sonatype

Brian Beard
bbeard@sonatype.com

Today’s innovative agencies build and release great software faster and more securely than their adversaries.

sonatype

The way we build software has changed forever. Which is mostly a good thing **(but not entirely).**

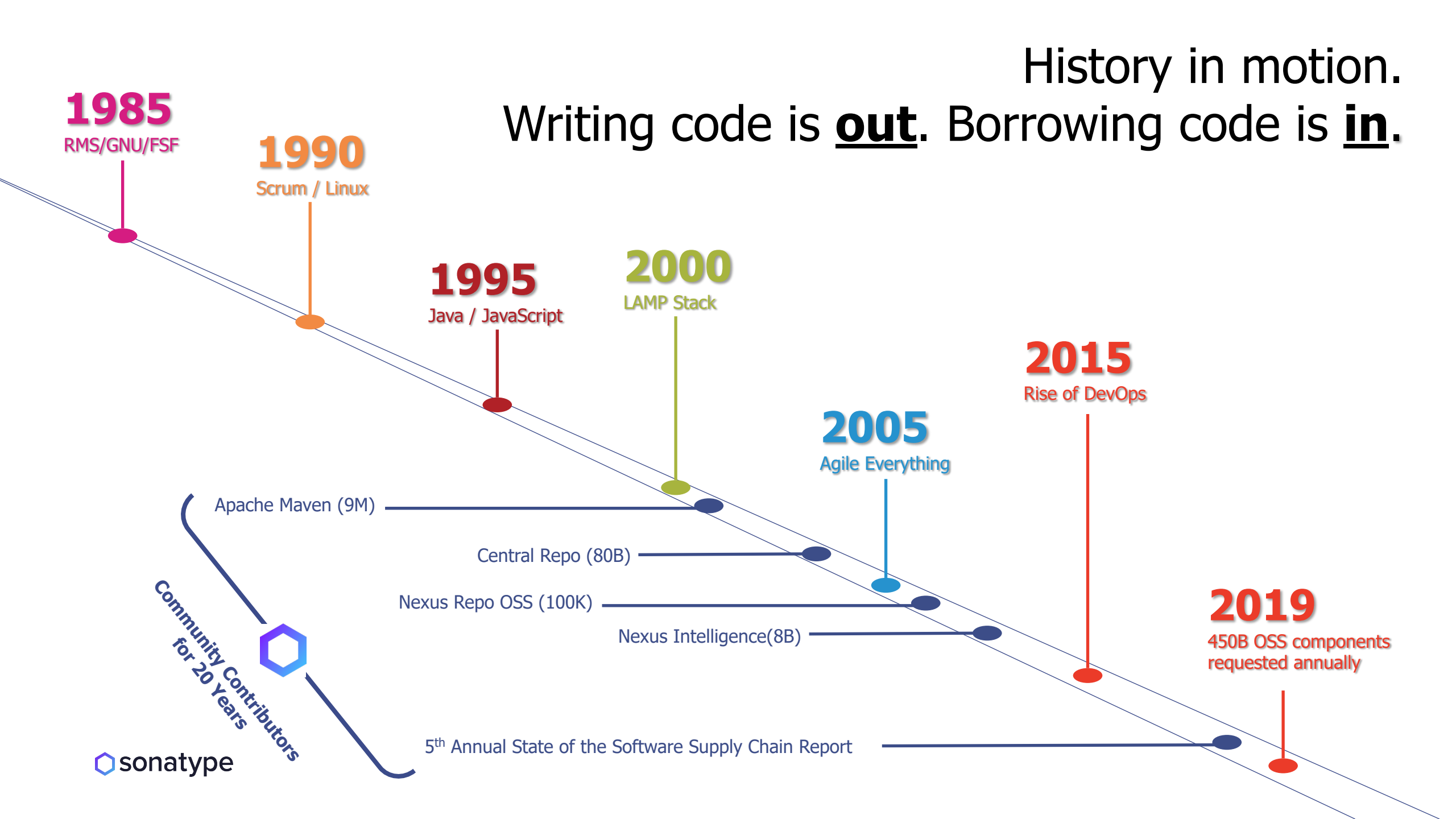
Intense pressure to deliver faster & more securely

Exponential growth in open source supply and demand (450B)

Open source not created equal. Ages like milk, not like wine.

History in motion.

Writing code is **out**. Borrowing code is **in**.



What is software supply chain management?
A new **(yet proven)** way of thinking.

1. Source parts from fewer and better suppliers.
2. Use only the highest quality parts.
3. Never pass known defects downstream.
4. Continuously track location of every part.

Everyone has a software supply chain.

(even if you don't call it that)

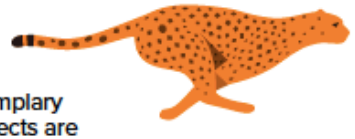
sonatype

And every developer in your software supply chain is in procurement

sonatype

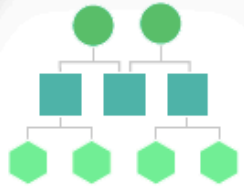
2019 State of the Software Supply Chain Report

sonatype



Exemplary Projects are **18x faster** at updating dependencies
pg. 13

Exemplary Projects are **3.4x faster** at remediating known vulnerabilities
pg. 29



Exemplary Dev Teams are **10x more likely** to schedule dependency updates
pg. 29

Exemplary Dev Teams experience a **55% reduction** in the use of vulnerable OSS component releases in automated environments
pg. 34

21,448 new open source releases per day
pg. 6

The top 5% of projects remediate security vulnerabilities **within 21 days**
pg. 14

Secure Dev Practices are **9.3x more likely** to proactively remove troublesome dependencies
pg. 31

313,000 average enterprise downloads of OSS components per year
pg. 27

Exemplary Dev Teams are **12x more likely** to have automated tools to manage open source dependencies
pg. 31

pg. 42

PCI introduces **new standards** for development teams using open source components

146B Java download requests in 2018, represented a **68%** year over year growth
pg. 9

pg. 38

71% increase in open source related breaches over the past five years

pg. 36

1 in 10 downloads of Java component releases have known vulnerabilities

51% of JavaScript components have a known security vulnerability
pg. 37

A Shifting Battlefront of Attacks

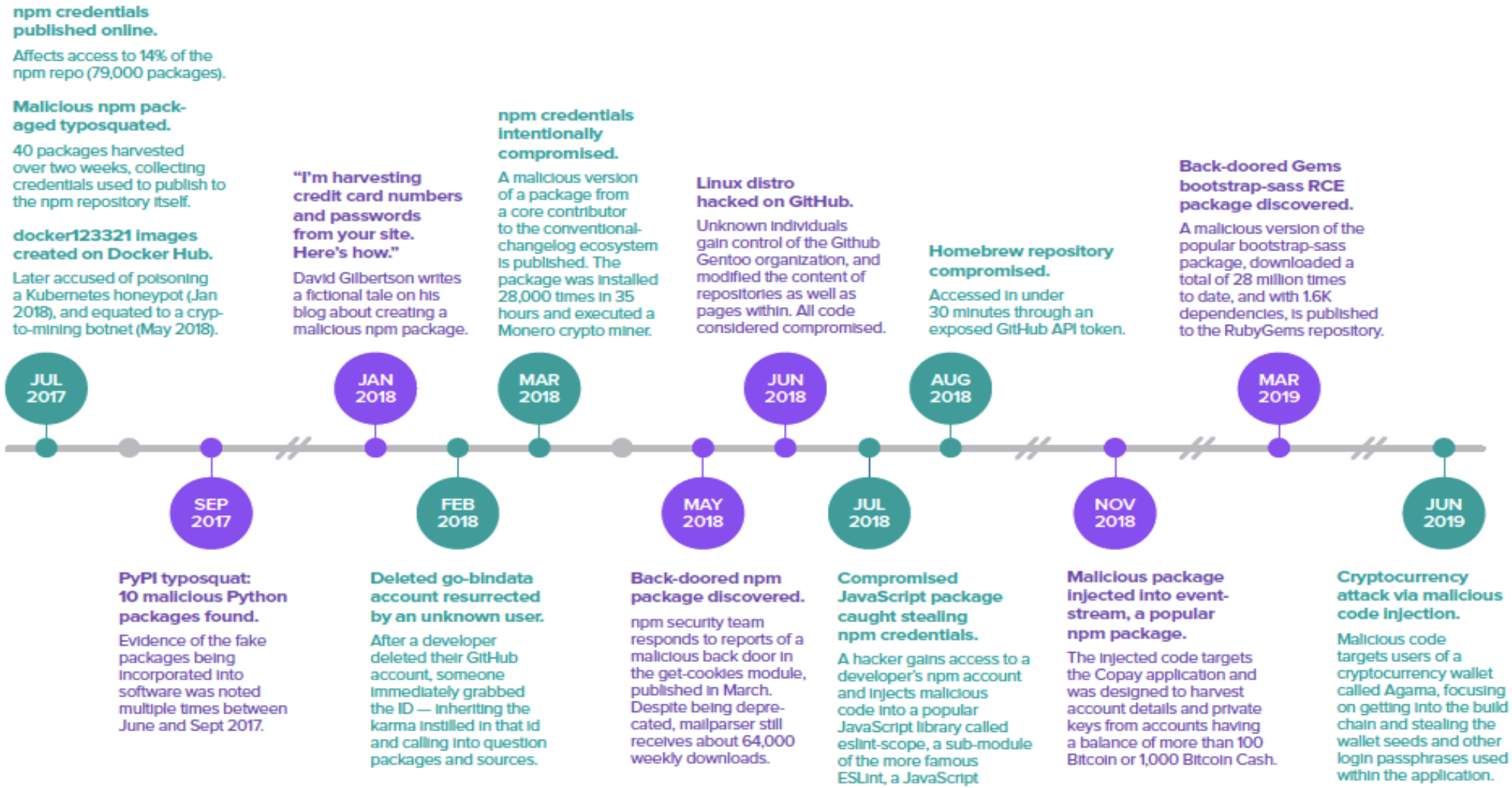
Malicious Code Injection

"Poisoning the Well"

sonatype

FIG 5E **A Shifting Battlefront of Attacks: Malicious Code Injection**

July 2017 – June 2019



Equifax was not alone – they all could have been different!

