



Brian Beard

bbeard@sonatype.com

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



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



Intense pressure to
deliver faster
& more securely



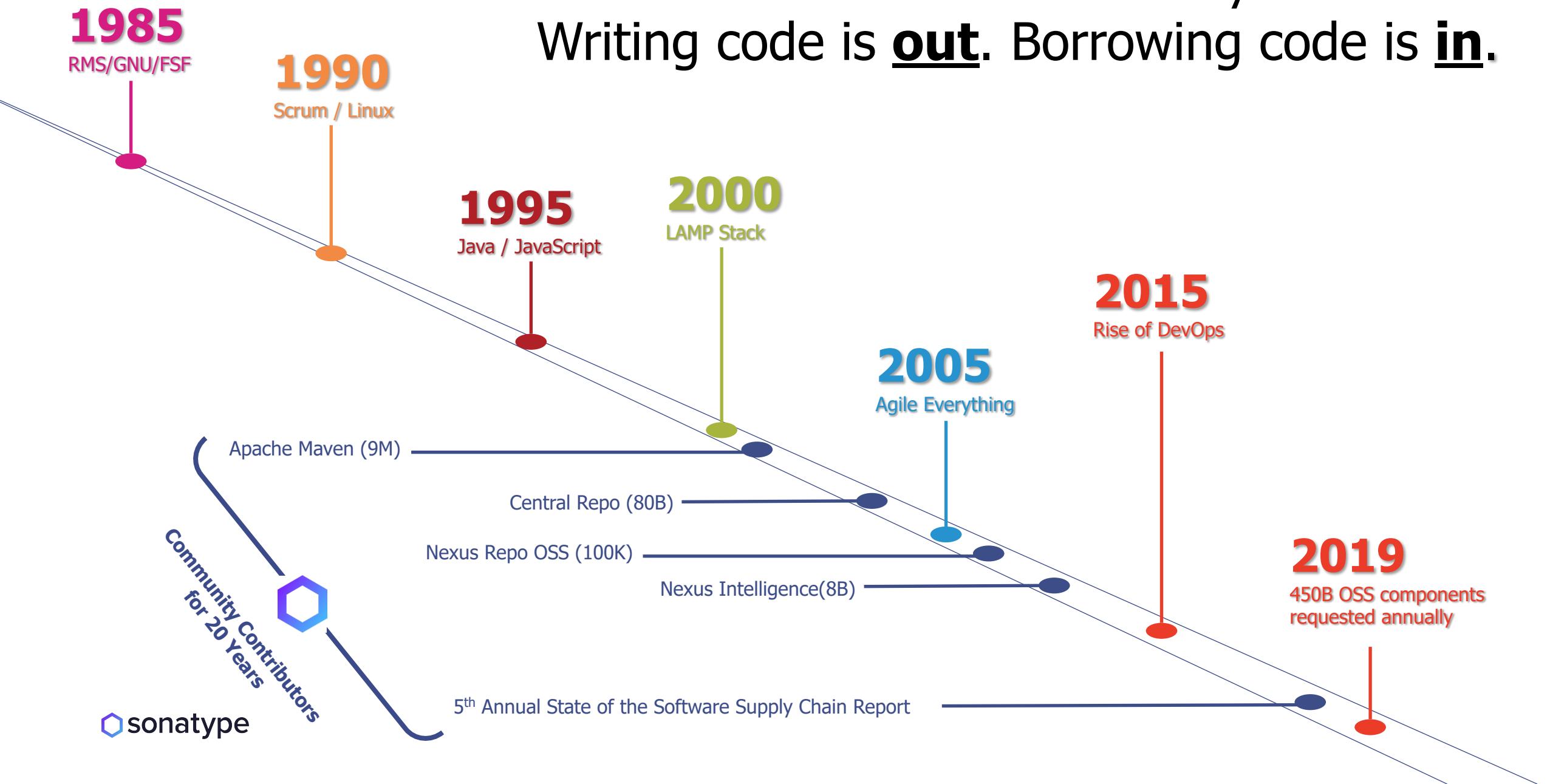
Exponential growth in
open source supply
and demand (450B)



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)



