



# Accelerate Innovation with Automated Security

Sonatype eBook



carahsoft.

For more information, contact Carahsoft or our reseller partners:  
[Sonatype@carahsoft.com](mailto:Sonatype@carahsoft.com) | 877-742-8468



# Accelerate Innovation with Automated Security

Full-Spectrum Software Supply Chain Automation



# 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:

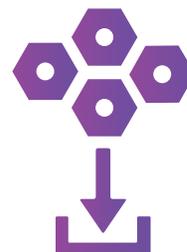
- ▶ Open source components are not created equal. Some are vulnerable from the start, while others go bad over time.
- ▶ Usage has become more complex. With tens of billions of downloads, it's increasingly difficult to manage libraries and direct dependencies.
- ▶ Transitive dependencies: if you are 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 automated dependency management  
and open source governance policies.**



of the components in most modern applications are open source.

**2.2 trillion**  
open source download  
requests of Java, npm, PyPI,  
and RubyGems in 2021.



**373,000+**  
average enterprise  
downloads of OSS  
components per year

## DevSecOps: Why is open source policy critical?

As the number of next-gen attacks continue to rise, DevOps organizations are making investments to better protect themselves. These organizations are taking steps to integrate and automate security across the development life cycle to build quality into their software.

According to the *2021 State of Software Supply Chain*:



**Only 25%**  
of utilized components  
are updated actively



YoY cyber-attacks  
aimed at open source  
suppliers increased by  
**650%**



Intelligent automation  
could save companies  
**\$192,000**  
per year



**29%**  
of popular projects  
contain known  
vulnerabilities

# Accelerate software supply chain security early, everywhere, at scale with the Nexus Platform.



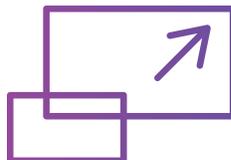
## Early

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**

“Nexus [Lifecycle] helps identify things that could be exploited...**the level of intelligence that we’re able to get from them is well ‘above and beyond’ anything we had before**, which has been helpful to paint a picture of actual 3rd party risks to people outside of security (i.e. the C-suite).”

—SENIOR SECURITY ARCHITECT

DRIVING ROI, THE CASE FOR  
A PROVEN SCA PLATFORM,  
HOBSON & COMPANY REPORT

## 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.**

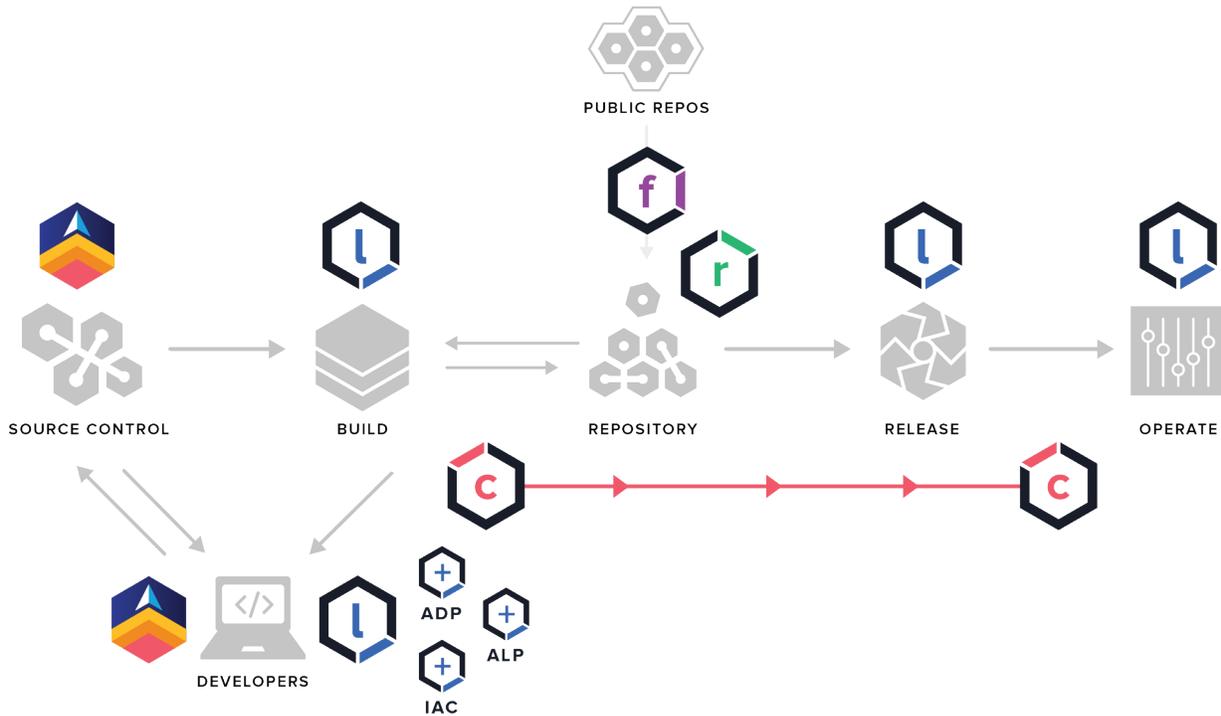
Through both automation and careful human curation, Nexus Intelligence is designed to give you results you can count on, saving you an average of \$14,000 in time per developer per year.

### **When it comes to security, speed matters.**

We implement a 12-hour fast track for critical and time-sensitive vulnerabilities. You’ll experience a **30% reduction in probability** of a breach and **90% reduction** in developer time spent researching, securing approval of and downloading quality OSS components when using the Nexus Platform.

# Full Spectrum Software Supply Chain Automation

Sonatype is the leader in developer-friendly, full-spectrum software supply chain management providing organizations total control of their cloud-native development lifecycles, including third-party open source code, first-party source code, infrastructure as code, and containerized code.



## nexus lifecycle

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

## nexus firewall

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

## nexus repository

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

## nexus container

Identify and remediate OSS risk in containers for build and run-time protection

## sonatype lift

Find and fix critical security, performance, reliability, and style issues in developer code.

“We’ve increased time to market by 20% in areas that are using Nexus, which management is really happy about.”

—SR. MANAGER, CI/CD

“By getting software into the company and into production without issues, we are better able to support the company earnings; **Nexus Lifecycle** has helped us increase the quality and predictability of our SDLC, increasing our business agility by 40%.”

—IT ARCHITECT

# Driving ROI with a Proven Platform

The value of a validated OSS governance and management solution is immediate and demonstrable.

ROI findings and attributes listed below are based on an organization with \$30 million in annual revenue realizing significant financial benefits from an investment in Sonatype's Nexus Platform:



## Developers

**400 developers** who each spend **1 hour per week** researching, securing approval for and searching/downloading quality OSS components and **1 hour per week** on remediation and rework.

