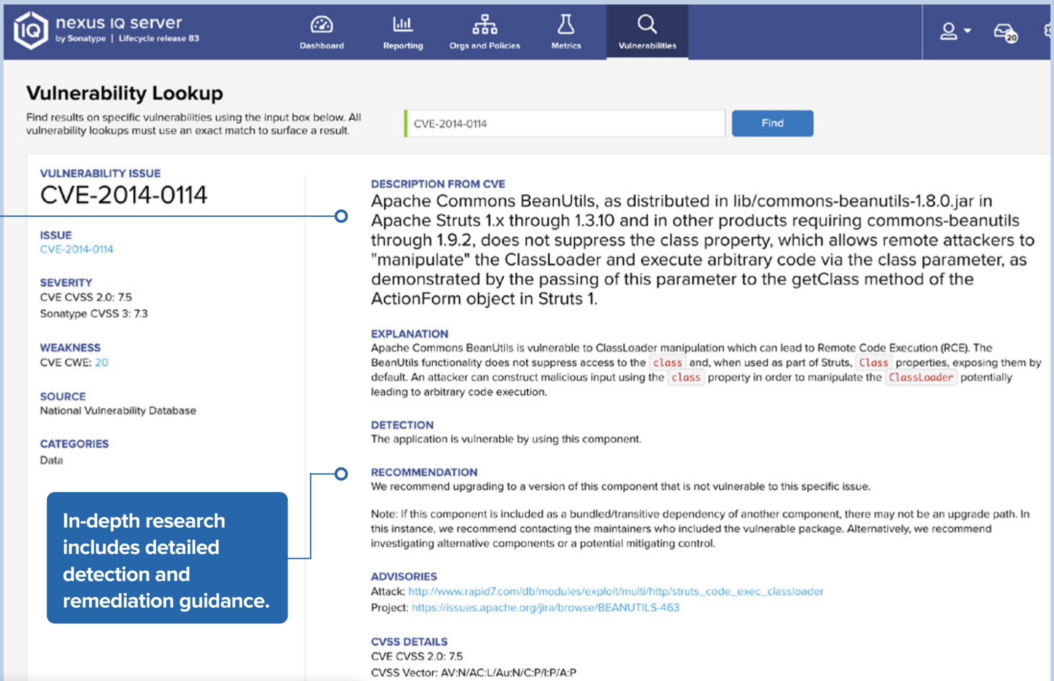
Get visibility and transparency for quick remediation.

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.



Vulnerability Lookup

Find results on specific vulnerabilities using the input box below. All vulnerability lookups must use an exact match to surface a result.

CVE-2014-0114 [Find]

VULNERABILITY ISSUE
CVE-2014-0114

ISSUE
CVE-2014-0114

SEVERITY
CVE CVSS 2.0: 7.5
Sonatype CVSS 3: 7.3

WEAKNESS
CVE CWE: 20

SOURCE
National Vulnerability Database

CATEGORIES
Data

DESCRIPTION FROM CVE
Apache Commons BeanUtils, as distributed in lib/commons-beanutils-1.8.0.jar in Apache Struts 1.x through 1.3.10 and in other products requiring commons-beanutils through 1.9.2, does not suppress the class property, which allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via the class parameter, as demonstrated by the passing of this parameter to the getClass method of the ActionForm object in Struts 1.

EXPLANATION
Apache Commons BeanUtils is vulnerable to ClassLoader manipulation which can lead to Remote Code Execution (RCE). The BeanUtils functionality does not suppress access to the `class` and, when used as part of Struts, `Class` properties, exposing them by default. An attacker can construct malicious input using the `class` property in order to manipulate the `ClassLoader` potentially leading to arbitrary code execution.

DETECTION
The application is vulnerable by using this component.

RECOMMENDATION
We recommend upgrading to a version of this component that is not vulnerable to this specific issue.

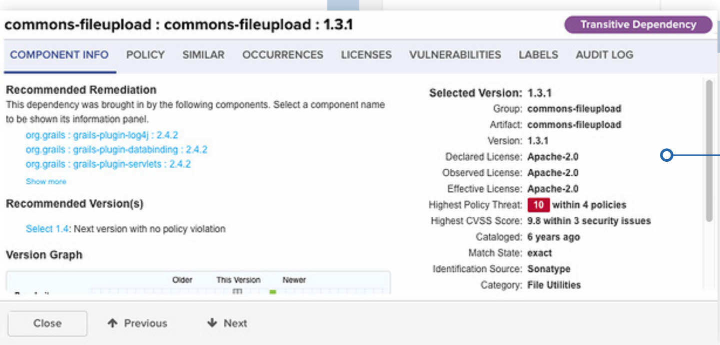
Note: If this component is included as a bundled/transitive dependency of another component, there may not be an upgrade path. In this instance, we recommend contacting the maintainers who included the vulnerable package. Alternatively, we recommend investigating alternative components or a potential mitigating control.