March 7
Apache Struts releases updated version to thwart vulnerability CVE-2017-5638

March 9
Cisco observes "a high number of exploitation events."

March 13
Okinawa Power
Japan Post

April 13
India Post

March '18
India's AADHAAR

3 Days in March

The Rest of the Story

March 8
NSA reveals Pentagon servers scanned by nation-states for vulnerable Struts instances

Struts exploit published to Exploit-DB.

March 10
Equifax
Canada Revenue Agency
Canada Statistics
GMO Payment Gateway

December '17
Monero Crypto Mining

Today
57% of the Fortune 100 continue to download vulnerable versions more than 2 years after announced

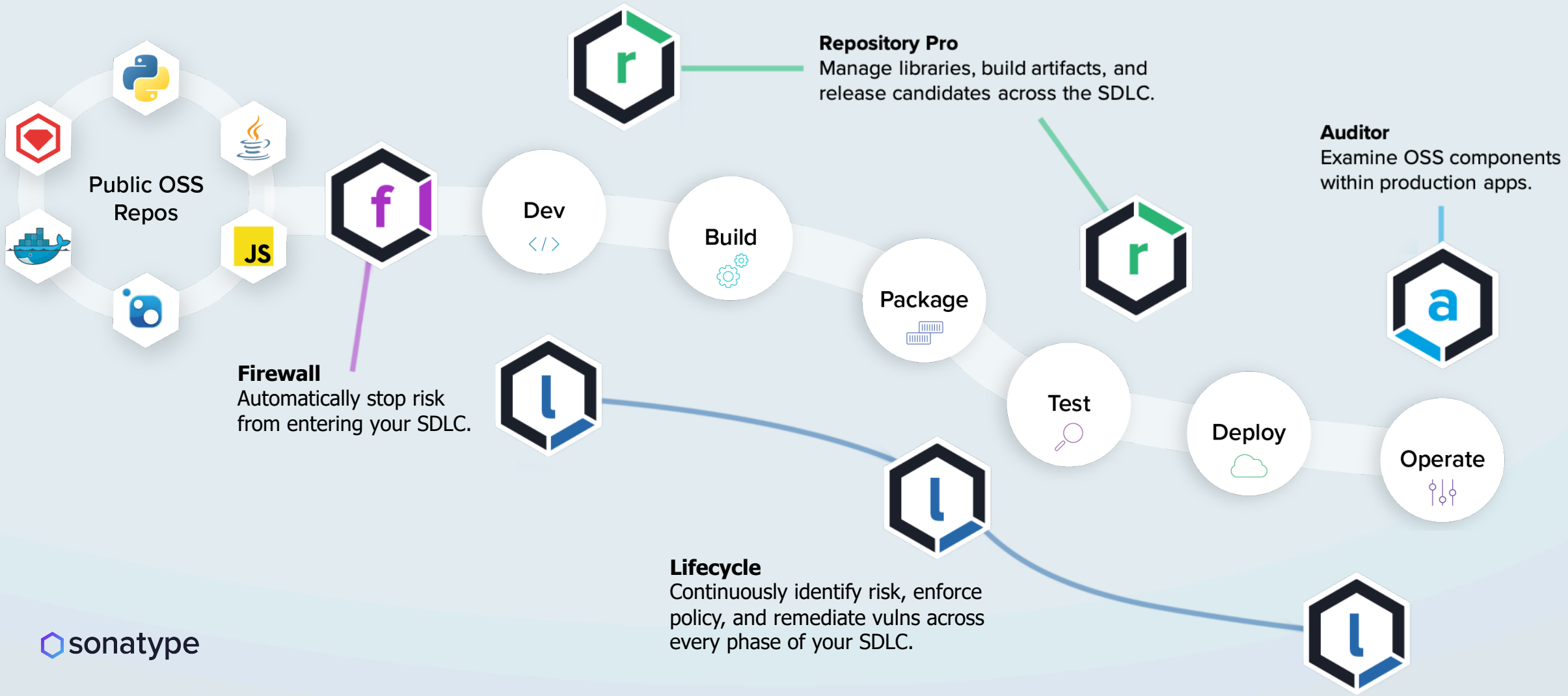
sonatype

And this is why Sonatype exists...

To unite software developers, security professionals, and IT operations on the same team and empower enterprises to continuously identify and remediate these and other open source risks, without slowing down innovation.

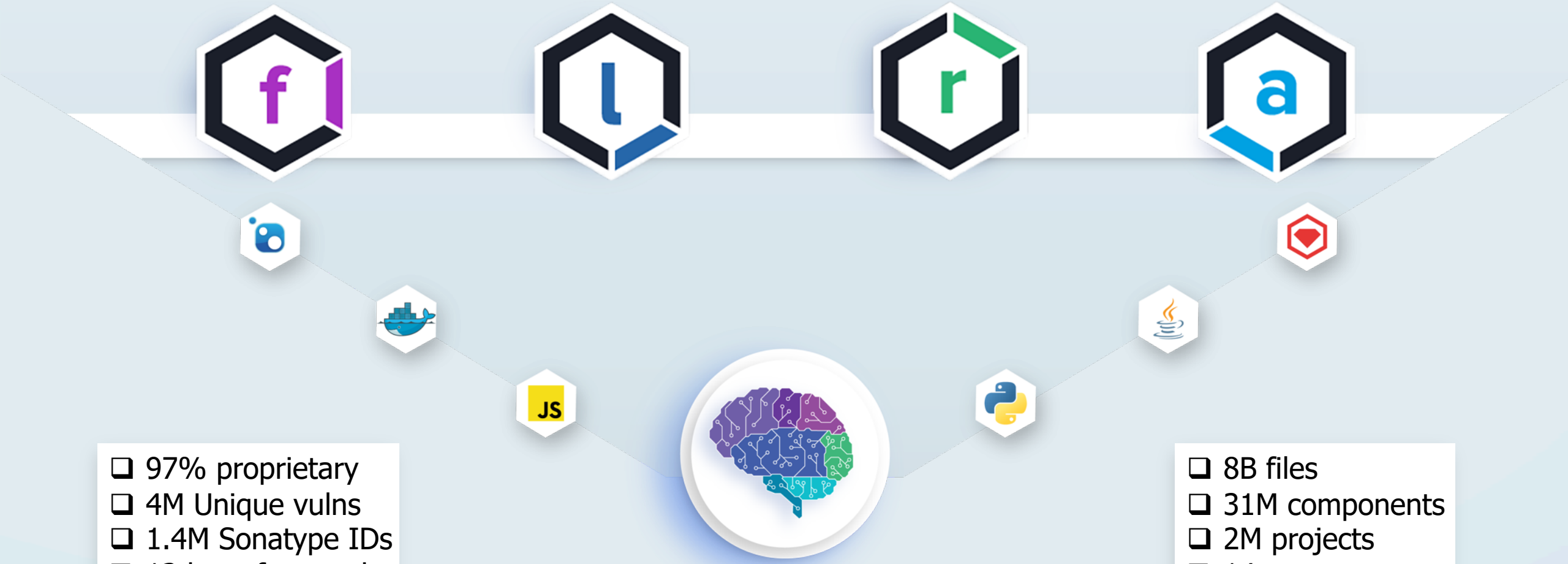
Say hello to the Nexus Platform.

Automatically enforce open source policy and control risk across every phase of the SDLC.



sonatype

100% powered by Nexus Intelligence.