## Application Security Teams

Application Security teams that spend a total of **80 hours per month** on OSS governance and management (including reviewing and approving OSS components) and 20 hours reviewing each of their application releases (assuming 24 releases per year).



“Customers interviewed reported **90% reduction in developer time** spent researching, securing approval of, and downloading quality OSS components.”

—DRIVING ROI, THE CASE FOR A PROVEN SCA PLATFORM, HOBSON & COMPANY REPORT

“Customers reported a **75% reduction** in time spent identifying locations of, and remediating, newly discovered vulnerable components.”

—DRIVING ROI, THE CASE FOR A PROVEN SCA PLATFORM, HOBSON & COMPANY REPORT

## PROVEN ROI

The typical organization, with an initial investment of \$250,000 generates a positive return in 2.7 months and a 3-year ROI of 635%.

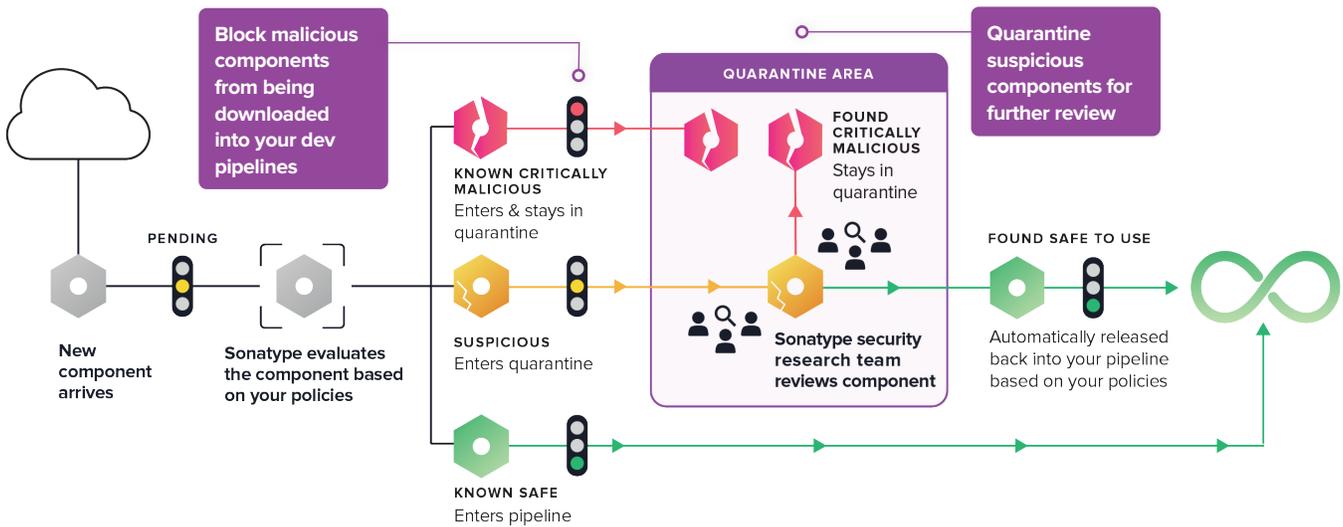
**Annual benefits exceed \$2,155,000.**





# YOUR FIRST LINE OF DEFENSE AGAINST MODERN SOFTWARE SUPPLY CHAIN ATTACKS.

Automatically detect and prevent malicious cyber attacks.



**You are protected** Firewall is currently monitoring 300 components in 1 repositories

Quarantine Status: Active on 1 of 1 repositories

Auto Release from Quarantine Status: Active releasing 3 of 5 policy condition types

Quarantine: 230 components in quarantine

Auto Released from Quarantine: 70 components released month-to-month

THREAT	POLICY NAME	QUARANTINE DATE	COMPONENT	REPOSITORY
10	Security-Critical	2021-05-10	com.pojosontheweb:woko-blobs-web:war:2.2-beta7	test-repo
10	Security-Critical	2021-05-10	org.mule.examples:mule-example-errorhandler:zip:3.4-M1	test-repo
10	Security-Critical	2021-05-10	org.atmosphere.samples:atmosphere-twitter-live-feed:war:0.8.2	test-repo
10	Security-Critical	2021-05-10	smartrics.restfature:smartrics-Restfature:zip:bin:4.0	test-repo

COMPONENT	QUARANTINE DATE	REPOSITORY	DATE CLEARED
org.apache.directory.studio:ldap.servers.apacheds.v154:jar:sources:2.0.0.v20120111	2021-05-10	test-repo	2021-05-10
org.glassfish.grizzly:grizzly-http:2.1	2021-05-10	test-repo	2021-05-10
org.ow2.jonas.autostart:jonas-full-starter:jar:full-starter:1.0.0-M2	2021-05-10	test-repo	2021-05-10
org.apache.portals.bridges:perl:war:1.0.4	2021-05-10	test-repo	2021-05-10
com.sun.grizzly:grizzly-http-websvr:1.9.18-o	2021-05-10	test-repo	2021-05-10
com.sun.faces:jsp-api:2.0.4-b11	2021-05-10	test-repo	2021-05-10