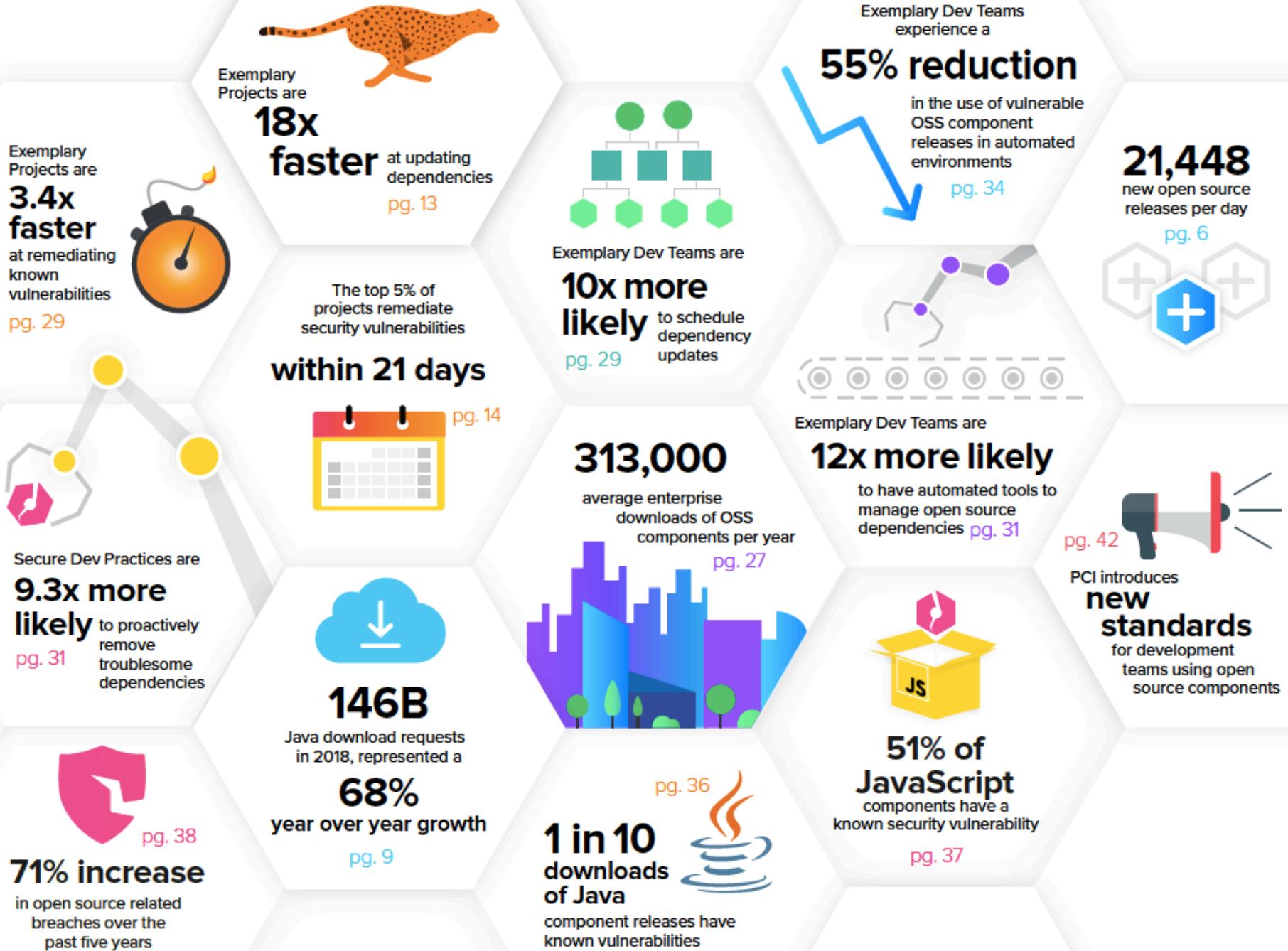
And every developer in your software supply chain is in procurement



85%

of your code is
sourced from
external suppliers

2019 State of the Software Supply Chain Report



A Shifting Battlefront of Attacks

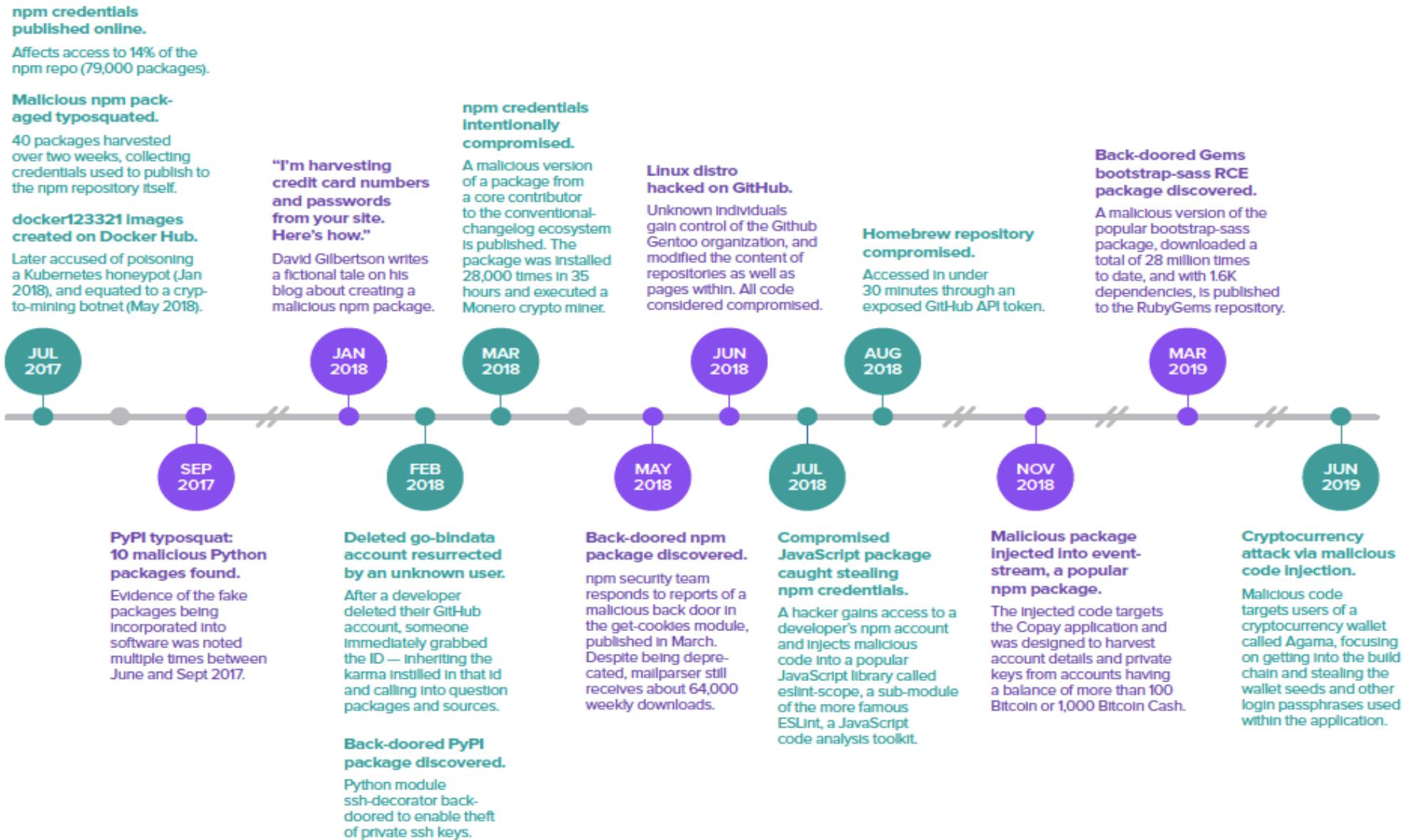
Malicious Code Injection

“Poisoning the Well”