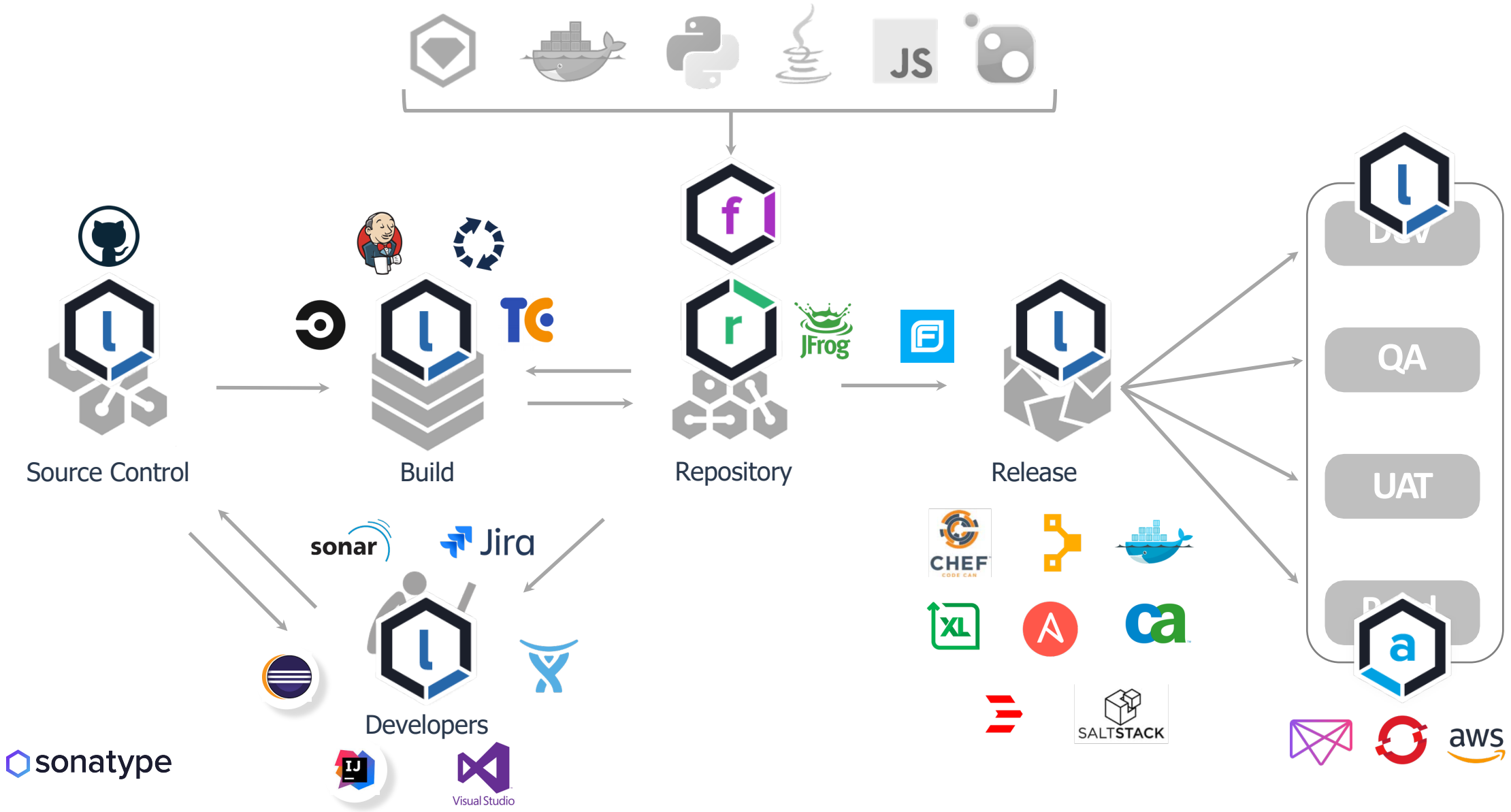
- ❑ 97% proprietary
- ❑ 4M Unique vulns
- ❑ 1.4M Sonatype IDs
- ❑ 12 hour fast tracks

- ❑ 8B files
- ❑ 31M components
- ❑ 2M projects
- ❑ 14 ecosystems

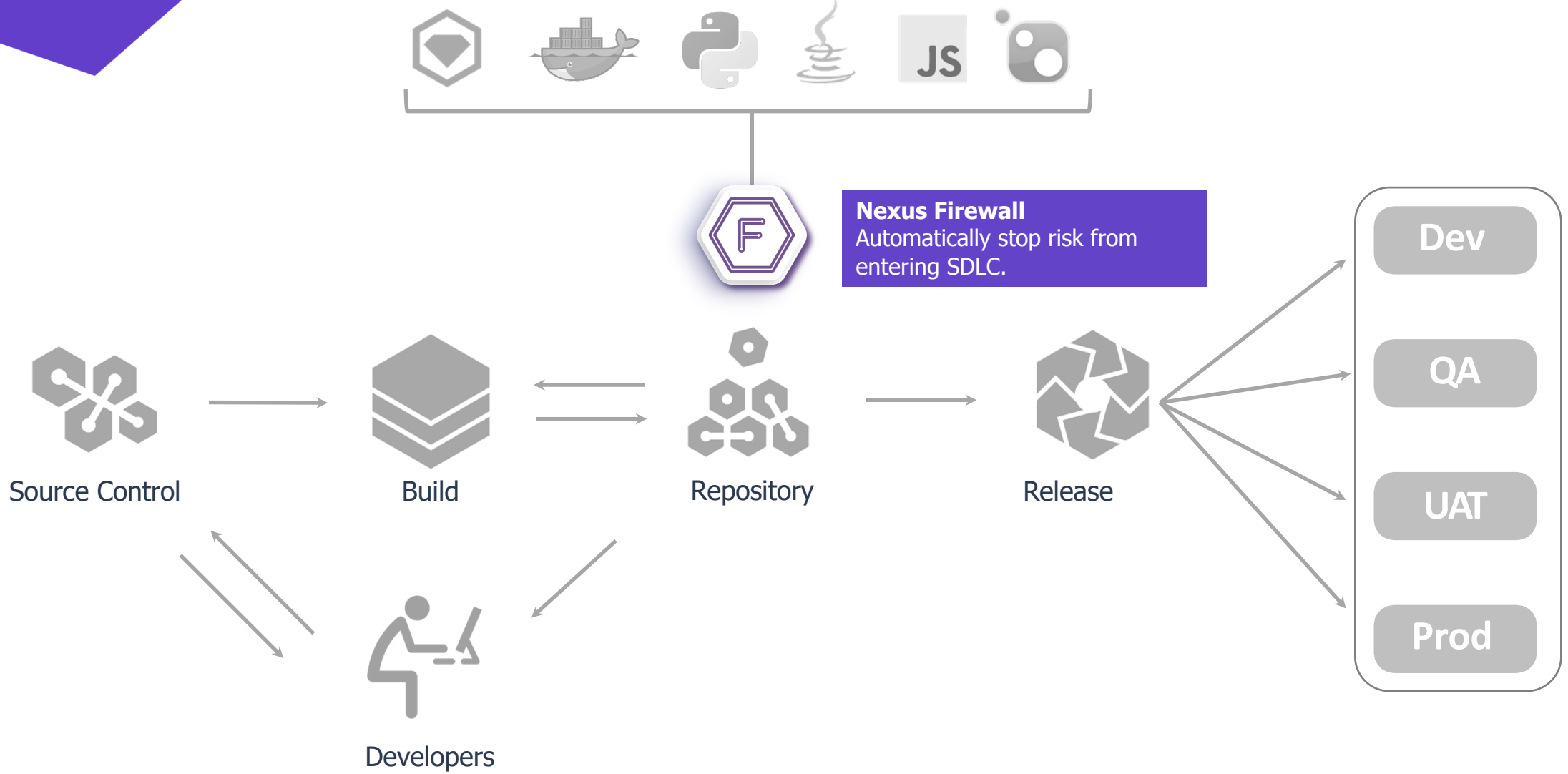
sonatype

Superior open source data service continuously refined by AI, machine learning, and 65 world class researchers.

Nexus integrates early and everywhere with your favorite pipeline tools.