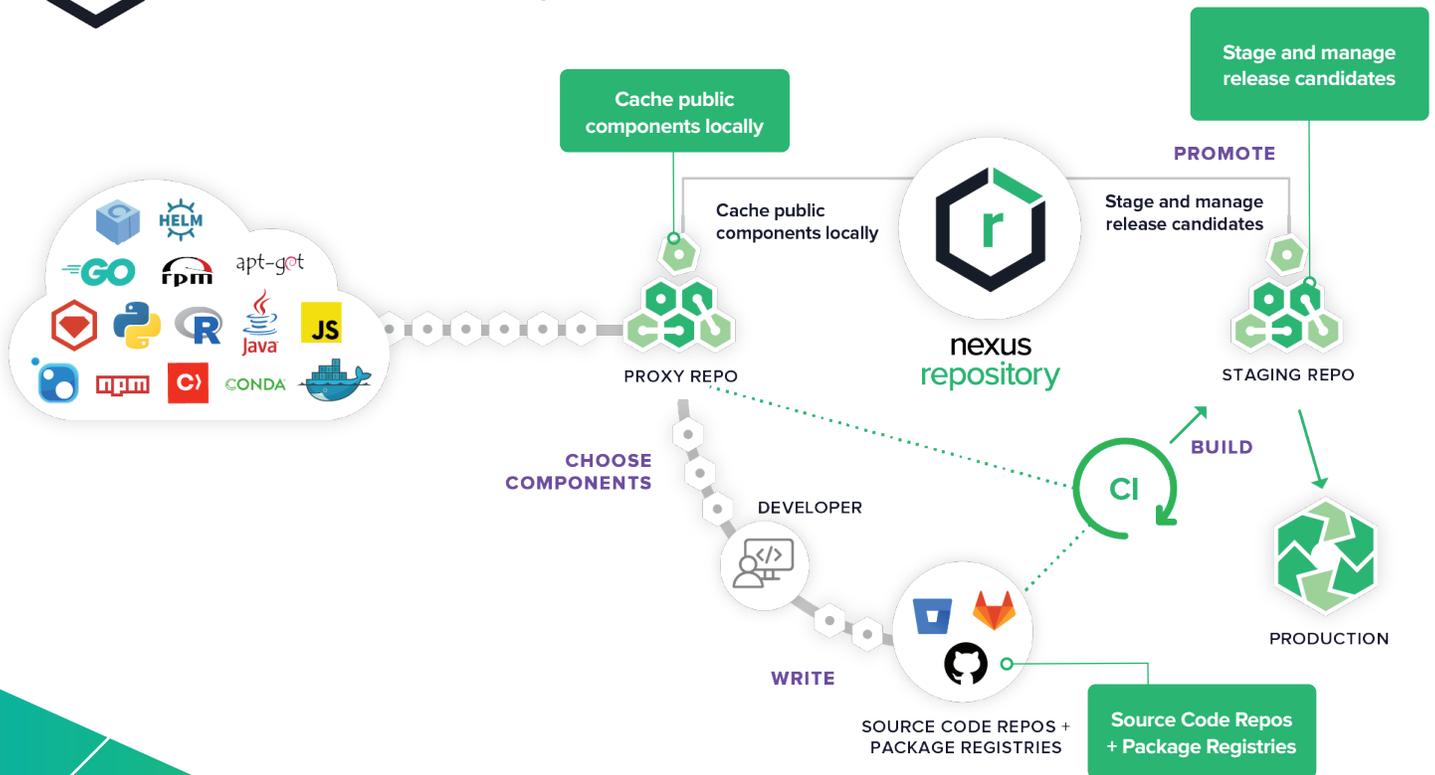
## Perimeter Control for All Software Supply Chains



Better together: Protect your Nexus Repository(Pro) with Firewall.



Using Artifactory? No problem. Nexus Firewall supports JFrog's Artifactory.



## A CENTRAL SOURCE OF CONTROL

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

“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



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.

## REPOSITORY COMPONENT INTELLIGENCE

# 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

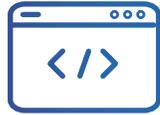
The screenshot displays the Sonatype Nexus Repository Manager interface. The top navigation bar includes the Sonatype logo, version PRO 3.35.0, and search results for 'struts2'. The main content area shows search results for 'struts2-core' with a path to a specific version: '/org/apache/struts/struts2-core/2.5.10/struts2-core-2.5.10.jer'. Below the search bar, there are tabs for 'Summary', 'Usage', 'Attributes', 'Component Tags', and 'Component IQ'. The 'Summary' tab is active, showing a 'Version Graph' and a 'Selected Version' section. The 'Version Graph' displays a bar chart of popularity and a table of policy threats, security, license, and quality for different versions. The 'Selected Version' section provides detailed information for version 2.5.10, including type, group, artifact, version, declared and observed licenses, effective license, highest policy threat (10 within 9 policies), highest CVSS score (10 within 9 security issues), integrity rating (Not Applicable), cataloged date (4 years ago), match state (exact), identification source (Sonatype), and category (Web Frameworks). A 'View Details' button is located at the bottom of the selected version section. Two green callout boxes are overlaid on the screenshot: one pointing to the search bar with the text 'Search and store open source and third-party components for all popular formats.' and another pointing to the version graph with the text 'Check the health of your open source components with up-to-date security, license, and quality information.'



# 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

**Identify which components violate policy from within the IDE.**

**Select best component version based on real-time intelligence.**

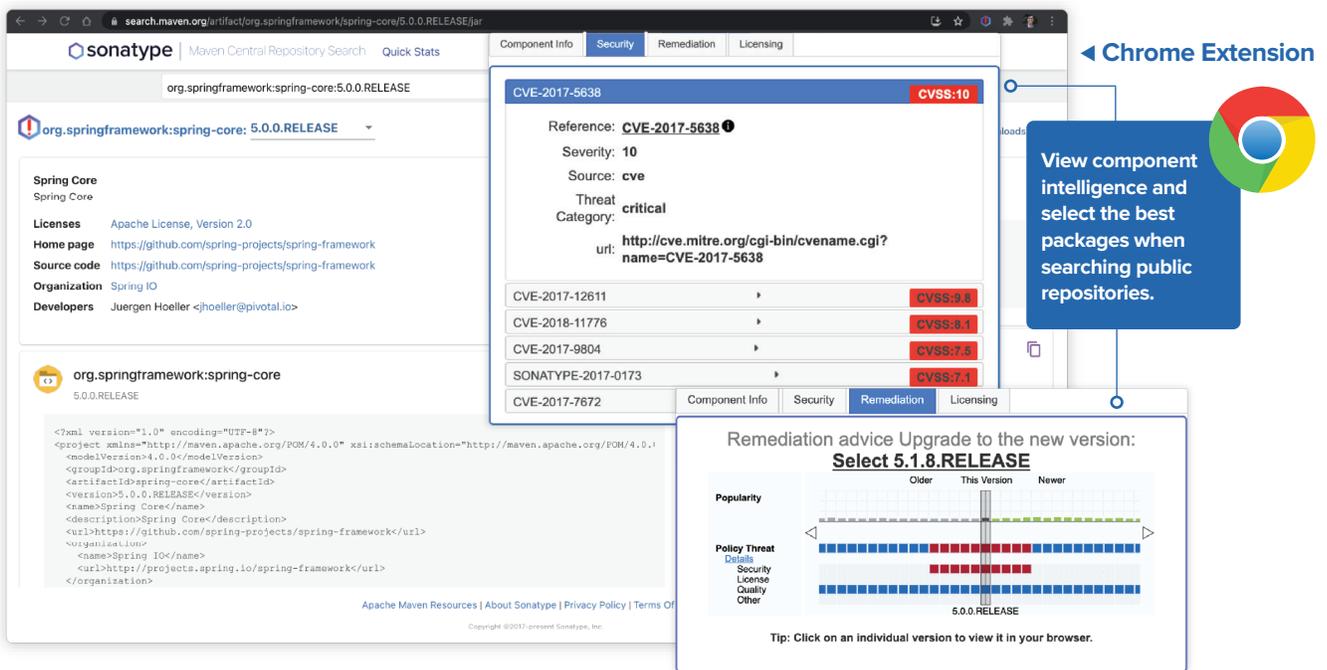
**Migrate to approved version with one click remediation.**

