sonatype | FINOS

They're in the Room With Us: Assessing Your Open Source Security Efficacy

Brian Fox
Co-founder and CTO
Sonatype

Tosha Ellison
Strategic Advisor
FINOS

Open source components make up

90%

of the modern software application

The average **modern software application** has

180

open source components

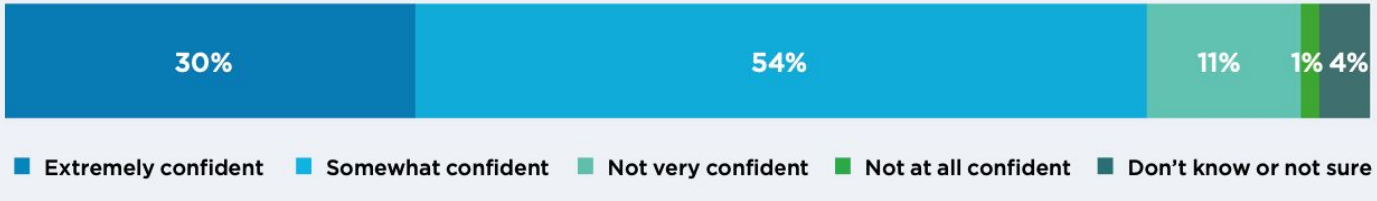
Financial Services See Value in OSS

88% of respondents say that using OSS ***improves software quality*** in their organization.

84% of respondents agree that using OSS ***delivers business value*** to their organization.

Confidence in OSS management is mixed

How confident are you in your organization's ability to control which open source software components are used in a development project? (select one)



How confident are you that the open source components your organization uses are maintained and up to date? (select one)

sonatype

Organizations think they have their software supply chains under control, but the data disagrees

68%

of survey respondents were **confident that their applications are not** using known vulnerable libraries

but in a random sample of enterprise applications…

68%

contained known vulnerabilities

DEPENDENCY CONSUMPTION ANALYSIS

EXPLORING THE STATE OF THE FINANCIAL SERVICES SOFTWARE SUPPLY CHAIN

FINOS Platinum and Gold Member Benefit

Blind spots exist for most organizations when it comes to the enforcement of policies around third-party dependency consumption - whether you know it or not!

The FINOS Dependency Consumption Analysis (DCA) initiative powered by Sonatype provides a comprehensive analysis of your organization's dependency management practices, as observed through your download activity from Maven Central.

https://www.finos.org/dependency-consumption-analysis

sonatype

Market Trends

sonatype

Sonatype the Creators & Stewards of Maven Central

In 2024, developers around the world made more than

1.4 TRILLION

requests from Maven Central.

Statistics as of 1st March 2024

13.2m

component versions stored in ...