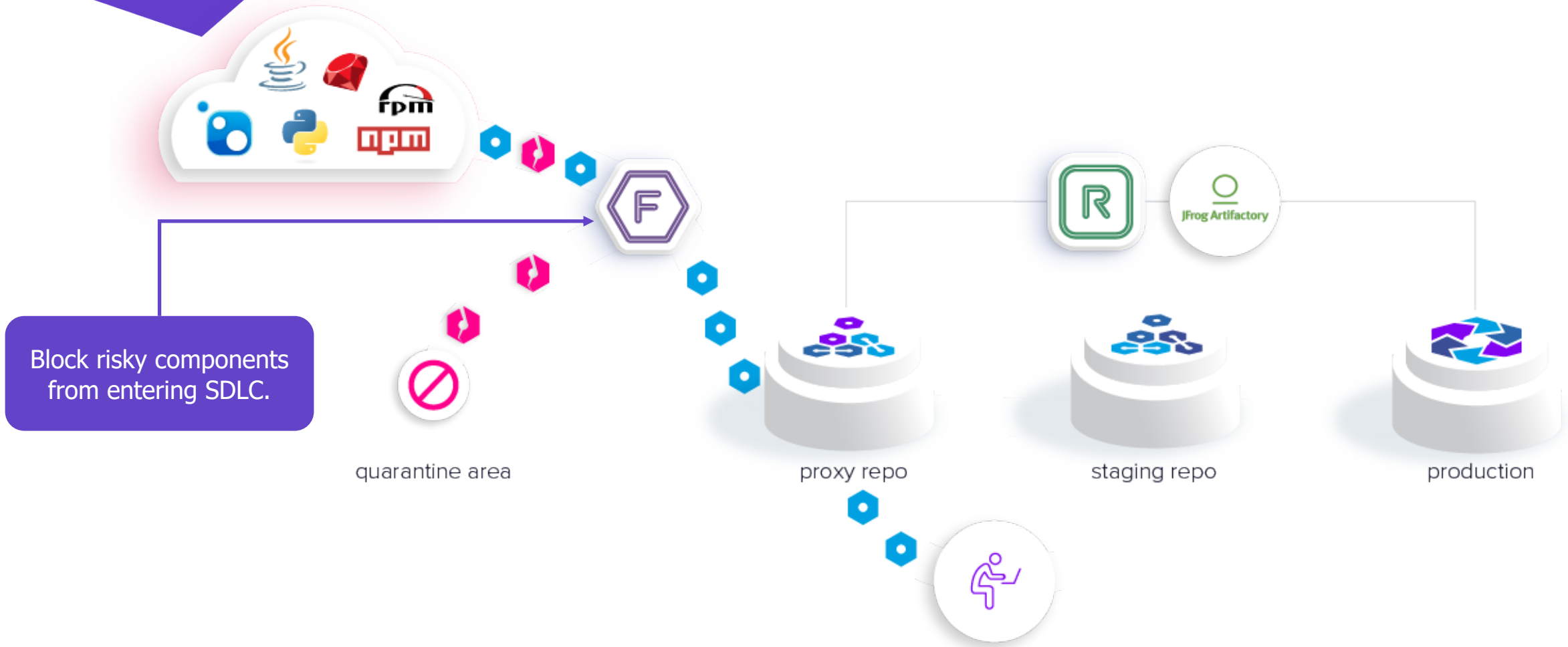


Nexus Firewall



sonatype

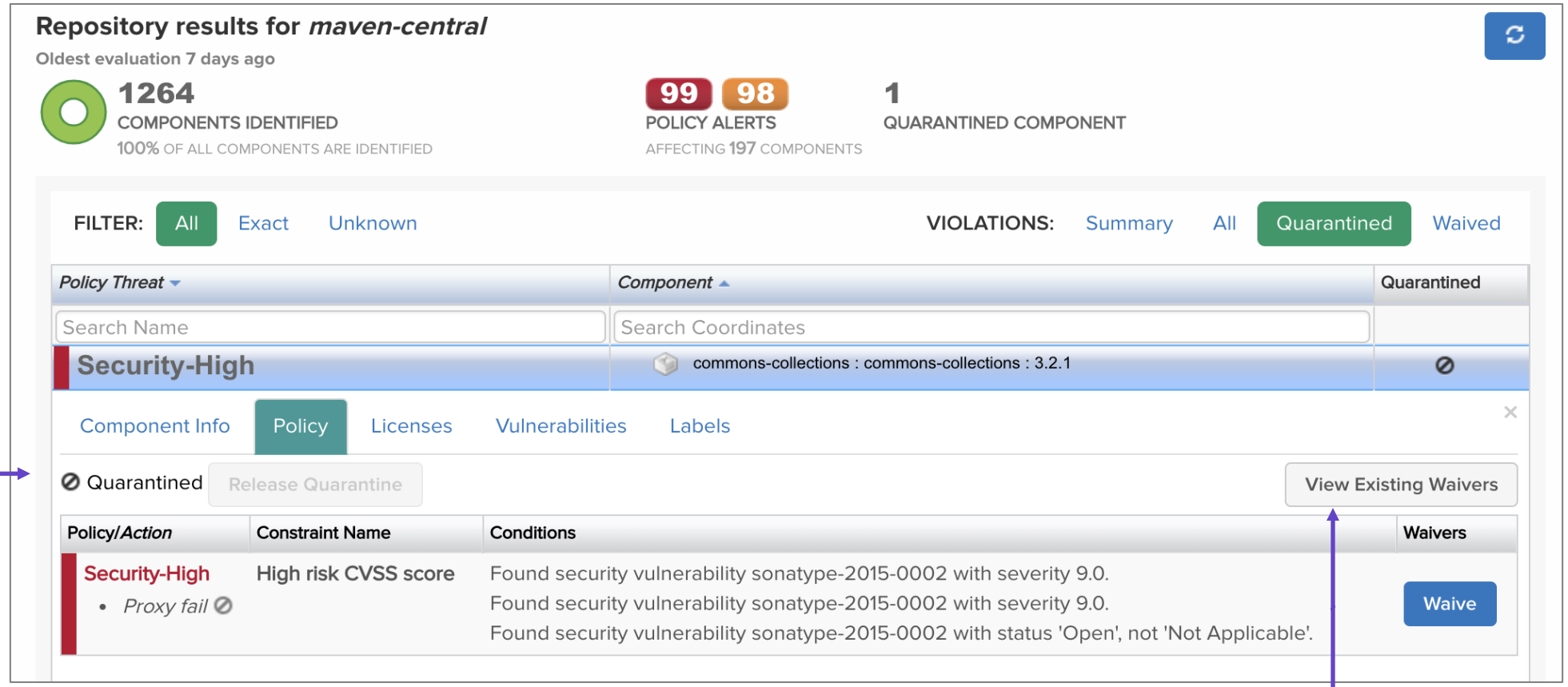
Nexus Firewall



sonatype

Nexus Firewall

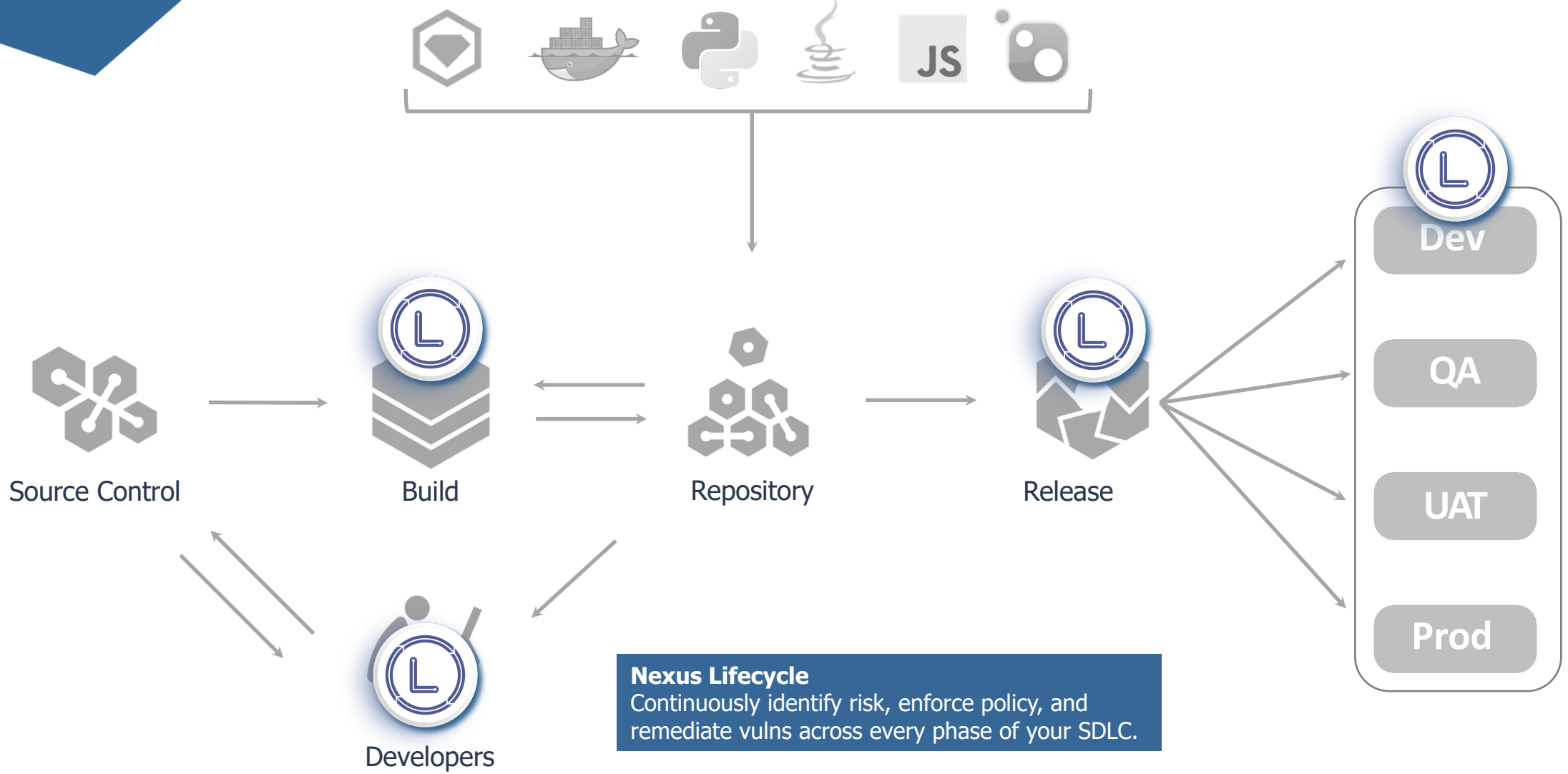
Block, analyze, and selectively admit components.