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



March '18

India's AADHAAR

3 Days in March

The Rest of the Story

March 8

USA 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

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.



Visibility



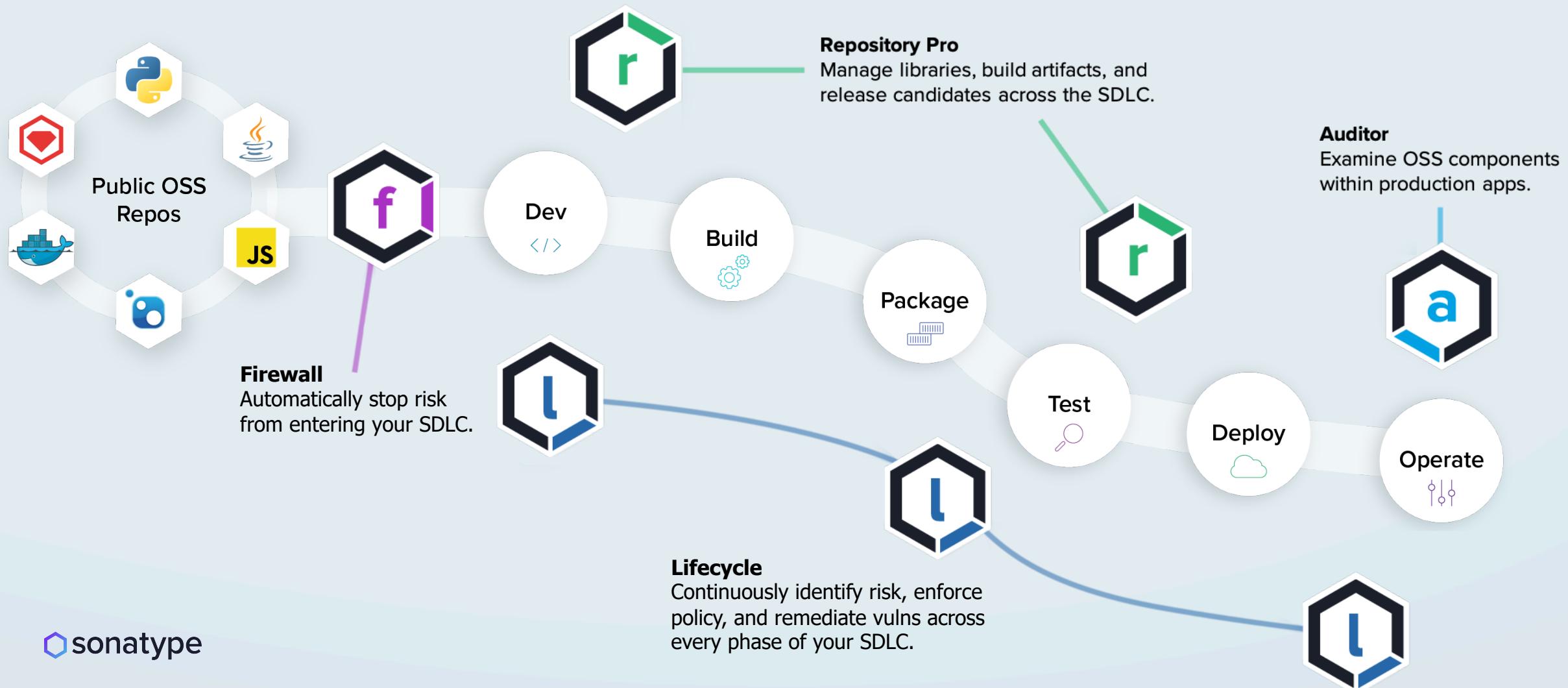
Culture



Alignment

Say hello to the Nexus Platform.