ADVISORIES
Attack: http://www.rapid7.com/db/modules/exploit/multi/http/struts_code_exec_classloader
Project: https://issues.apache.org/jira/browse/BEANUTILS-463

CVSS DETAILS
CVE CVSS 2.0: 7.5
CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Easy to understand description written for developers by developers.

In-depth research includes detailed detection and remediation guidance.



commons-fileupload : commons-fileupload : 1.3.1

Recommended Remediation

This dependency was brought in by the following components. Select a component name to be shown its information panel.

org.grails : grails-plugin-log4j : 2.4.2
org.grails : grails-plugin-databinding : 2.4.2
org.grails : grails-plugin-servlets : 2.4.2
Show more

Recommended Version(s)

Select 1.4: Next version with no policy violation

Version Graph

Selected Version: 1.3.1
Group: commons-fileupload
Artifact: commons-fileupload
Version: 1.3.1
Declared License: Apache-2.0
Observed License: Apache-2.0
Effective License: Apache-2.0
Highest Policy Threat: 10 within 4 policies
Highest CVSS Score: 9.8 within 3 security issues
Cataloged: 6 years ago
Match State: exact
Identification Source: Sonatype
Category: File Utilities

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

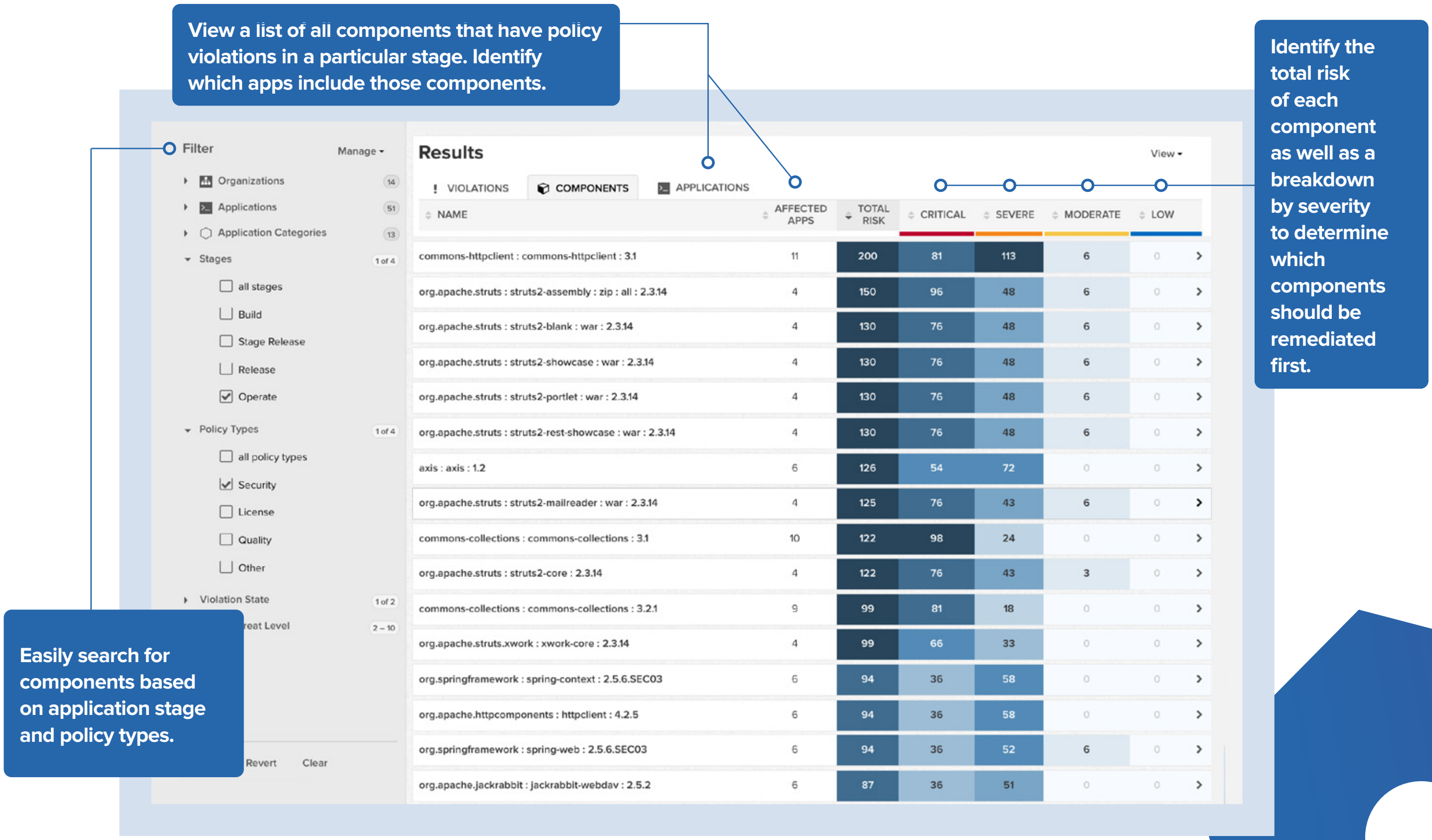
Continuously monitor for new defects.