43.6TB

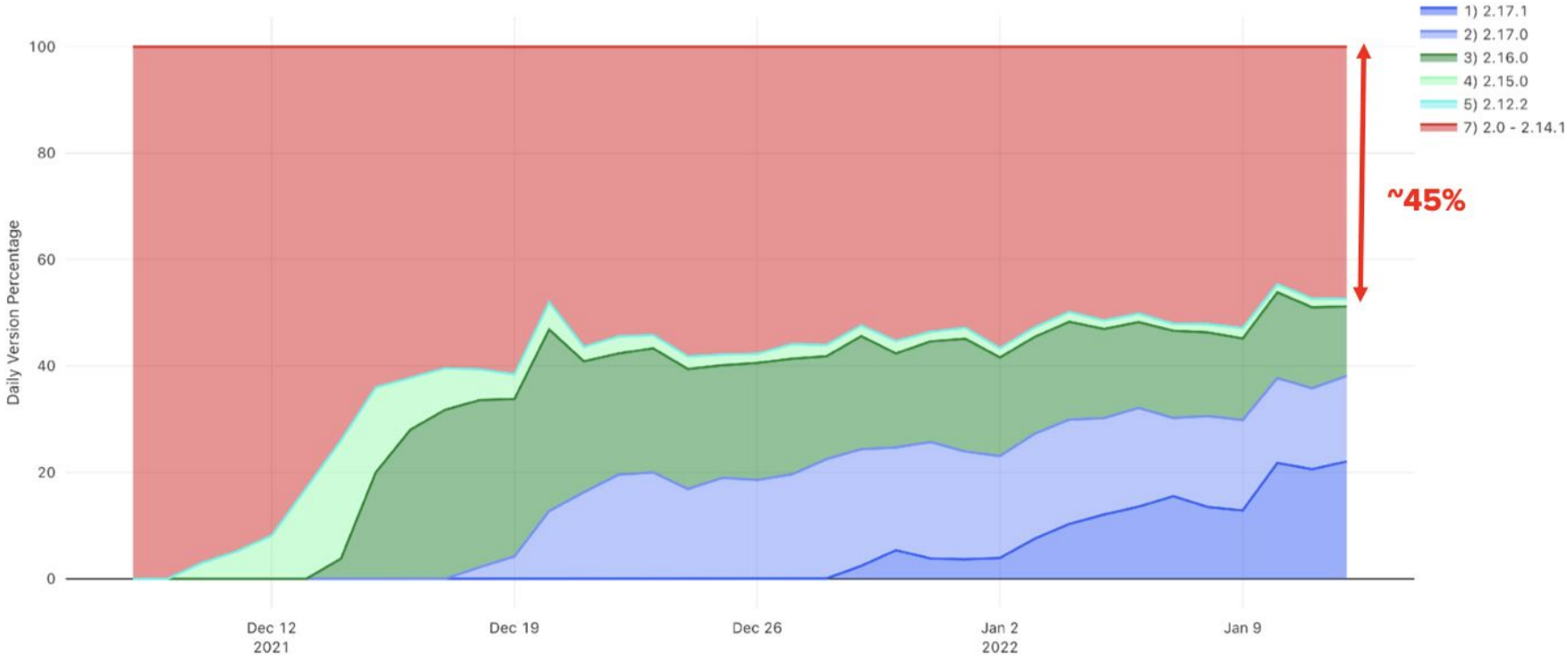
... of files representing approximately ...

84k

... namespaces / organizations / publishers

sonatype

Log4j Download Patterns (Global Downloads)



sonatype

SOFTWARE SUPPLY CHAIN STATISTICS, 2023

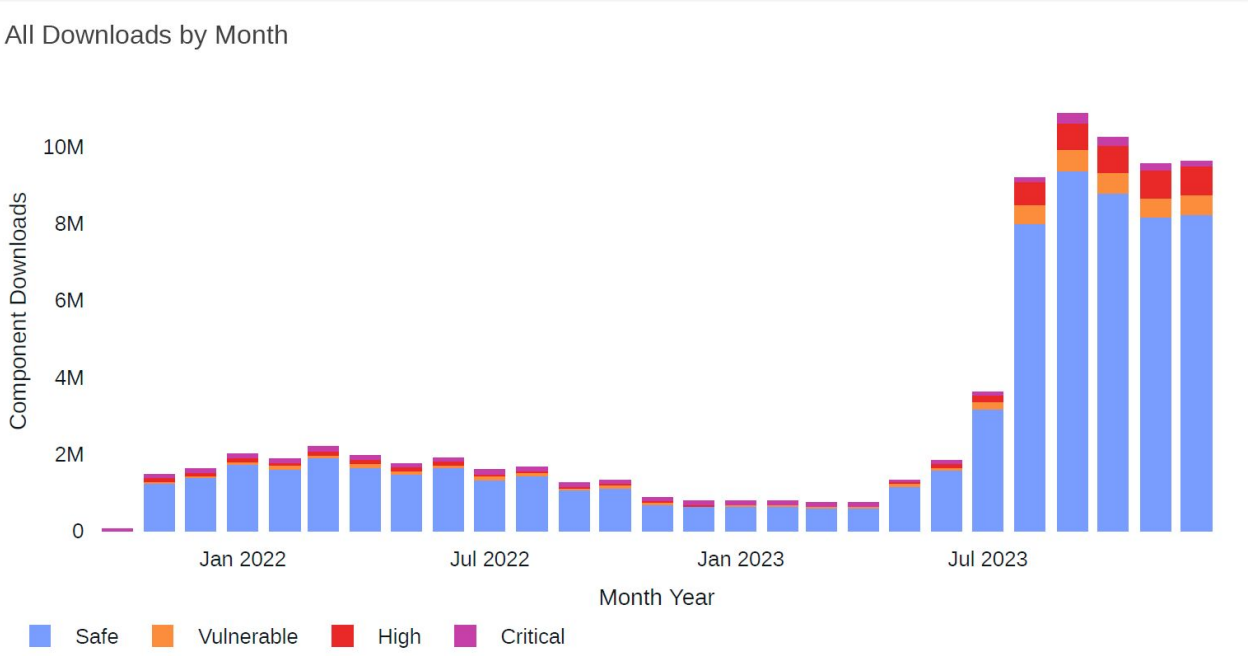
Ecosystem	Total Projects	Total Project Versions	2023 Annual Request Volume Estimate	YoY Project Growth	YoY Download Growth	Average Versions Released per Project
Java (Maven)	557k	12.2M	1.0T	28%	25%	22
JavaScript (npm)	2.5M	37M	2.6T[1]	27%	18%	15
Python (PyPI)	475K	4.8M	261B[2]	28%	31%	10
.NET (NuGet)	367K	6M	162B[3]	28%	43%	17
Total/ Avgs	**3.9M**	**60M**	**4T**	**29%**	**33%**	**15**