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



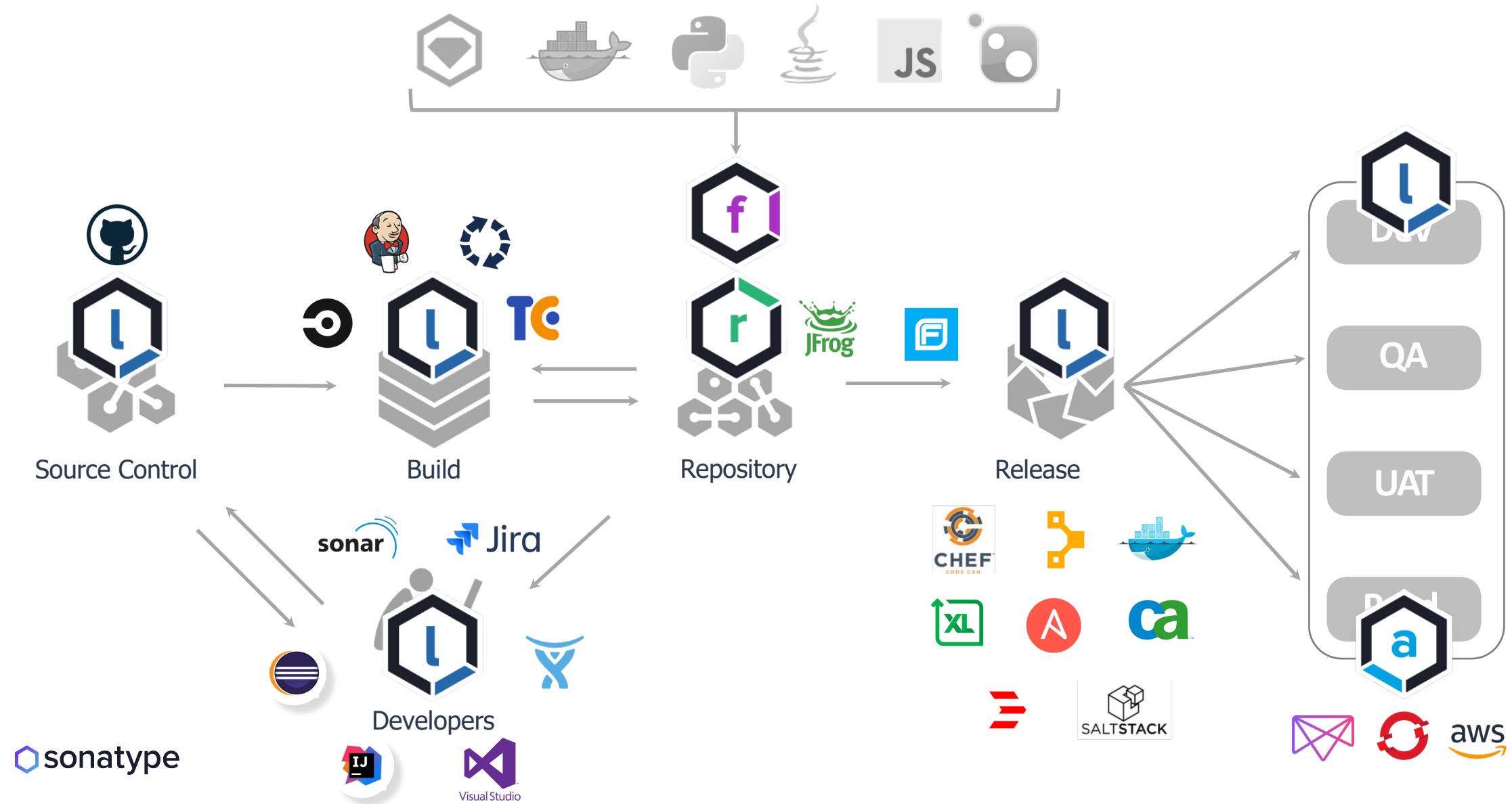
100% powered by Nexus Intelligence.



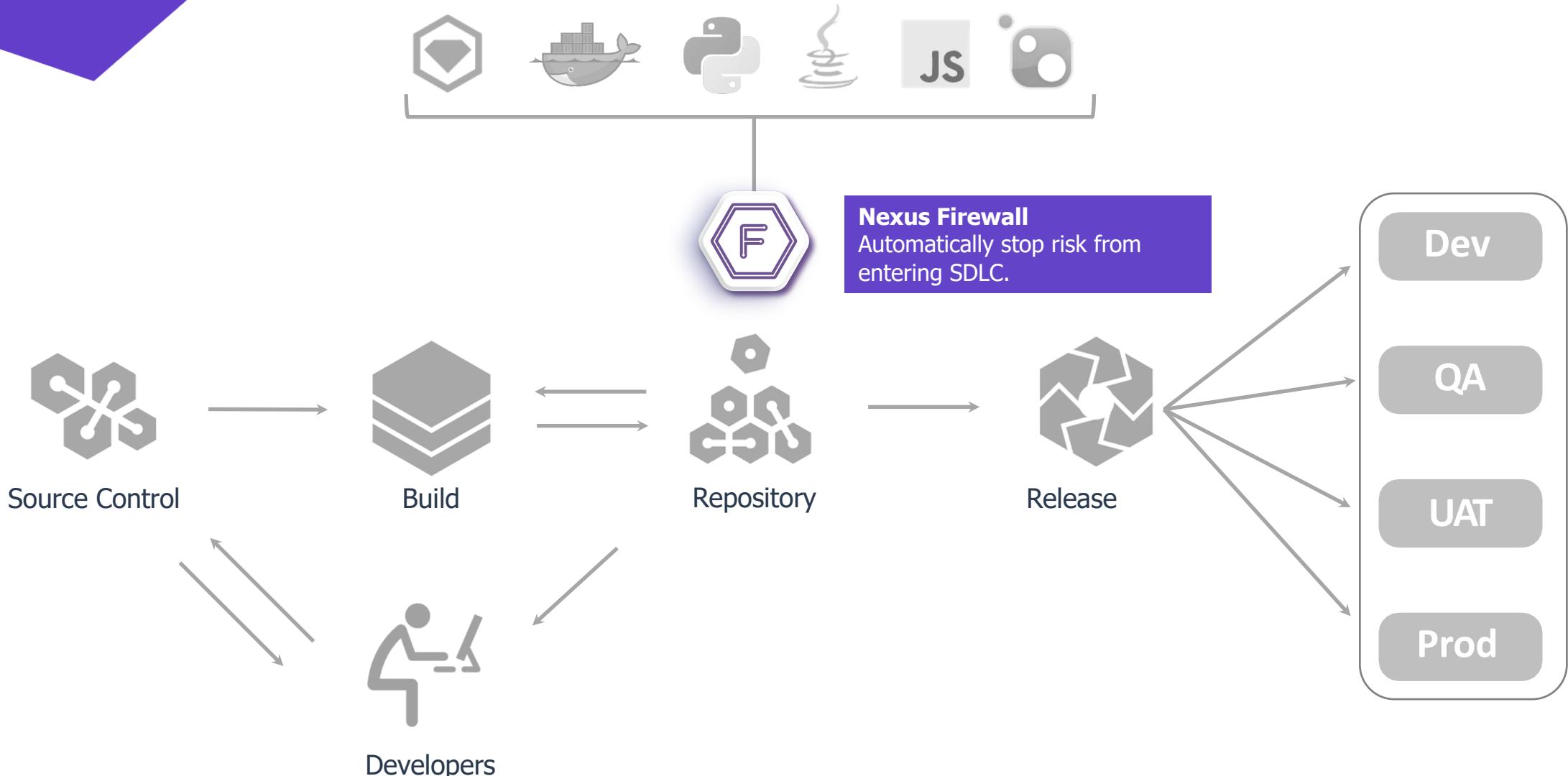
- 97% proprietary
- 4M Unique vulns
- 1.4M Sonatype IDs
- 12 hour fast tracks