**Summary: log4j-core - 2.7**  
 Recommended Version(s)  
 Select 2.13.2: Next version with no policy violation  
 Select 2.13.3: Next version with no policy violations for this component and its dependencies

**Selected Version: 2.7**  
 Type: maven  
 Group: org.apache.logging.log4j  
 Artifact: log4j-core  
 Version: 2.7  
 Declared License: Apache-2.0  
 Observed License: Apache-2.0  
 Effective License: Apache-2.0  
 Highest Policy Threat: 10 within 3 policies  
 Highest CVSS Score: 9.8 within 2 security issues  
 Integrity Rating: Not Applicable  
 Cataloged: 5 years ago  
 Match State: exact  
 Identification Source: Sonatype  
 Category: Logging  
 Website: [link]

# 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.

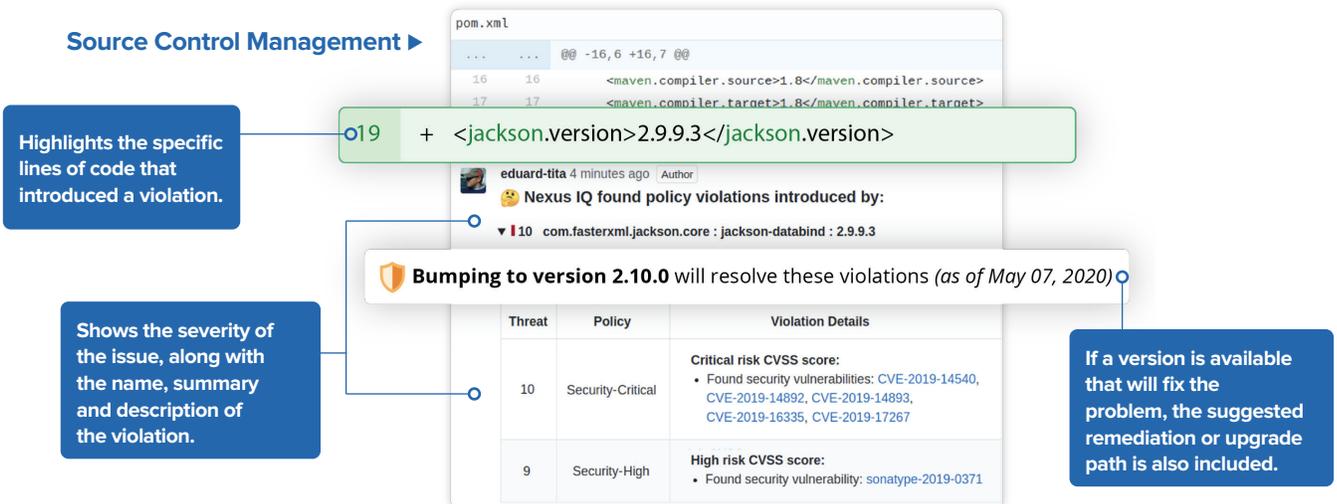
**Remediation advice Upgrade to the new version: Select 5.1.8.RELEASE**

Popularity: Older | This Version | Newer

Policy Threat Details: Security, License, Quality, Other

Tip: Click on an individual version to view it in your browser.