1 Figure estimated using npm download counts to from January to August 2023 as queried from https://github.com/npm/registry/blob/master/docs/download-counts.md
2 YoY growth estimated based on known PyPI downloads from January to August 2023 as queried from https://console.cloud.google.com/marketplace/product/gcp-public-data-pypi/
3 YoY growth estimated based on known NuGet Gallery downloads from January to August 2023 as queried from https://www.nuget.org/stats

Maven Central Report for ACME Manufacturing

sonatype

All Downloads mainly from The Desert



Total Downloads:

100,540,786

Monthly Downloads:

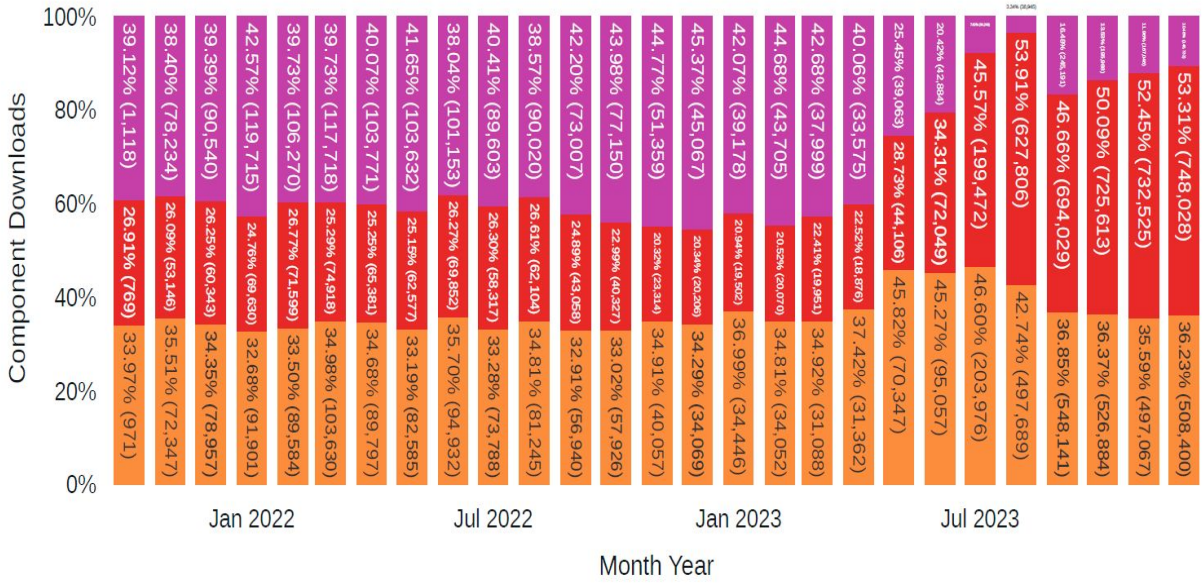
3,866,953

All Downloads via Nexus:

0.95 %

sonatype

All Vulnerable Downloads Only Maven/Java



Total Downloads:

13,950,033

Average: Industry 10-15%

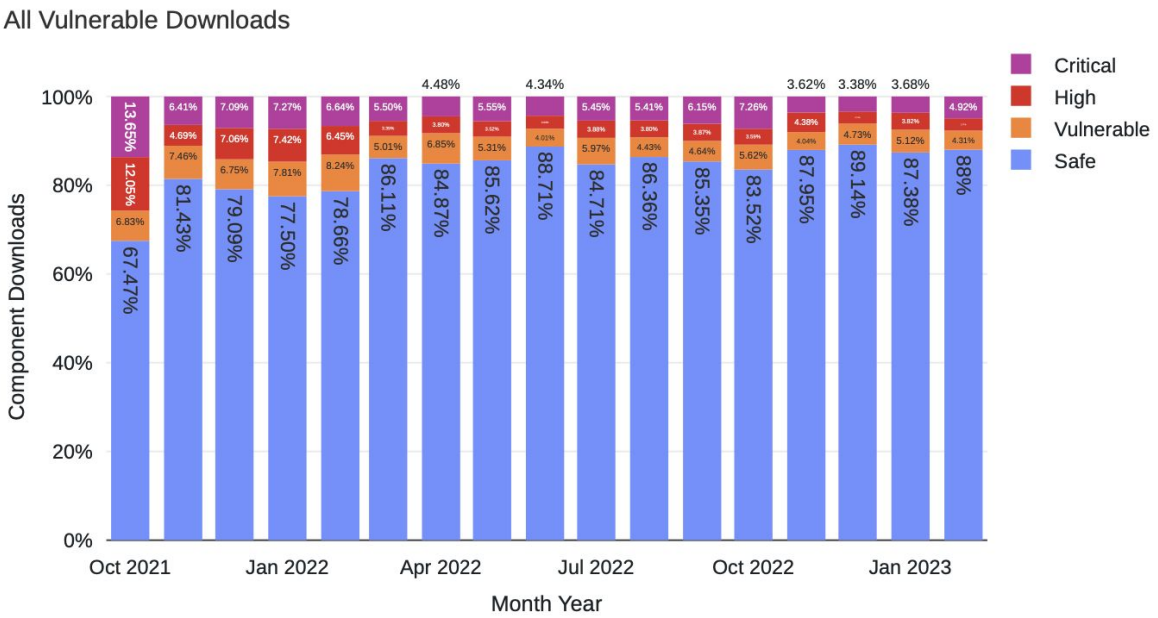
14%

Repo Versions

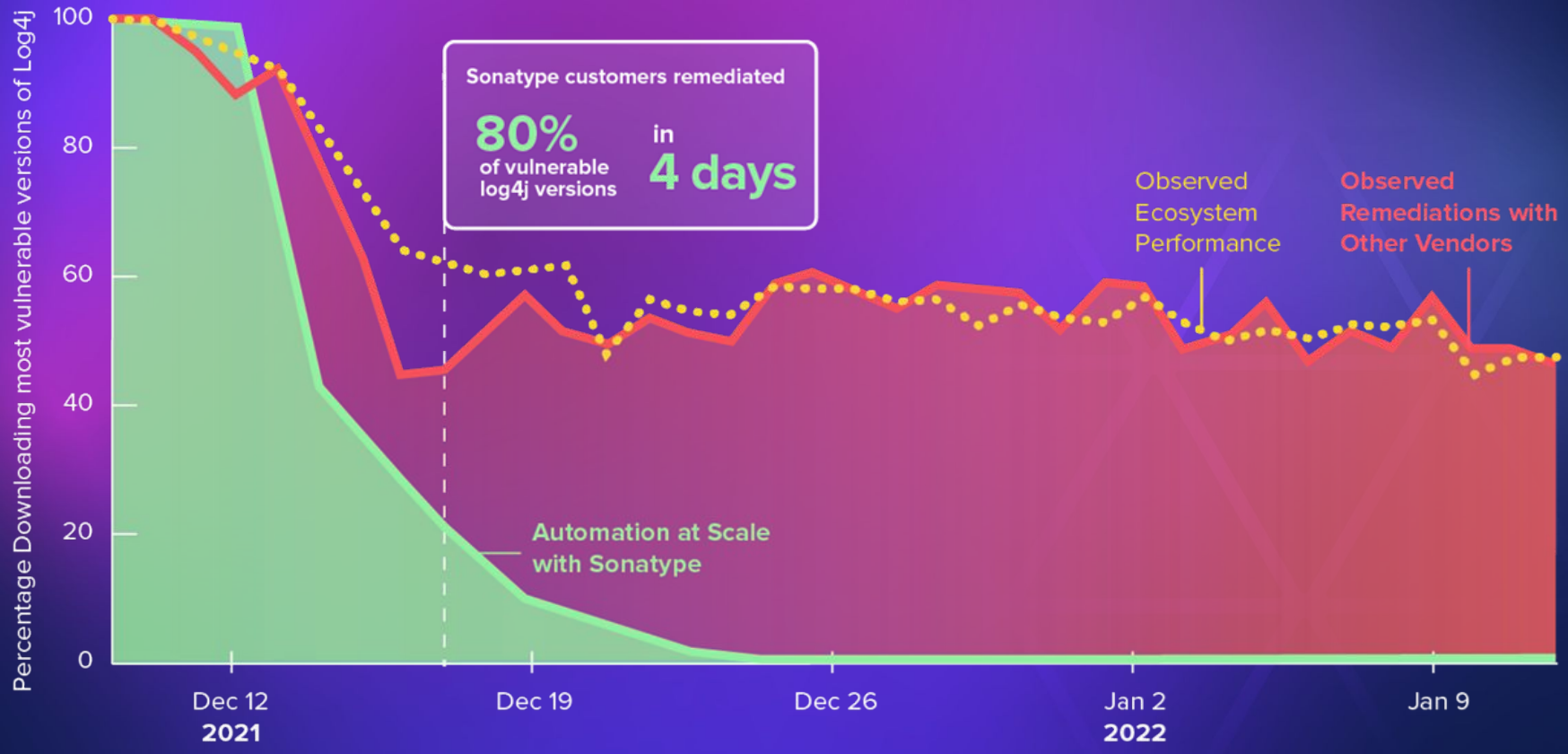
2.14.4-03	3.39.0-01
2.15.1-02	3.38.1-01
2.14.13-01	3.34.0-01