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

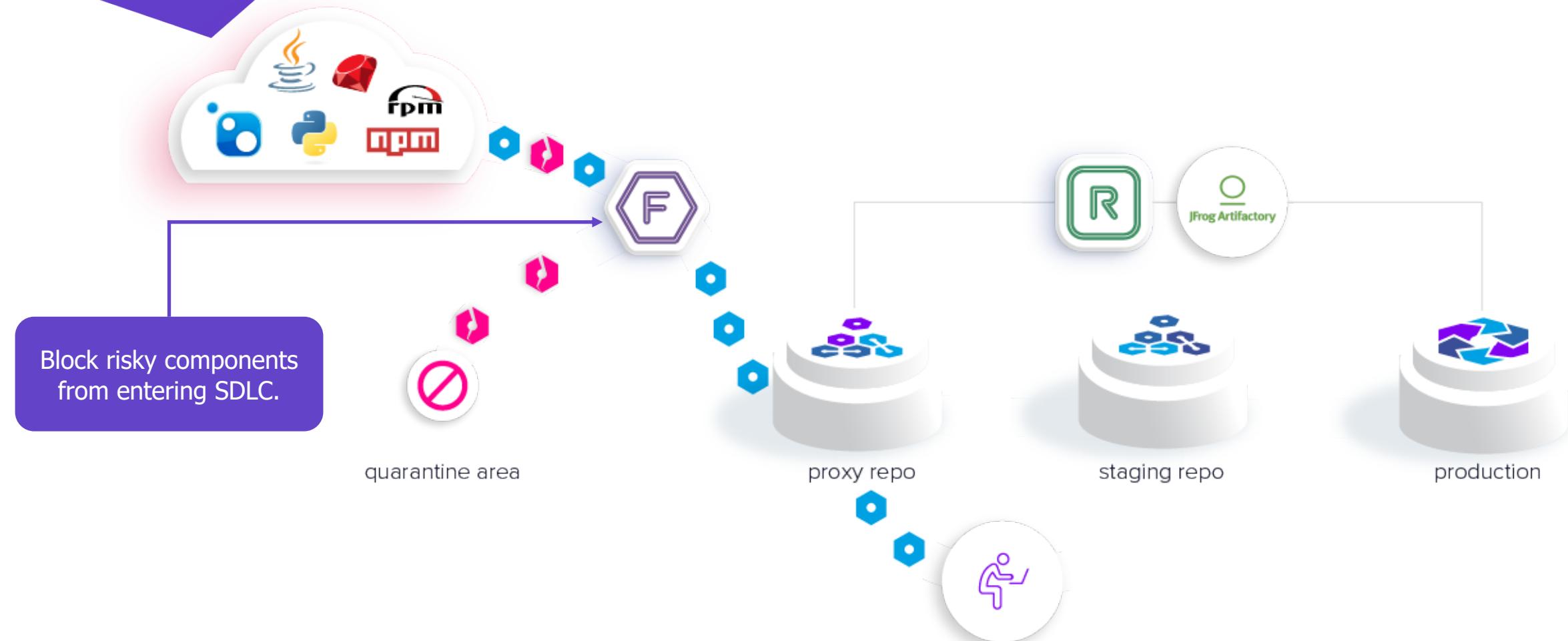
Nexus integrates early and everywhere with your favorite pipeline tools.



Nexus Firewall



Nexus Firewall



Nexus Firewall

Block, analyze, and selectively admit components.

Repository results for *maven-central*
Oldest evaluation 7 days ago

1264 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE IDENTIFIED

99 POLICY ALERTS
AFFECTING **197** COMPONENTS

1 QUARANTINED COMPONENT

FILTER: All Exact Unknown **VIOLATIONS:** Summary All Quarantined Waived

Policy Threat ▾	Component ▾	Quarantined
Search Name	Search Coordinates	
Security-High	commons-collections : commons-collections : 3.2.1	∅