Waive policy violations for component use when necessary.

sonatype

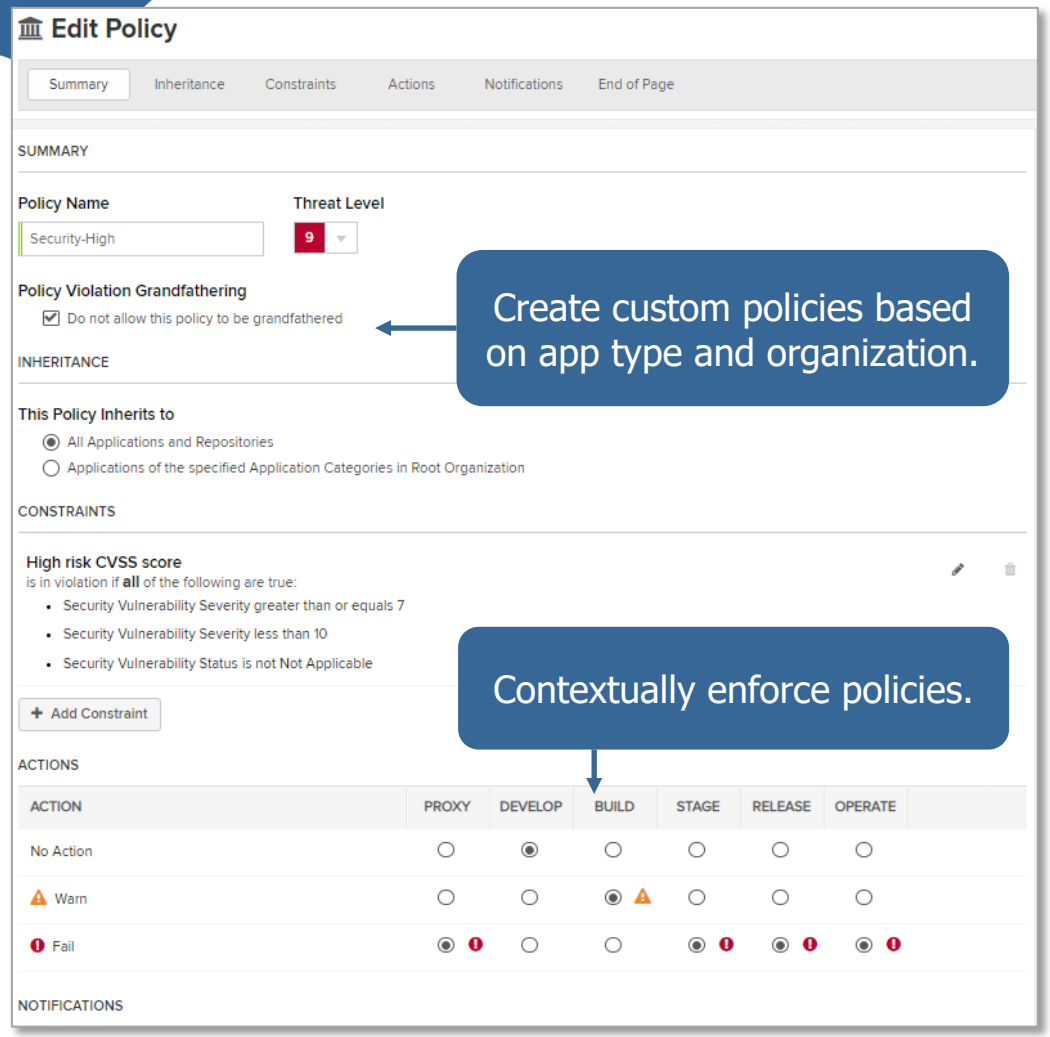
Nexus Lifecycle



Nexus Lifecycle
Continuously identify risk, enforce policy, and remediate vulns across every phase of your SDLC.

sonatype

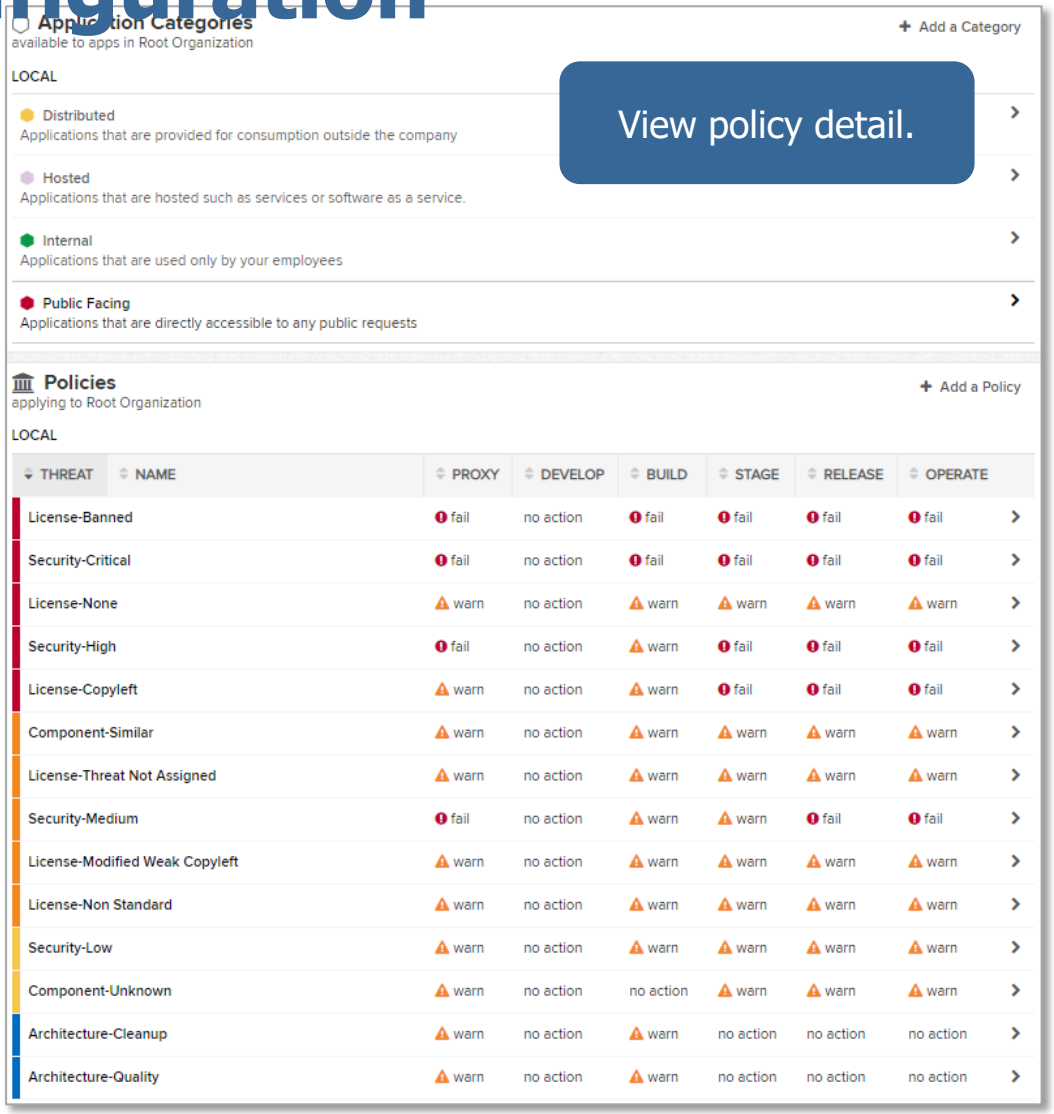
Nexus Lifecycle - Policy Configuration



Create custom policies based on app type and organization.

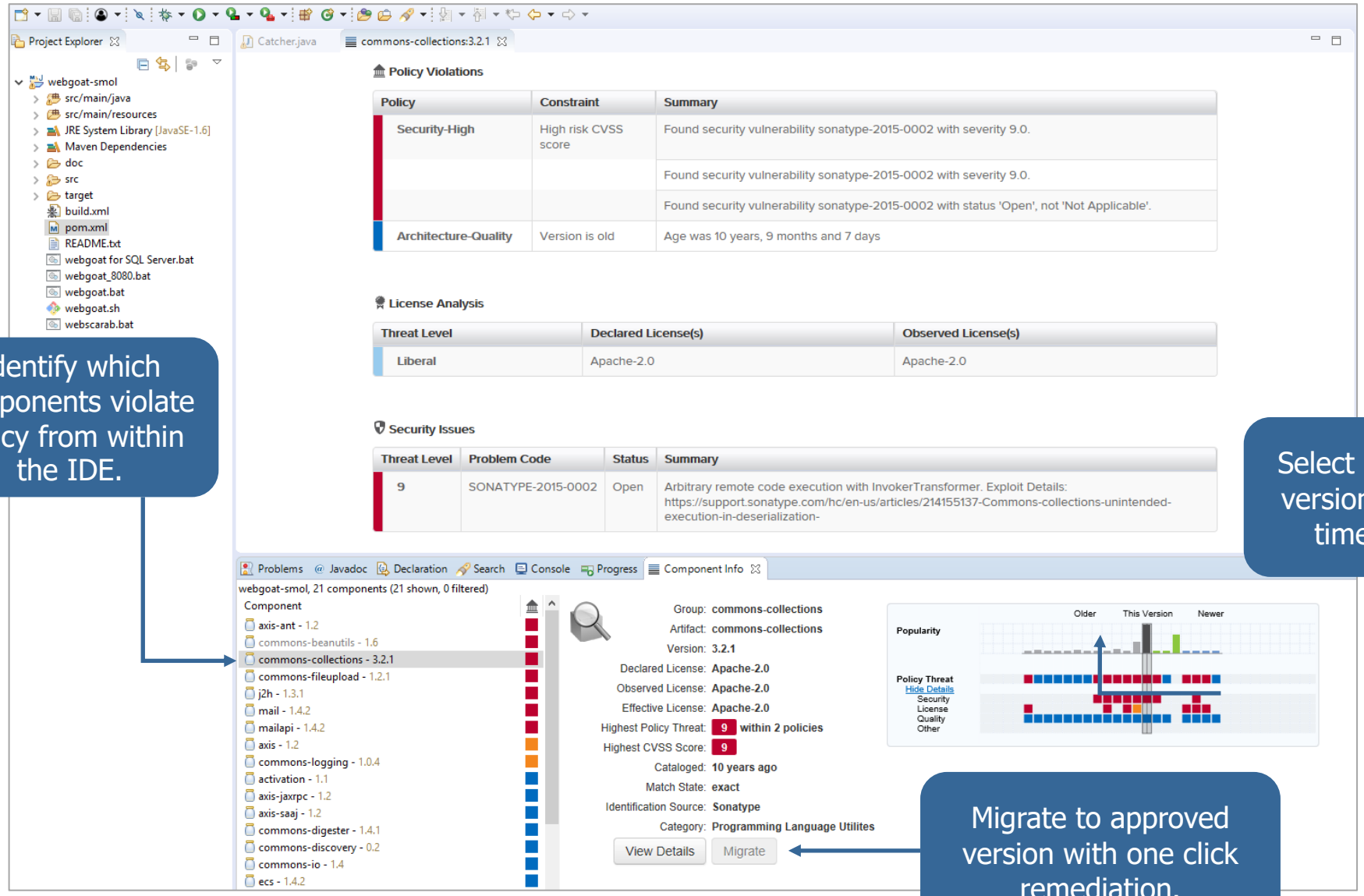
Contextually enforce policies.