## Source Control Management



Highlights the specific lines of code that introduced a violation.

```

pom.xml
...
16 16 <maven.compiler.source>1.8</maven.compiler.source>
17 17 <maven.compiler.target>1.8</maven.compiler.target>
+ <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	Policy	Violation Details
10	Security-Critical	<b>Critical risk CVSS score:</b> • Found security vulnerabilities: CVE-2019-14540, CVE-2019-14892, CVE-2019-14893, CVE-2019-16335, CVE-2019-17267
9	Security-High	<b>High risk CVSS score:</b> • Found security vulnerability: sonatype-2019-0371

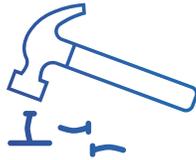
Shows the severity of the issue, along with the name, summary and description of the violation.

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

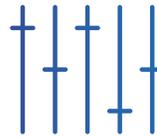
# Analyze and enforce policies *automatically*.



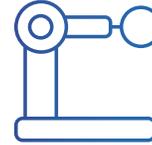
Ensure that policies are enforced as components are consumed across a variety of development tools.



Replace inefficient workflows and the burden of manual reviews.



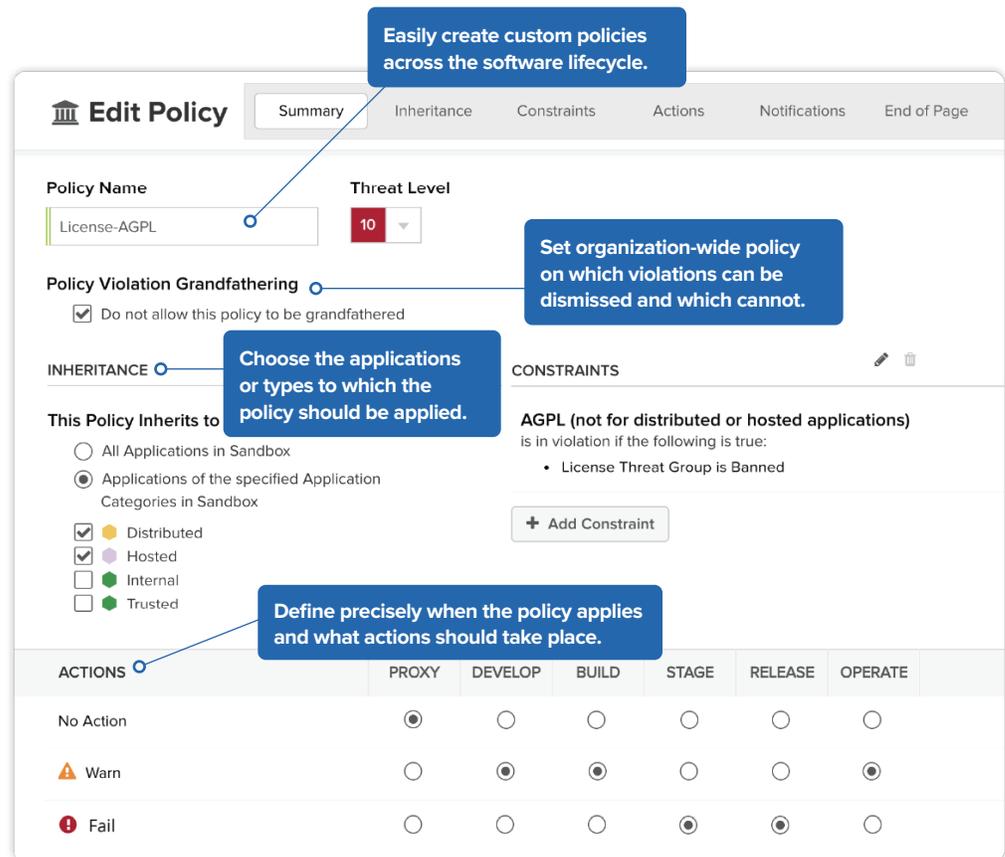
Customize policies to meet specific compliance goals or mandates OR use our default policies to gain an immediate view of security, license, and quality risk.



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.**

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

- License Threat Group is Banned

ACTIONS	PROXY	DEVELOP	BUILD	STAGE	RELEASE	OPERATE
No Action	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Warn	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Fail	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>



# 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

**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.**

THREAT	POLICY	COMPONENT
10	Security-Critical	com.fasterxml:jackson.core : jackson-databind : 2.6.1
10	Security-Critical	com.thoughtworks:xstream : xstream : 1.4.8
10	Security-Critical	commons-collections : commons-collections : 3.2.1
10	Security-Critical	commons-fileupload : commons-fileupload : 1.3.2
10	Security-Critical	org.apache.struts : struts2-core : 2.5.10
10	Security-Critical	org.richfaces : richfaces-core : 4.5.17.Final
10	Security-Critical	org.springframework : spring-core : 4.1.6.RELEASE
10	Security-Critical	com.fasterxml:jackson.core : jackson-core : 2.6.1
10	Security-Critical	com.itextpdf : itextpdf : 5.5.6
10	Security-Critical	commons-beanutils : commons-beanutils : 1.9.2

“Nexus Lifecycle gives us visibility into types of vulnerabilities that we didn’t have before, including specific information about how the vulnerability is exploited and if we’re vulnerable based on how we used it. The product also informs us which application or team it belongs to. The ease of research and identifying a remediation path has saved our developers 2-4 hours per Vulnerability.”

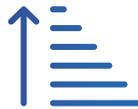
—DEVOPS MANAGER,  
DRIVING ROI, THE CASE FOR  
A PROVEN SCA PLATFORM,  
HOBSON & COMPANY REPORT



## Get visibility and transparency for quick remediation.



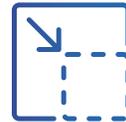
One dashboard easily filtered to support development, operations, security, and compliance.



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.

# Continuously monitor for new defects.

“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



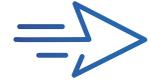
An automated early warning system to identify newly discovered defects.



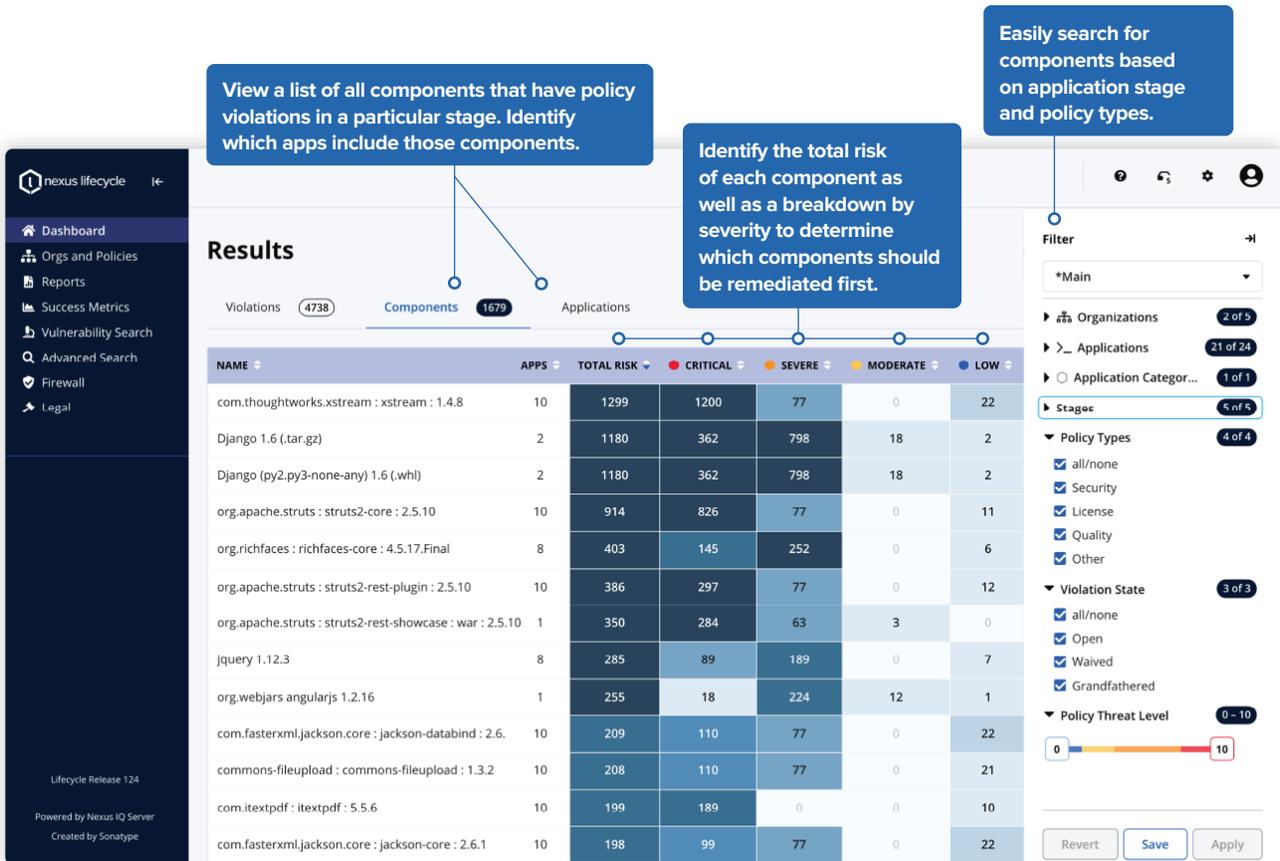
Detailed intelligence on vulnerabilities including precise root cause and component dependencies.



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.**

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

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

NAME	APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
com.thoughtworks.xstream : xstream : 1.4.8	10	1299	1200	77	0	22
Django 1.6 (.tar.gz)	2	1180	362	798	18	2
Django (py2.py3-none-any) 1.6 (.whl)	2	1180	362	798	18	2
org.apache.struts : struts2-core : 2.5.10	10	914	826	77	0	11
org.richfaces : richfaces-core : 4.5.17.Final	8	403	145	252	0	6
org.apache.struts : struts2-rest-plugin : 2.5.10	10	386	297	77	0	12
org.apache.struts : struts2-rest-showcase : war : 2.5.10	1	350	284	63	3	0
jquery 1.12.3	8	285	89	189	0	7
org.webjars angularajs 1.2.16	1	255	18	224	12	1
com.fasterxml.jackson.core : jackson-databind : 2.6	10	209	110	77	0	22
commons-fileupload : commons-fileupload : 1.3.2	10	208	110	77	0	21