Component Info Policy Licenses Vulnerabilities Labels

Quarantined

View Existing Waivers

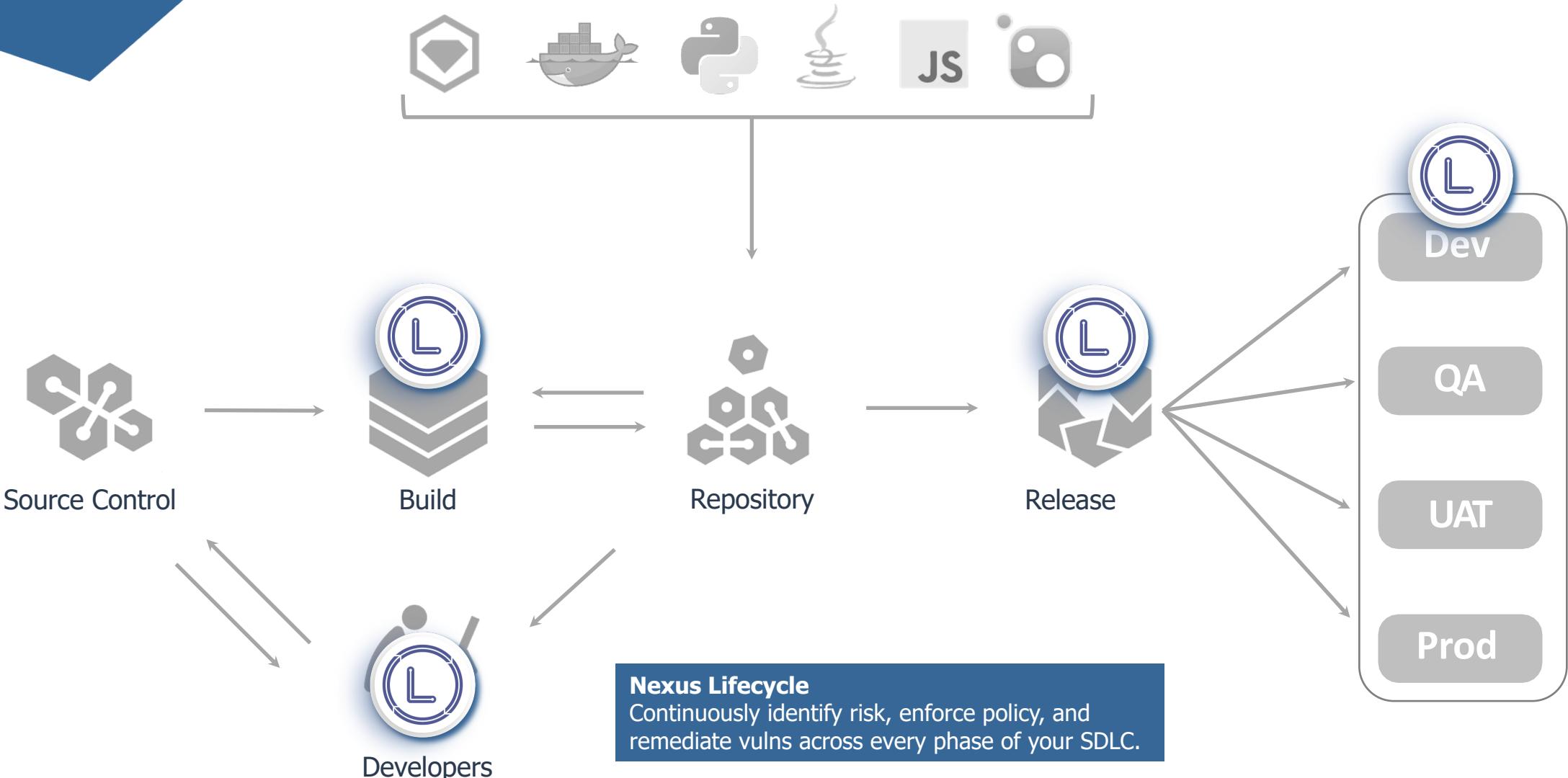
Policy/Action	Constraint Name	Conditions
Security-High • Proxy fail	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with status 'Open', not 'Not Applicable'.

Waivers

Waive

Waive policy violations for component use when necessary.

Nexus Lifecycle



Nexus Lifecycle - Policy Configuration

Edit Policy

Summary Inheritance Constraints Actions Notifications End of Page

SUMMARY

Policy Name: Security-High Threat Level: 9

Policy Violation Grandfathering: Do not allow this policy to be grandfathered

INHERITANCE

This Policy Inherits to:

- All Applications and Repositories
- Applications of the specified Application Categories in Root Organization

CONSTRAINTS

High risk CVSS score: is in violation if all of the following are true:

- Security Vulnerability Severity greater than or equals 7
- Security Vulnerability Severity less than 10
- Security Vulnerability Status is not Not Applicable

+ Add Constraint

ACTIONS

Action	Proxy	Develop	Build	Stage	Release	Operate
No Action	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Warn	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fail	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

NOTIFICATIONS

Create custom policies based on app type and organization.

Contextually enforce policies.

Application Categories available to apps in Root Organization

+ Add a Category

View policy detail.

LOCAL	
Distributed	Applications that are provided for consumption outside the company
Hosted	Applications that are hosted such as services or software as a service.
Internal	Applications that are used only by your employees
Public Facing	Applications that are directly accessible to any public requests

Policies applying to Root Organization

+ Add a Policy

THREAT	NAME	PROXY	DEVELOP	BUILD	STAGE	RELEASE	OPERATE
License-Banned	fail fail no action fail fail fail fail fail fail						
Security-Critical	fail fail no action fail fail fail fail fail fail						
License-None	warn warn no action warn warn warn warn warn warn						
Security-High	fail fail no action warn warn fail fail fail fail						
License-Copyleft	warn warn no action warn fail fail fail fail fail						
Component-Similar	warn warn no action warn warn warn warn warn warn						
License-Threat Not Assigned	warn warn no action warn warn warn warn warn warn						
Security-Medium	fail fail no action warn warn fail fail fail fail						
License-Modified Weak Copyleft	warn warn no action warn warn warn warn warn warn						
License-Non Standard	warn warn no action warn warn warn warn warn warn						
Security-Low	warn warn no action warn warn warn warn warn warn						
Component-Unknown	warn warn no action no action warn warn warn warn						
Architecture-Cleanup	warn warn no action warn warn no action no action						
Architecture-Quality	warn warn no action warn warn no action no action						