View policy detail.



sonatype

Nexus Lifecycle – IDE Integration



Identify which components violate policy from within the IDE.

Select best component version based on real-time intelligence.

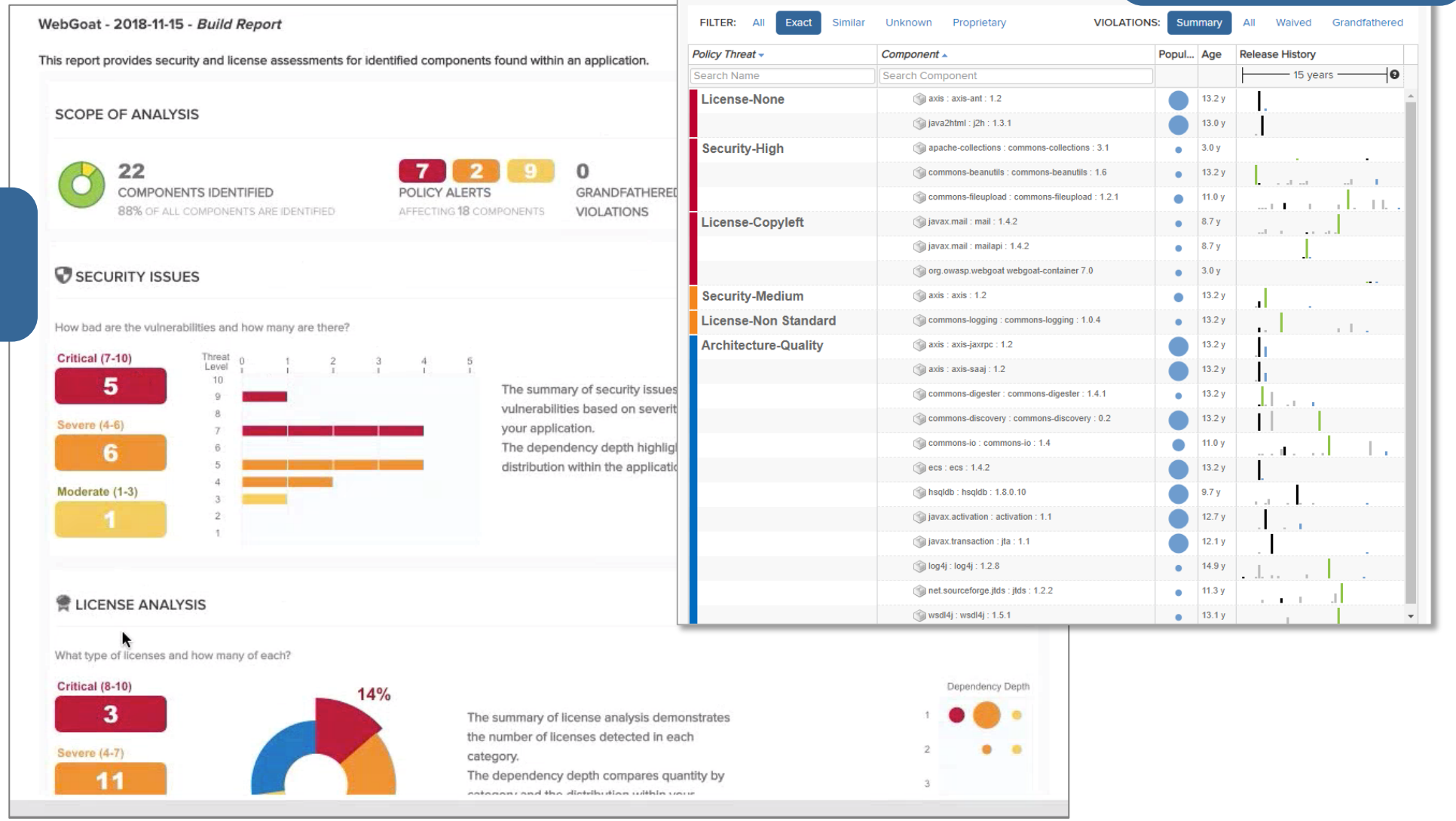
Migrate to approved version with one click remediation.

sonatype

Nexus Lifecycle – Reporting

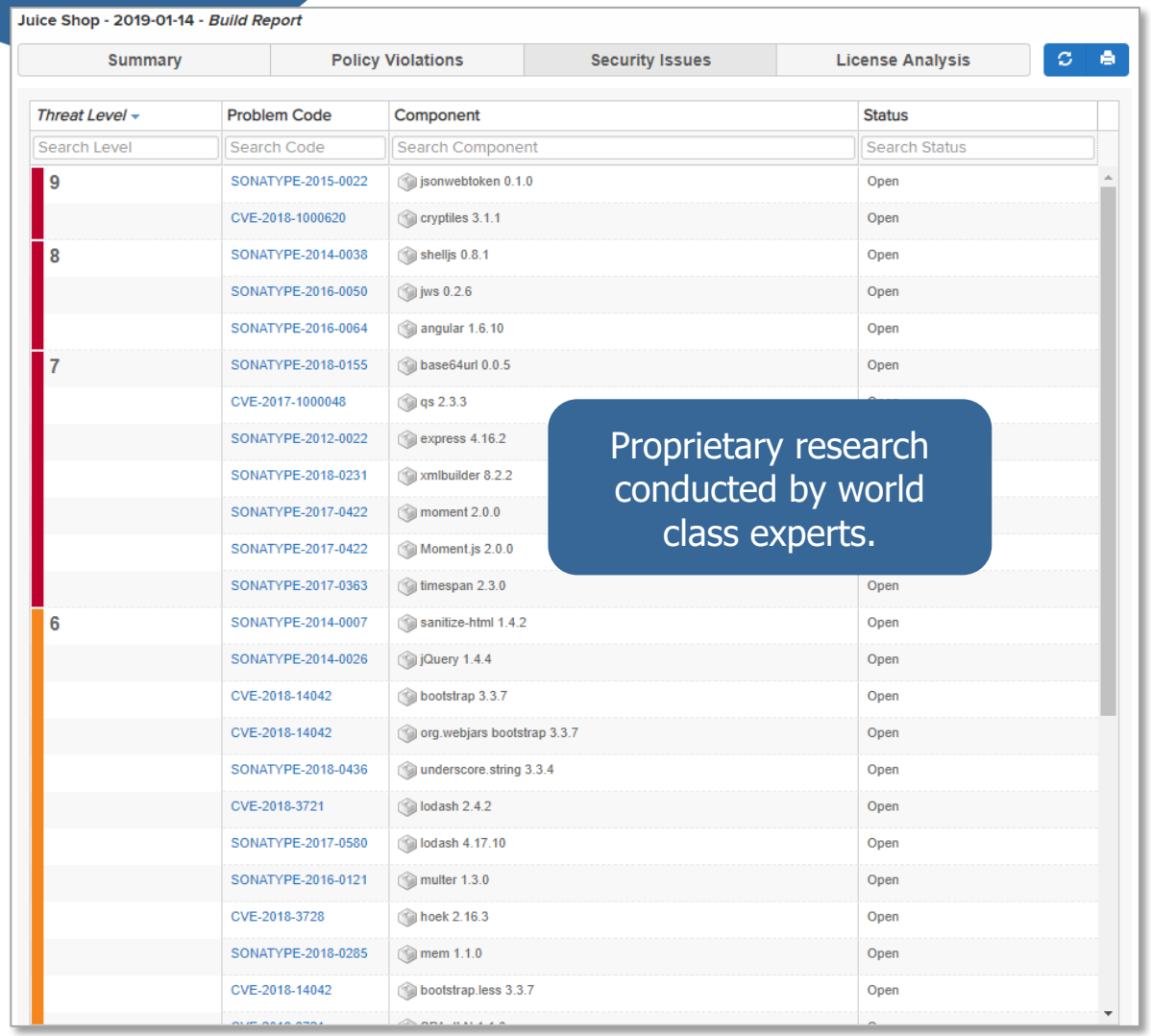
Policy based bill of materials.

Summary view of security and license policy violations.