com.itextpdf : itextpdf : 5.5.6	10	199	189	0	0	10
com.fasterxml.jackson.core : jackson-core : 2.6.1	10	198	99	77	0	22



# Identify and fix container vulnerabilities.

Nexus Lifecycle scans the application layer of your containers, and provides precise component intelligence for Java, JavaScript, NuGet, Python, etc.

Nexus Lifecycle leverages Nexus Container intelligence to directly provide information about your images and registries back in the same familiar Lifecycle report, alongside other application vulnerabilities and evaluation results



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

### test-app Develop Report

Triggered by CLI on 2021-07-06 18:31:01 UTC-0600 — Commit 1c72a4b3ec2505439e7aaade1ddbc927bfaba89f

51 60 4 115 VIOLATIONS Affecting 62 components 604 COMPONENTS 100% of all components identified 0 GRANDFATHERED violations

THREAT	POLICY	COMPONENT
10	Security-Critical	file : rhel:8.1 : 5.33-16.el8_3.1
10	Security-Critical	file-libs : rhel:8.4 : 5.33-16.el8_3.1
10	Security-Critical	gnutls : rhel:8.4 : 3.6.14-8.el8_3
10	Security-Critical	

#### maven-openjdk8 : rhel:8.4 : 1:3.6.2-6.module+el8.4.0+9250+1786af37

COMPONENT INFO POLICY SIMILAR OCCURRENCES LICENSES VULNERABILITIES LABELS AUDIT LOG

**Recommended Version(s)**  
No recommended versions are available for the current component

**Selected Version:** 1:3.6.2-6.module+el8.4.0+9250+1786af37

Type: container  
name: maven-openjdk8  
namespace: rhel:8.4  
version: 1:3.6.2-6.module+el8.4.0+9250+1786af37

Declared License: Not Provided  
Observed License: Not Provided  
Effective License: Not Provided

Highest Policy Threat: 10  
Highest CVSS Score: 9.1  
CaidlogId: -  
Match State: exact  
Identification Source: Sonatype-Container  
Category: Other

Get detailed remediation guidance and take action with a robust policy engine to set custom policies, apply waivers, and break builds.

View all application and container vulnerability information in one location.

## ADVANCED LEGAL PACK

Automate legal compliance and eliminate regulatory risk



Automated attribution reports (or third party notices). Save, customize, and edit reports as needed.



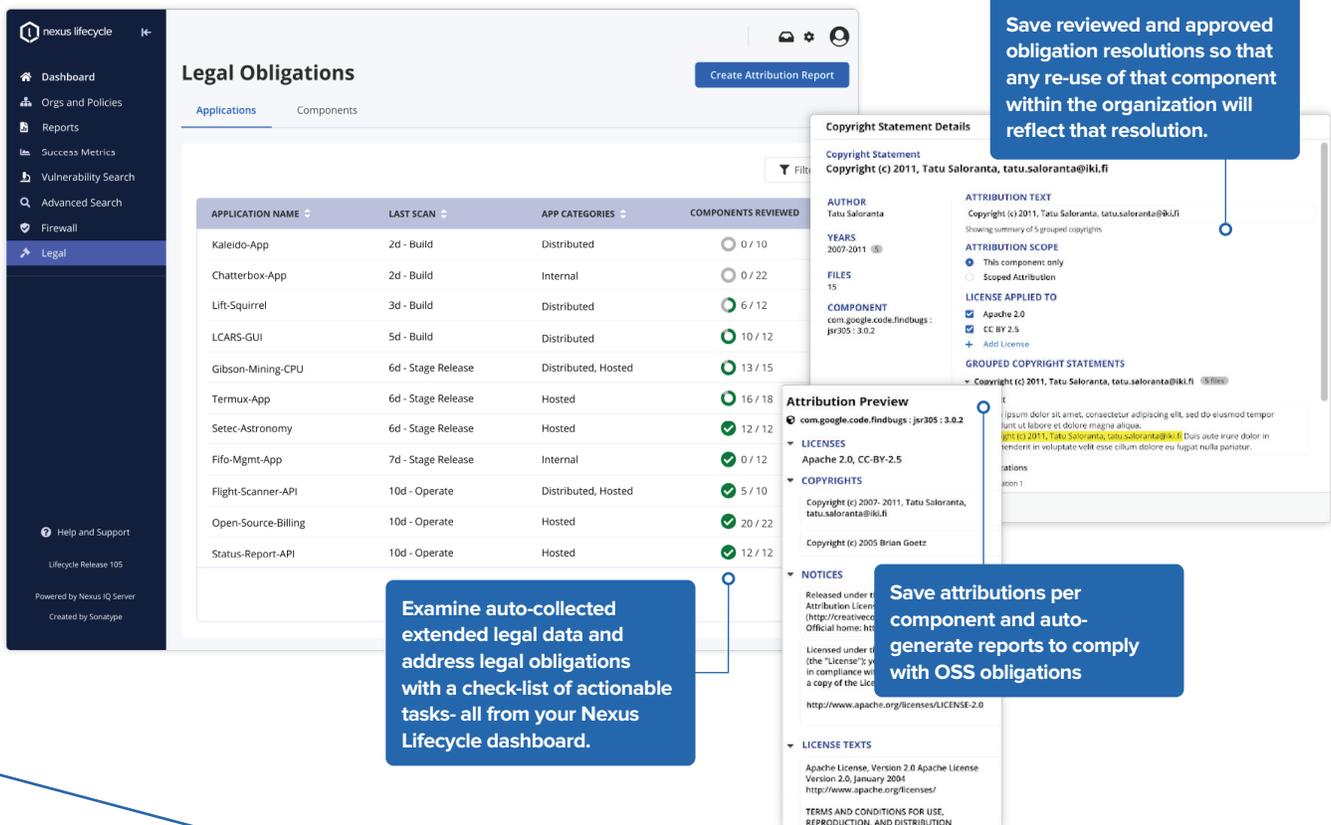
Provides an easy way to click through and resolve obligation issues for automated compliance workflows.



Our machine learning algorithms and natural language processing detect legal data, with additional insights on how to best comply with an obligation.



Easily look up licenses, read through obligations, view annotated license texts, and export lists with our License Obligation Review Tool (LORT).



**Save reviewed and approved obligation resolutions so that any re-use of that component within the organization will reflect that resolution.**

APPLICATION NAME	LAST SCAN	APP CATEGORIES	COMPONENTS REVIEWED
Kaleido-App	2d - Build	Distributed	0 / 10
Chatterbox-App	2d - Build	Internal	0 / 22
Lift-Squirrel	3d - Build	Distributed	6 / 12
LCARS-GUI	5d - Build	Distributed	10 / 12
Gibson-Mining-CPU	6d - Stage Release	Distributed, Hosted	13 / 15
Termux-App	6d - Stage Release	Hosted	16 / 18
Setec-Astronomy	6d - Stage Release	Hosted	12 / 12
Fifo-Mgmt-App	7d - Stage Release	Internal	0 / 12
Flight-Scanner-API	10d - Operate	Distributed, Hosted	5 / 10
Open-Source-Billing	10d - Operate	Hosted	20 / 22
Status-Report-API	10d - Operate	Hosted	12 / 12

**Examine auto-collected extended legal data and address legal obligations with a check-list of actionable tasks- all from your Nexus Lifecycle dashboard.**

**Save attributions per component and auto-generate reports to comply with OSS obligations**

**Copyright Statement Details**  
 Copyright Statement  
 Copyright (c) 2011, Tatu Saloranta, tatu.saloranta@iki.fi

**Attribution Preview**  
 com.google.code.findbugs: jsr305: 3.0.2

**LICENSES**  
 Apache 2.0, CC-BY-2.5

**COPYRIGHTS**  
 Copyright (c) 2007- 2011, Tatu Saloranta, tatu.saloranta@iki.fi  
 Copyright (c) 2005 Brian Goetz

**NOTICES**  
 Released under the Attribution License (http://creativecommons.org/licenses/by/2.0/)  
 Licensed under the "License"; you must comply with the terms in a copy of the license at http://www.apache.org/licenses/LICENSE-2.0

**LICENSE TEXTS**  
 Apache License, Version 2.0 Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

**TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION**



## INFRASTRUCTURE AS CODE PACK

Secure what you build and where you run it.