Nexus Lifecycle – IDE Integration

The screenshot shows an IDE interface with the following components:

- Project Explorer:** Shows a project named "webgoat-smol" with various files and folders like pom.xml, README.txt, and build.xml.
- Central Panel:** Displays analysis results for the artifact "commons-collections:3.2.1".
 - Policy Violations:** Lists violations under "Security-High" and "Architecture-Quality".
 - License Analysis:** Shows threat level as "Liberal" and declared license as "Apache-2.0".
 - Security Issues:** Lists a single issue: "SONATYPE-2015-0002" (Threat Level 9) with a summary about arbitrary remote code execution.
- Component Info Panel:** Provides detailed information for "commons-collections:3.2.1".
 - Component List:** Lists dependencies: axis-ant - 1.2, commons-beanutils - 1.6, commons-collections - 3.2.1 (highlighted), 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.
 - Popularity:** A chart comparing popularity of this version against older and newer versions.
 - Policy Threat:** Summary of policy threats, including highest threat (9) and CVSS score (9).
 - Identification Source:** Sonatype.
 - Category:** Programming Language Utilities.
 - Actions:** Buttons for "View Details" and "Migrate".

Annotations:

- A callout bubble points to the "Policy Violations" section with the text: "Identify which components violate policy from within the IDE."
- A callout bubble points to the "Popularity" chart with the text: "Select best component version based on real-time intelligence."
- A callout bubble points to the "Migrate" button with the text: "Migrate to approved version with one click remediation."

Nexus Lifecycle – Reporting

Policy based
bill of materials.

Summary view of
security and license
policy violations.

WebGoat - 2018-11-15 - Build Report

This report provides security and license assessments for identified components found within an application.

SCOPE OF ANALYSIS

**22**

COMPONENTS IDENTIFIED

88% OF ALL COMPONENTS ARE IDENTIFIED

7

POLICY ALERTS

AFFECTING 18 COMPONENTS

2**9****0**GRANDFATHERED
VIOLATIONS

SECURITY ISSUES

How bad are the vulnerabilities and how many are there?

Critical (7-10)

5

Severe (4-6)

6

Moderate (1-3)

1

The summary of security issues
vulnerabilities based on severity
your application.
The dependency depth highlights
distribution within the application

LICENSE ANALYSIS

What type of licenses and how many of each?

Critical (8-10)

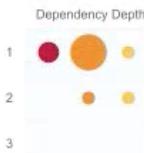
3

Severe (4-7)

11

The summary of license analysis demonstrates
the number of licenses detected in each
category.

The dependency depth compares quantity by
dependency and the distribution within each



WebGoat - 2019-01-17 - Release Report

Summary

Policy Violations

Security Issues

Policy Threat	Component	Popul...	Age	Violations	
				All	Waived
License-None	axis : axis-ant : 1.2	●	13.2 y		
	java2html : j2h : 1.3.1	●	13.0 y		
Security-High	apache-collections : commons-collections : 3.1	●	3.0 y		
	commons-beanutils : commons-beanutils : 1.6	●	13.2 y		
	commons-fileupload : commons-fileupload : 1.2.1	●	11.0 y		
License-Copyleft	javax.mail : mail : 1.4.2	●	8.7 y		
	javax.mail : mailapi : 1.4.2	●	8.7 y		
	org.owasp.webgoat webgoat-container 7.0	●	3.0 y		
Security-Medium	axis : axis : 1.2	●	13.2 y		
License-Non Standard	commons-logging : commons-logging : 1.0.4	●	13.2 y		
Architecture-Quality	axis : axis-jaxrpc : 1.2	●	13.2 y		
	axis : axis-saaj : 1.2	●	13.2 y		
	commons-digester : commons-digester : 1.4.1	●	13.2 y		
	commons-discovery : commons-discovery : 0.2	●	13.2 y		
	commons-io : commons-io : 1.4	●	11.0 y		
	ecs : ecs : 1.4.2	●	13.2 y		
	hsqldb : hsqldb : 1.8.0.10	●	9.7 y		
	javax.activation : activation : 1.1	●	12.7 y		
	javax.transaction : jta : 1.1	●	12.1 y		
	log4j : log4j : 1.2.8	●	14.9 y		
	net.sourceforge.jtds : jtds : 1.2.2	●	11.3 y		
	wsdl4j : wsdl4j : 1.5.1	●	13.1 y		

Nexus Lifecycle – Curated Security Data

Juice Shop - 2019-01-14 - Build Report

Threat Level	Problem Code	Component	Status
9	SONATYPE-2015-0022	jsonwebtoken 0.1.0	Open
	CVE-2018-1000620	cryptiles 3.1.1	Open
8	SONATYPE-2014-0038	shelljs 0.8.1	Open
	SONATYPE-2016-0050	jws 0.2.6	Open
	SONATYPE-2016-0064	angular 1.6.10	Open
7	SONATYPE-2018-0155	base64url 0.0.5	Open
	CVE-2017-1000048	qs 2.3.3	Open
	SONATYPE-2012-0022	express 4.16.2	Open
	SONATYPE-2018-0231	xmlbuilder 8.2.2	Open
	SONATYPE-2017-0422	moment 2.0.0	Open
	SONATYPE-2017-0422	Moment.js 2.0.0	Open
	SONATYPE-2017-0363	timespan 2.3.0	Open
6	SONATYPE-2014-0007	sanitize-html 1.4.2	Open
	SONATYPE-2014-0026	jQuery 1.4.4	Open
	CVE-2018-14042	bootstrap 3.3.7	Open
	CVE-2018-14042	org.webjars bootstrap 3.3.7	Open
	SONATYPE-2018-0436	underscore.string 3.3.4	Open
	CVE-2018-3721	lodash 2.4.2	Open
	SONATYPE-2017-0580	lodash 4.17.10	Open
	SONATYPE-2016-0121	multer 1.3.0	Open
	CVE-2018-3728	hoek 2.16.3	Open
	SONATYPE-2018-0285	mem 1.1.0	Open
	CVE-2018-14042	bootstrap-less 3.3.7	Open
	CVE-2018-3721	SQLi-Me 1.1.0	Open

Proprietary research conducted by world class experts.