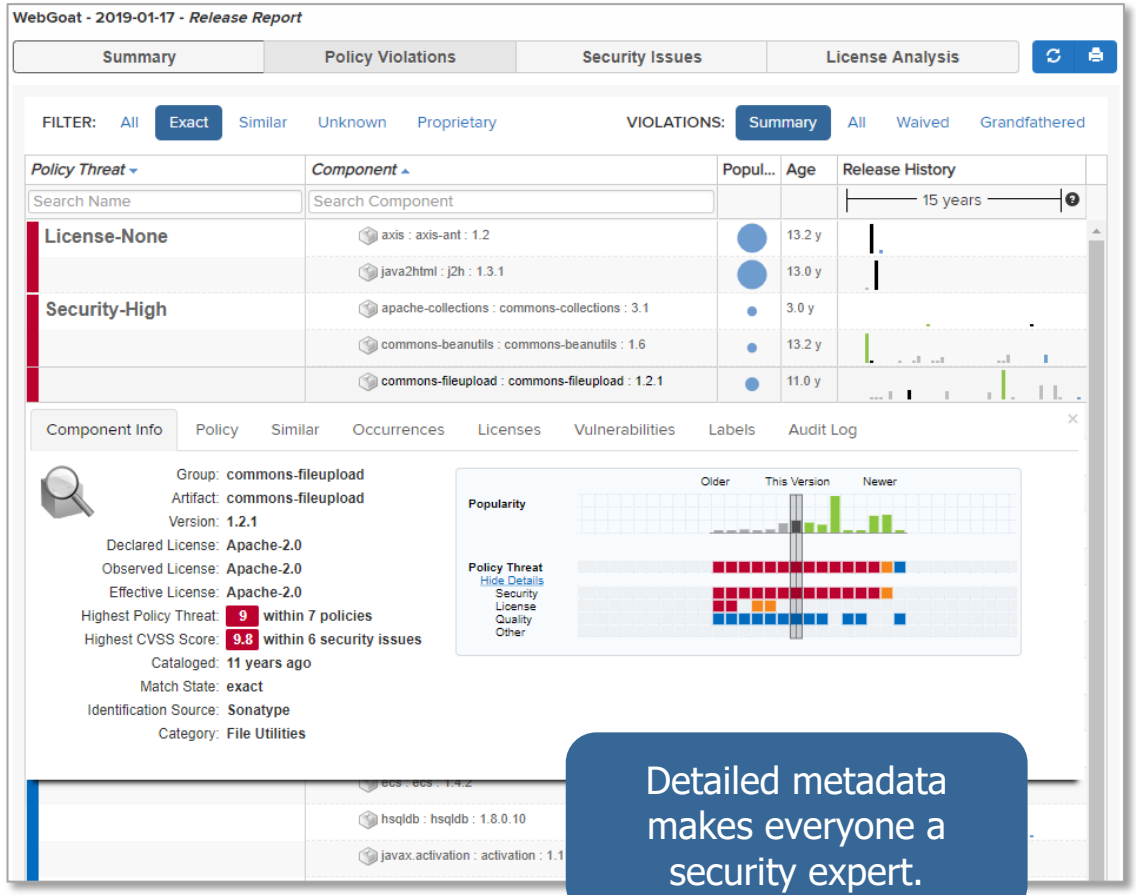


sonatype

Nexus Lifecycle – Curated Security Data



Proprietary research conducted by world class experts.



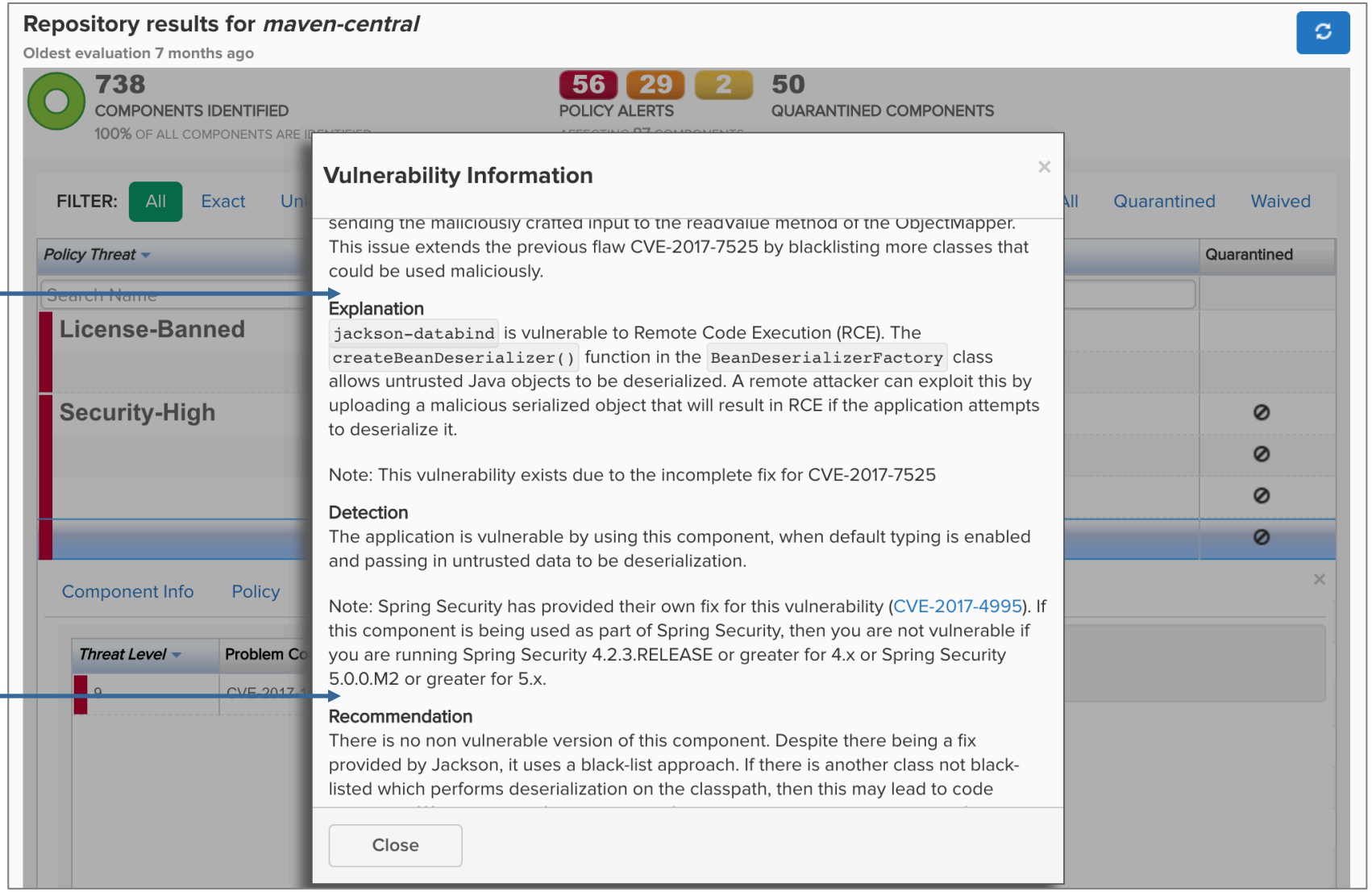
Detailed metadata makes everyone a security expert.

sonatype

Nexus Lifecycle – Remediation Guidance

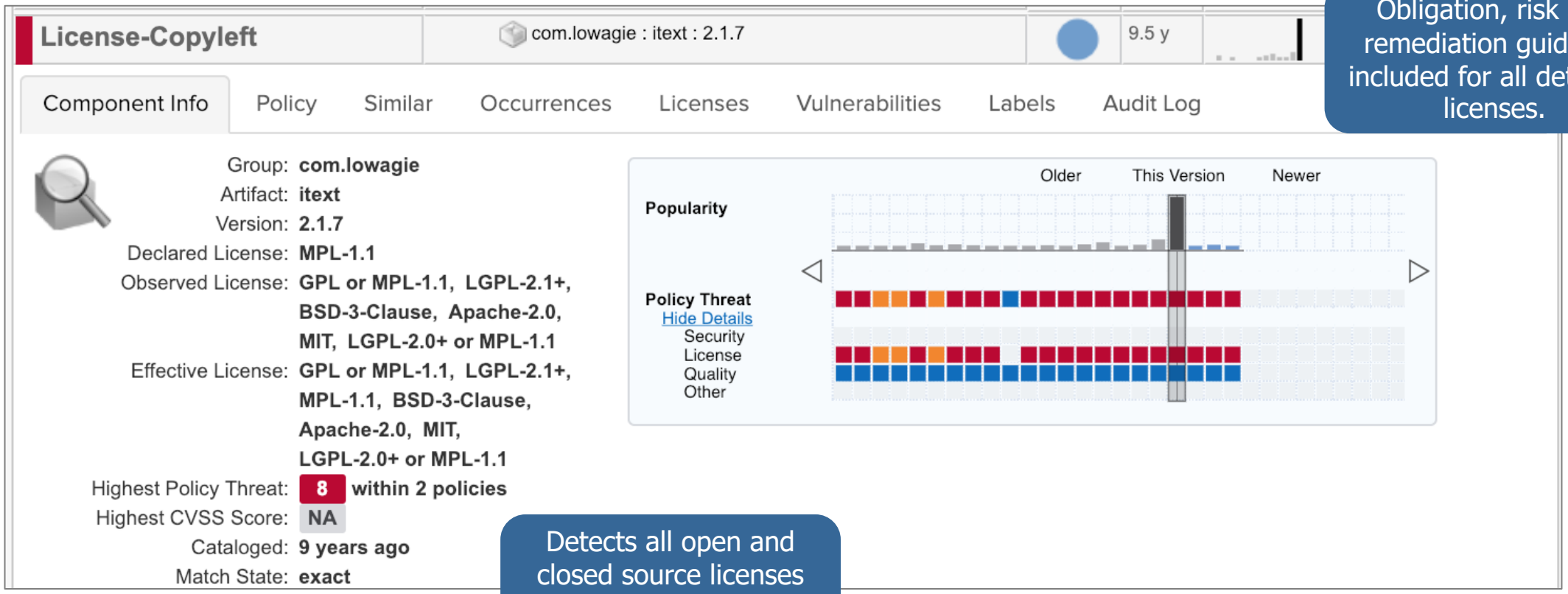
Easy to understand description written for developers by developers.