See infrastructure violations in the Nexus Lifecycle report alongside open source vulnerabilities.



Deep insights into the severity and root cause of cloud infrastructure misconfigurations.



Get remediation guidance to fix violations by leveraging new cloud infrastructure and compliance data, and pinpointing specific compliance issues.



Built on the most comprehensive set of rules and compliance mappings, with out-of-the-box support for multiple security benchmarks.

**Security-High** High risk CVSS score  
Build failed

**CONDITIONS**

- Found security vulnerability F-R00035 with severity >= 7
- Found security vulnerability F-R00035 with severity > 9

**Release Report**

131 0 16 147 VIOLATIONS Affecting 55 components 59 COMPONENTS 78% of all components identified 0 GRANDFATHERED Violations

THREAT	POLICY	COMPONENT
10	Security-Critical	aws_cloudtrail.foo: aws.large.tfplan : current
10	Security-Critical	aws_db_instance.example : aws.large.tfplan : current
10	Security-Critical	aws_s3_bucket.bucket : aws.large.tfplan : current
10	Security-Critical	aws_s3_bucket.cf-bucket : aws.large.tfplan : current
10	Security-Critical	aws_s3_bucket.config_example : aws.large.tfplan : current
10	Security-Critical	aws_s3_bucket.hoge : aws.large.tfplan : current
10	Security-Critical	aws_s3_bucket.inventory : aws.large.tfplan : current

10 Security-Critical aws\_db\_instance : aws.large.tfplan : current

9 Security-High com.fasterxml.jackson.core : jackson-core : 2.0.4

Deep insights into severity and root cause with remediation guidance on specific compliance rules impacted.

View infrastructure violations alongside all of your open source vulnerabilities in Nexus Lifecycle

# Protect containers from build to production.

Full life cycle vulnerability (CVE) & compliance scanning — during build, registry scans, and run-time. Manage container and application-level risk with admission controls to stop vulnerabilities from entering your SDLC, policy management to guide and enforce actions, and detailed remediation guidance



Real-time vulnerability scanning during run-time for hosts and orchestration platforms, such as Kubernetes.



Monitor live containers for suspicious process and file system activity and privilege escalation detection, with host process blocking.



Continuously monitor running containers to prevent insider attacks which bypass network L3/L4 protections and safeguard sensitive data, PII, credit cards etc., with the only container DLP engine.

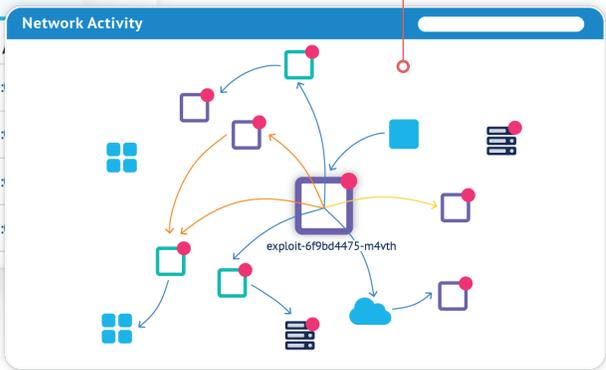
Containers AUTO SCAN REFRESH

NAME	NODE	APP...	STATE	SCAN STATUS	HIGH	SCANNED AT
iodine-client	gke-nv-sonatype-de...	HTTP	Monitor	Finished	392	Feb 25, 2021

Pid	Command	User	Status	Action	Started
37170	/usr/bin/python3 -u /sbin/my_init	! root	Sleeping	Allow	Feb 10 12:
37197	/usr/bin/runsvdir -P /etc/service	! root	Sleeping	Allow	Feb 10 12:
37198	runsv syslog-forwarder	! root	Sleeping	Allow	Feb 10 12:
37206	tail -f -n 0 /var/log/syslog	! root	Sleeping	Allow	Feb 10 12:

Automatically inspect and learn all network traffic at Layer 7 including visualization of containers, connections, violations, threats — in real-time.



Prevent vulnerable & non-compliant images from deploying with automated compliance testing as well as templates for: GDPR, PCI, HIPAA, and NIST.



Integrated with orchestration and management platforms



# Find critical bugs in your code, with the click of a button.

Lift provides developers feedback the same way their teammates do — as comments in code review. The issues you need to care about, right where you want to see them, and at the moment you can most easily fix them.



24+ code analyzer integrations that go beyond traditional linting to perform deep code analysis to catch critical performance and reliability issues.



Lift finds security vulnerabilities in both your third-party open-source code and first-party source code.



Lift is pre-tuned to eliminate false positives and uses machine learning to measure which bugs developers fix most — delivering more accurate results over time.



Simple to install on cloud repos or with Kubernetes and OpenShift, with 2-5x faster scan results. Both SaaS and self-hosted options work with any business or deployment model.

Catch code quality issues early in the dev pipeline to enhance SAST scans during final security reviews.

Analyze each pull request to find and fix security, performance, reliability, and style issues where they are 70x more likely to get fixed by developers.