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.



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.

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient : commons-httpclient : 3.1	11	200	81	113	6	0
org.apache.struts : struts2-assembly : zip : all : 2.3.14	4	150	96	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	130	76	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	98	24	0	0
org.apache.struts : struts2-core : 2.3.14	4	122	76	43	3	0
commons-collections : commons-collections : 3.2.1	9	99	81	18	0	0
org.apache.struts.xwork : xwork-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

nexus lifecycle

Identify and fix container vulnerabilities.

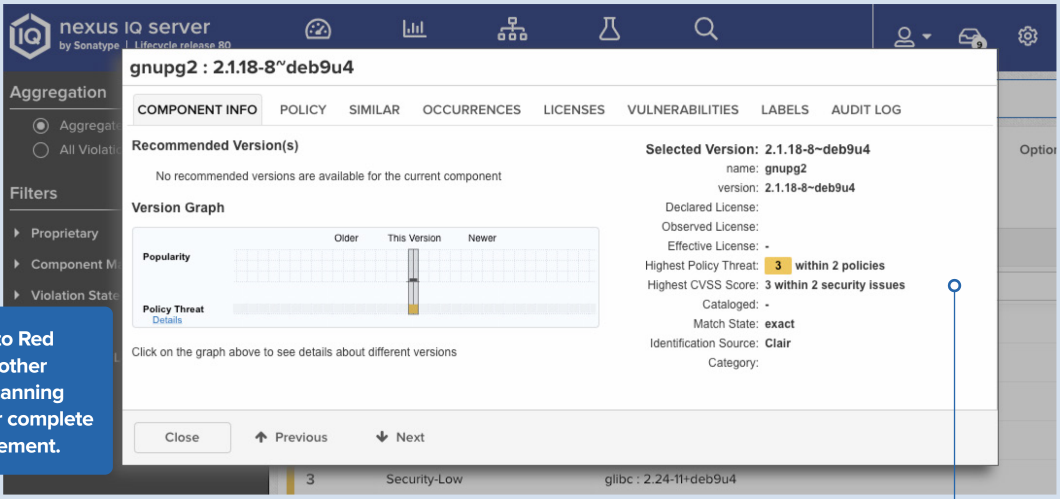
View open source risk at all layers (runtime, operating system, and application levels).

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 ▶



gnupg2 : 2.1.18-8~deb9u4

COMPONENT INFO | POLICY | SIMILAR | OCCURRENCES | LICENSES | VULNERABILITIES | LABELS | AUDIT LOG

Recommended Version(s)