In-depth research includes detailed detection and remediation guidance.



sonatype

Nexus Lifecycle – Licensing Intelligence



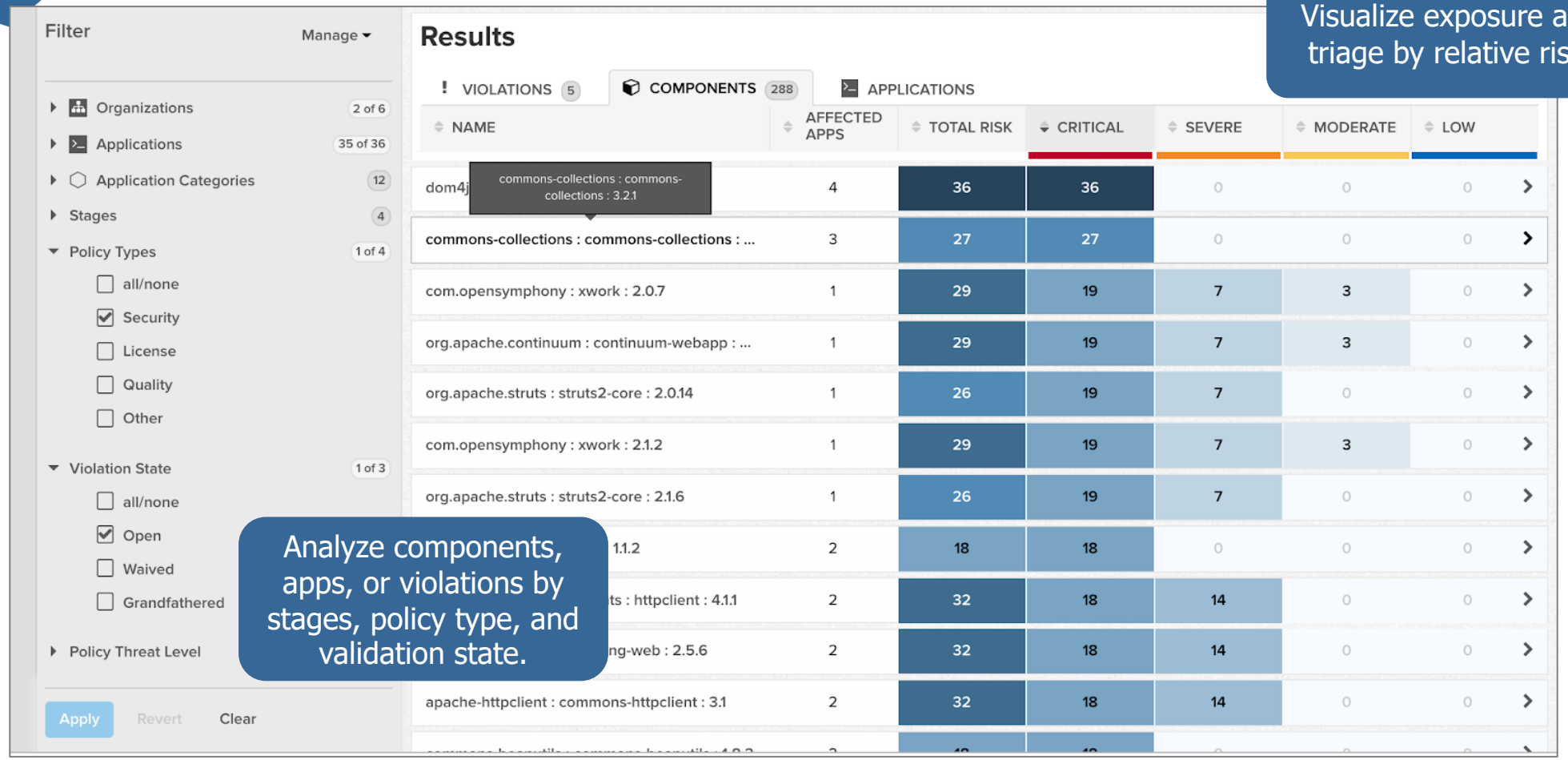
Obligation, risk and remediation guidance included for all detected licenses.

Detects all open and closed source licenses including declared, observed, and effective.

sonatype

Nexus Lifecycle – Dashboard

Visualize exposure and triage by relative risk.



Analyze components, apps, or violations by stages, policy type, and validation state.

sonatype

Nexus Lifecycle – Success Metrics

See violation trends over time and determine MTTR.

Mean Time to Resolution by Month

This data represents the average age of violations that were resolved each month in 18 applications over the past 12 months. A violation that does not reappear in a subsequent evaluation is considered resolved.

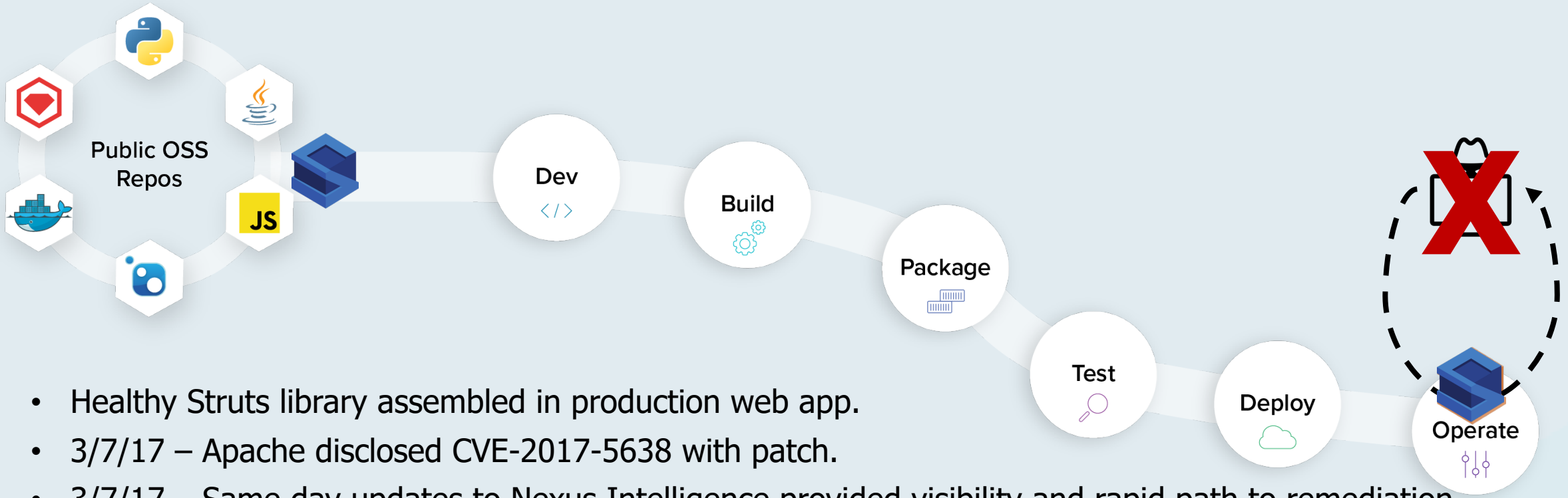
Applications with Violations by Policy Type

Over the past 12 months, **18** out of 18 applications contained violations, and **17** contained **critical** violations.

Demonstrate risk reduction to senior management.

sonatype

With Nexus – Equifax would have been different.



- Healthy Struts library assembled in production web app.
- 3/7/17 – Apache disclosed CVE-2017-5638 with patch.
- 3/7/17 – Same day updates to Nexus Intelligence provided visibility and rapid path to remediation.
- 3/10/17 – Criminals searching for vulnerable apps find none, look elsewhere.

But don’t take our word for it.

“Open source governance must work with developers; not against them. With Sonatype we’ve eliminated 54,000 hours of manual processes and created automated controls that have improved developer productivity by 28% and reduced cost by 30%.”

-Mike Garcia, SVP

“A key element of our transformation is modernizing how we build and deliver software applications so that security is built in from the start. As part of this we trust Sonatype’s Nexus platform to provide insight, visibility and automated governance of our use of open source libraries throughout the development and operations lifecycle.”

-Bryson Koehler, Chief Technology Officer

sonatype


UNITED STATES FEDERAL RESERVE SYSTEM
DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF JUSTICE
THE DEPARTMENT OF THE TREASURY 1789
DEPARTMENT OF STATE UNITED STATES OF AMERICA
DEPARTMENT OF HEALTH & HUMAN SERVICES USA
DEPARTMENT OF THE ARMY UNITED STATES OF AMERICA 1775
DEPARTMENT OF THE AIR FORCE MCMXLVII
DEPARTMENT OF THE NAVY UNITED STATES OF AMERICA
DEPARTMENT OF THE NAVY UNITED STATES MARINE CORPS
DEFENSE INFORMATION SYSTEMS AGENCY
UNITED STATES DEPARTMENT OF AGRICULTURE

Questions?
Contact us:

Brian Beard
703-608-4593
bbeard@sonatype.com