```
...Demo/src/main/java/com/mapbox/mapboxandroiddemo/examples/javaservices/MatrixApiActivity.java Outdated
135 + if (pointOfSelectedStation != null) {
136 + String selectedBoltFeatureName = renderedStationFeatures.get(0).getStringProperty(STA
137 + List<Feature> featureList = featureCollection.features();
138 + for (int i = 0; i < featureList.size(); i++) {

lift-bot bot on Oct 5, 2019
NULL_DEREFERENCE: object featureList last assigned on line 137 could be null and is dereferenced at line 138.

langsmith force-pushed the lu-matrixapi-refactor branch from 4be4ff9 to 044102a on Oct 5, 2019
lift-bot bot reviewed on Oct 5, 2019
...Demo/src/main/java/com/mapbox/mapboxandroiddemo/examples/javaservices/MatrixApiActivity.java Outdated
135 + if (pointOfSelectedStation != null) {
136 + String selectedBoltFeatureName = renderedStationFeatures.get(0).getStringProperty(STA
137 + List<Feature> featureList = featureCollection.features();
138 + for (int i = 0; i < featureList.size(); i++) {

lift-bot bot on Oct 5, 2019
NULL_DEREFERENCE: object featureList last assigned on line 137 could be null and is dereferenced at line 138.

solr/core/src/java/org/apache/solr/core/SolrCores.java Outdated
112 - transientSolrCoreCache.close();
113 - }
114 + // Release transient core cache.
115 + getTransientCacheHandler().close();

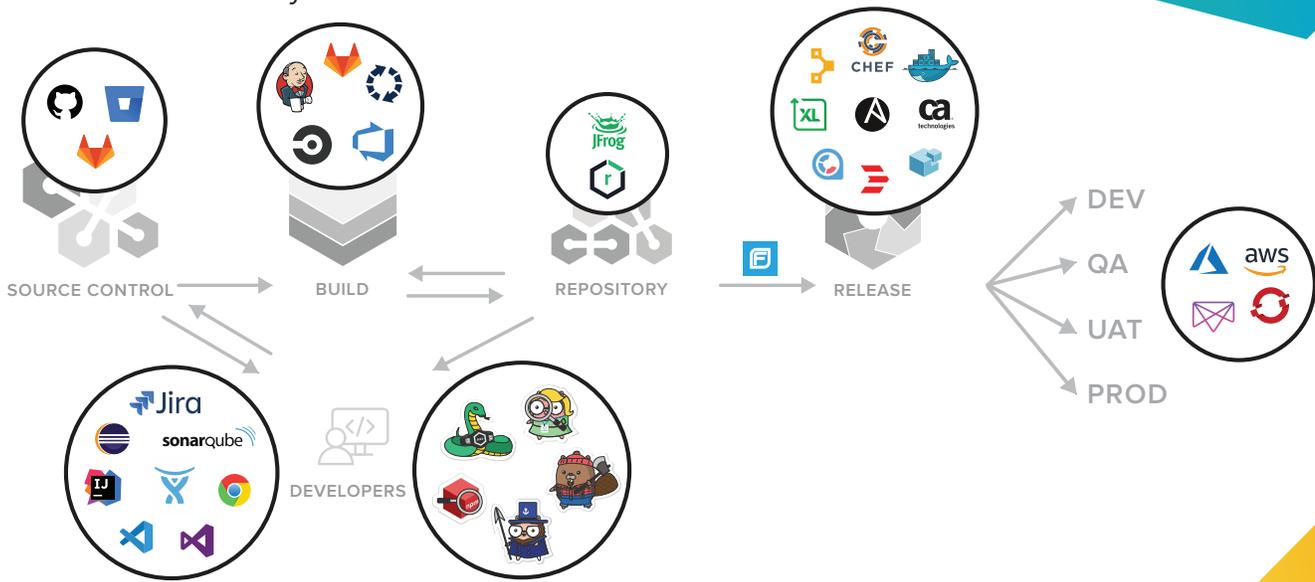
lift-bot bot on Nov 9, 2020
THREAD_SAFETY_VIOLATION: Read/Write race. Non-private method SolrCores.close() indirectly reads without synchronization from this.transientSolrCoreCacheFactory. Potentially races with write in method SolrCores.load(...). Reporting because this access may occur on a background thread.

eddie on Nov 9, 2020 Contributor
@kalle lift-bot makes a good point; there should be a synchronized (modifyLock) around grabbing getTransientCacheHandler and calling close on it.

kalle on Nov 9, 2020 Author Contributor
+1 thanks lift-bot!
```

# Integrations? You better believe it.

We work where you work.



## Shift Left with High Performance.

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.](https://www.sonatype.com/appscan)

[sonatype.com/get-nexus](https://sonatype.com/get-nexus)

**GET STARTED TODAY!**



Sonatype is the leader in developer-friendly, full-spectrum software supply chain management providing organizations total control of their cloud-native development life cycles, including third-party open source code, first-party source code, infrastructure as code, and containerized code. The company supports 70% of the Fortune 100 and its commercial and open source tools are trusted by 15 million developers around the world. With a vision to transform the way the world innovates, Sonatype helps organizations of all sizes build higher quality software that's more aligned with business needs, more maintainable, and more secure.

Sonatype has been recognized by Fast Company as one of the Best Workplaces for Innovators in the world, two years in a row and has been named to the Deloitte Technology Fast 500 and Inc. 5000 list for the past five years. For more information, please visit [Sonatype.com](https://www.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 6HU  
United Kingdom

### APAC Office

60 Martin Place  
Level 1  
Sydney, NSW 2000  
Australia

### Sonatype Inc.

[www.sonatype.com](https://www.sonatype.com)  
Sonatype Copyright 2020  
All Rights Reserved.



Thank you for downloading this Sonatype eBook! Carahsoft serves as the Master Government Aggregator and Distributor for Sonatype, offering expertise in government procurement processes and practices with purchasing available via GSA, SEWP V, The Quilt and other contract vehicles.

To learn how to take the next step toward acquiring Sonatype solutions, please check out the following resources and information:



For additional resources:  
[carah.io/SonatypeResources](https://carah.io/SonatypeResources)



For upcoming events:  
[carah.io/SonatypeEvents](https://carah.io/SonatypeEvents)



For additional solutions:  
[carah.io/SonatypeProducts](https://carah.io/SonatypeProducts)



For additional Open Source solutions:  
[carah.io/OpenSourceSolutions](https://carah.io/OpenSourceSolutions)



To set up a meeting:  
[Sonatype@Carahsoft.com](mailto:Sonatype@Carahsoft.com)  
(877)-742-8468



To purchase, check out the contract vehicles available for procurement:  
[carah.io/SonatypeContracts](https://carah.io/SonatypeContracts)