WebGoat - 2019-01-17 - Release Report

Policy Threat	Component	Popul...	Age	Release History
License-None	axis : axis-ant : 1.2	●	13.2 y	
	java2html : j2h : 1.3.1	●	13.0 y	
	apache-collections : commons-collections : 3.1	●	3.0 y	
	commons-beanutils : commons-beanutils : 1.6	●	13.2 y	
	commons-fileupload : commons-fileupload : 1.2.1	●	11.0 y	

Detailed metadata makes everyone a security expert.

Nexus Lifecycle – Remediation Guidance

Easy to understand
description written for
developers by developers.

In-depth research
includes detailed
detection and
remediation guidance.

The screenshot shows the Sonatype Nexus Lifecycle interface. At the top, it displays 'Repository results for maven-central' with 'Oldest evaluation 7 months ago'. Key statistics are shown: 738 COMPONENTS IDENTIFIED (green circle), 56 POLICY ALERTS (red), 29 POLICY ALERTS (orange), 2 POLICY ALERTS (yellow), and 50 QUARANTINED COMPONENTS (grey). A modal window is open, titled 'Vulnerability Information', detailing a specific issue:

- Description:** Describes a security flaw involving malicious input to the readValue method of ObjectMapper.
- Explanation:** Explains that jackson-databind is vulnerable to Remote Code Execution (RCE) due to a bug in the createBeanDeserializer() function of BeanDeserializerFactory.
- Note:** Mentions an incomplete fix for CVE-2017-7525.
- Detection:** States the application is vulnerable when default typing is enabled and untrusted data is deserialized.
- Note:** Notes Spring Security has provided their own fix (CVE-2017-4995) for this vulnerability if used with Spring Security 4.2.3.RELEASE or greater for 4.x or Spring Security 5.0.0.M2 or greater for 5.x.
- Recommendation:** Advises there is no non-vulnerable version of the component; it uses a black-list approach.

The interface also includes a 'Component Info' section with a 'Threat Level' dropdown set to '0' and a 'Problem ID' of 'CVE-2017-1'. A 'Policy' section is also visible. On the right, a sidebar shows tabs for 'All', 'Quarantined', and 'Waived', with 'Quarantined' selected. Below the sidebar is a table with four rows, each containing a 'Quarantined' status indicator.

Nexus Lifecycle – Licensing Intelligence

License-Copyleft

com.lowagie : itext : 2.1.7

9.5 y

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

Component Info Policy Similar Occurrences Licenses Vulnerabilities Labels Audit Log

Group: com.lowagie
Artifact: itext
Version: 2.1.7
Declared License: MPL-1.1
Observed License: GPL or MPL-1.1, LGPL-2.1+, BSD-3-Clause, Apache-2.0, MIT, LGPL-2.0+ or MPL-1.1
Effective License: GPL or MPL-1.1, LGPL-2.1+, MPL-1.1, BSD-3-Clause, Apache-2.0, MIT, LGPL-2.0+ or MPL-1.1
Highest Policy Threat: 8 within 2 policies
Highest CVSS Score: NA
Cataloged: 9 years ago
Match State: exact

Popularity

Older This Version Newer

Policy Threat Hide Details

Security License Quality Other

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

Nexus Lifecycle – Dashboard

Filter

Manage ▾

- ▶ Organizations 2 of 6
- ▶ Applications 35 of 36
- ▶ Application Categories 12
- ▶ Stages 4
- ▼ Policy Types
 - all/none
 - Security
 - License
 - Quality
 - Other
- ▼ Violation State 1 of 3
 - all/none
 - Open
 - Waived
 - Grandfathered
- ▶ Policy Threat Level

Apply Revert Clear

Results

! VIOLATIONS 5 COMPONENTS 288 APPLICATIONS

NAME	AFFECTED APPS	TOTAL RISK	Critical	Severe	Moderate	Low	
dom4j commons-collections : commons-collections : 3.2.1	4	36	36	0	0	0	>
commons-collections : commons-collections : ...	3	27	27	0	0	0	>
com.opensymphony : xwork : 2.0.7	1	29	19	7	3	0	>
org.apache.continuum : continuum-webapp : ...	1	29	19	7	3	0	>
org.apache.struts : struts2-core : 2.0.14	1	26	19	7	0	0	>
com.opensymphony : xwork : 2.1.2	1	29	19	7	3	0	>
org.apache.struts : struts2-core : 2.1.6	1	26	19	7	0	0	>
...	1.1.2	2	18	18	0	0	>
...	...	2	32	18	14	0	>
...	...	2	32	18	14	0	>
...	...	2	32	18	14	0	>
...	...	2	18	18	0	0	>

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

Visualize exposure and triage by relative risk.

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.

17	With Security Violations	17	Critical	
10	With License Violations	3	Critical	
18	With Quality Violations	0	Critical	
14	With Other Violations	0	Critical	

Demonstrate risk reduction to senior management.

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**







Questions?

Contact us:

Brian Beard

703-608-4593

bbeard@sonatype.com