No recommended versions are available for the current component

Version Graph

Older | This Version | Newer

Popularity

Policy Threat
Details

Click on the graph above to see details about different versions

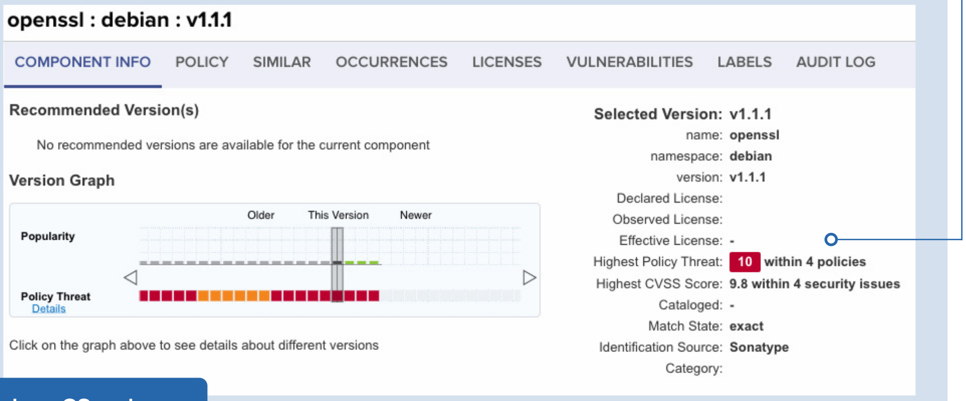
Selected Version: 2.1.18-8~deb9u4
name: gnupg2
version: 2.1.18-8~deb9u4
Declared License:
Observed License:
Effective License: -
Highest Policy Threat: 3 within 2 policies
Highest CVSS Score: 3 within 2 security issues
Cataloged: -
Match State: exact
Identification Source: Clair
Category:

Close | ↑ Previous | ↓ Next

3 Security-Low glibc : 2.24-11+deb9u4

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.



openssl : debian : v1.1.1

COMPONENT INFO | POLICY | SIMILAR | OCCURRENCES | LICENSES | VULNERABILITIES | LABELS | AUDIT LOG

Recommended Version(s)

No recommended versions are available for the current component

Version Graph

Older | This Version | Newer

Popularity

Policy Threat
Details

Click on the graph above to see details about different versions

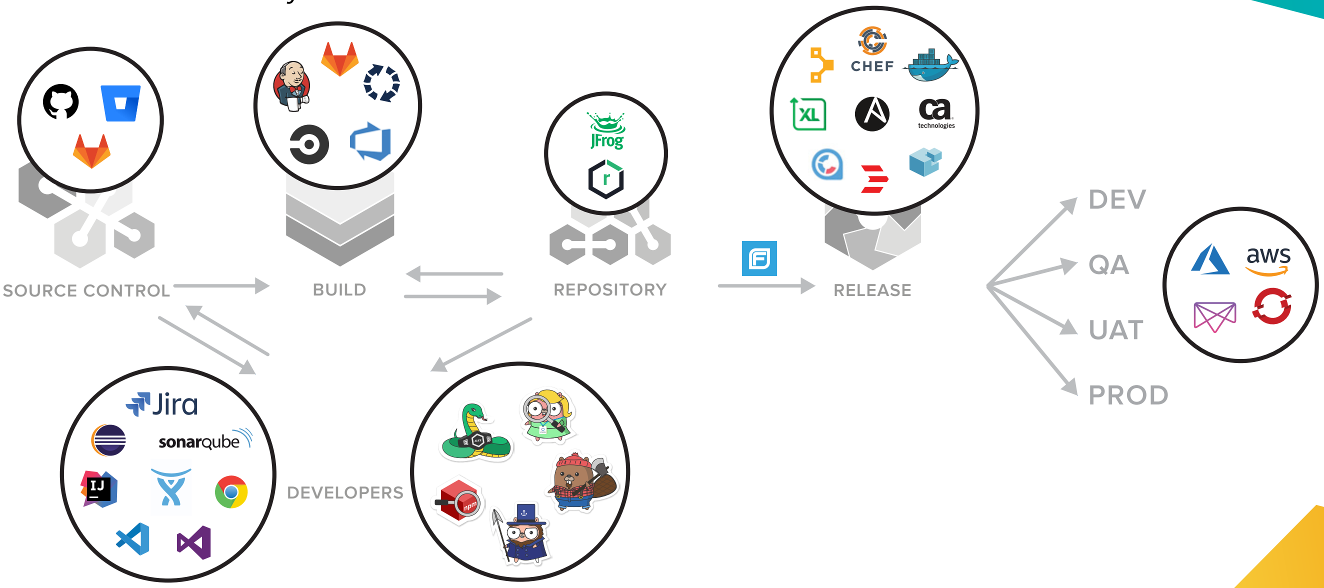
Selected Version: v1.1.1
name: openssl
namespace: debian
version: v1.1.1
Declared License:
Observed License:
Effective License: -
Highest Policy Threat: 10 within 4 policies
Highest CVSS Score: 9.8 within 4 security issues
Cataloged: -
Match State: exact
Identification Source: Sonatype
Category:

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