sonatype

Vulnerable Downloads by Month

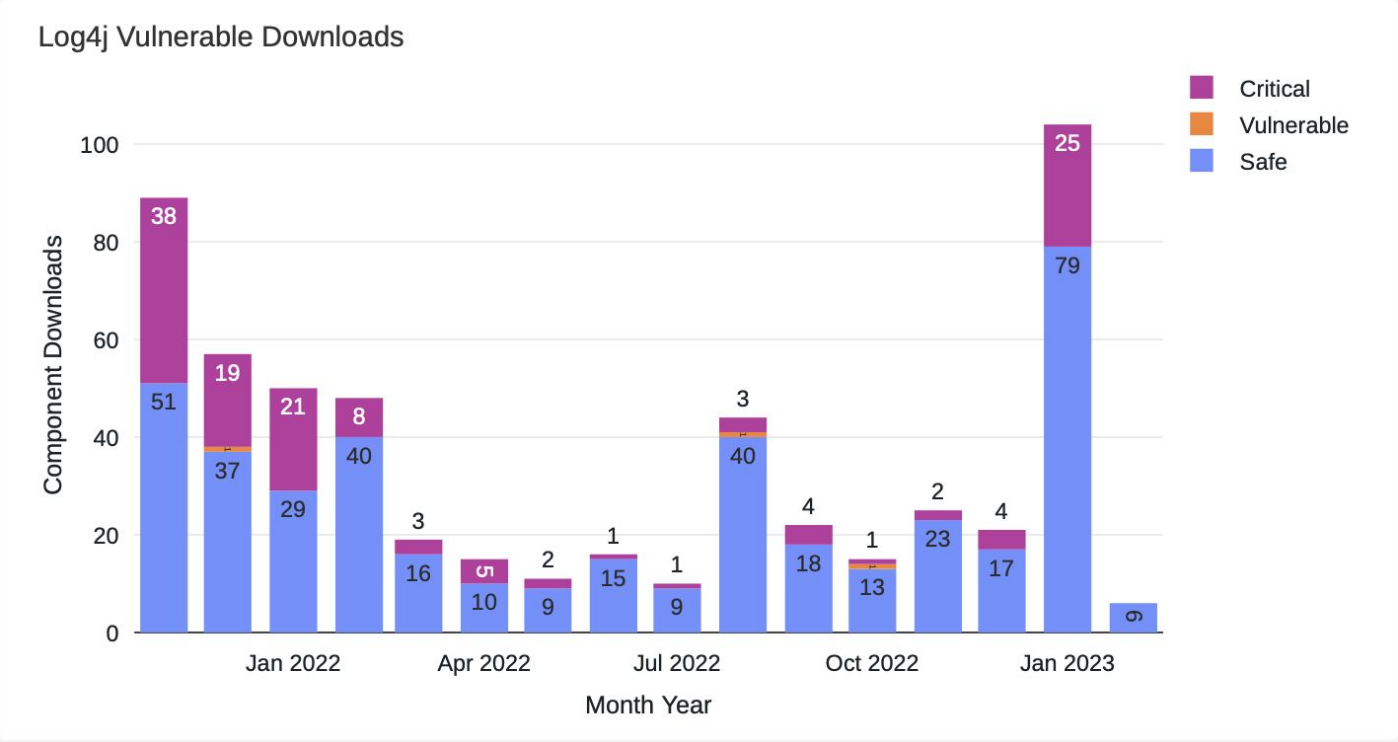


sonatype


Percentage Downloading most vulnerable versions of Log4j
100
80
60
40
20
0
Sonatype customers remediated
80%
of vulnerable log4j versions
in
4 days
Observed Ecosystem Performance
Observed Remediations with Other Vendors
Automation at Scale with Sonatype
Dec 12
2021
Dec 19
Dec 26
Jan 2
2022
Jan 9

sonatype

Downloads of Log4J CVE-2021-44228

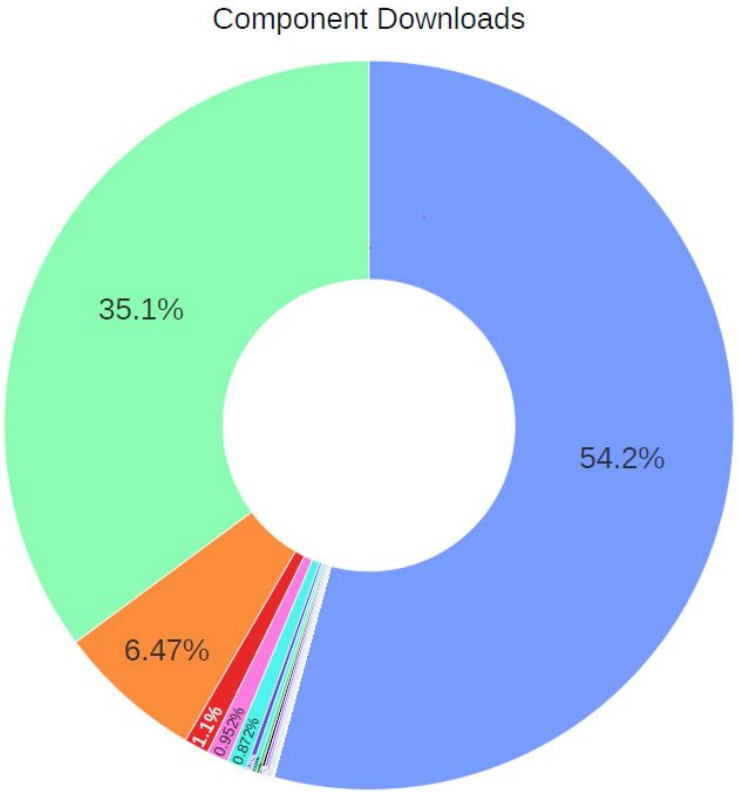


sonatype

Critical Vulnerable Downloads

sonatype

Risk



Top Downloaders:

Gradle and **Apache-Maven**

Log4J Downloads Last 4 Months:

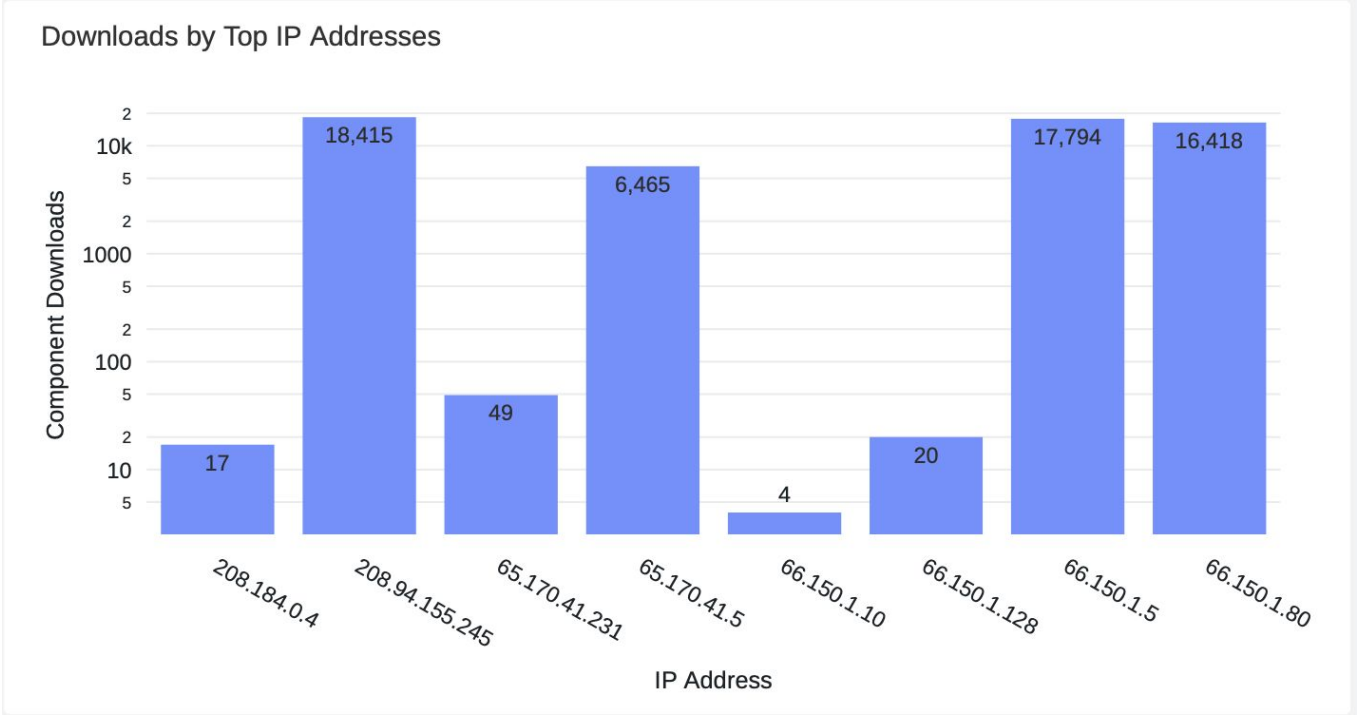
97,313

% of Apache-Maven Log4J Downloads:

91.2%

sonatype

Downloads By IP



sonatype

Interesting Observations

Total Spring4Shell Downloads:

16,587

Total AGPL Downloads:

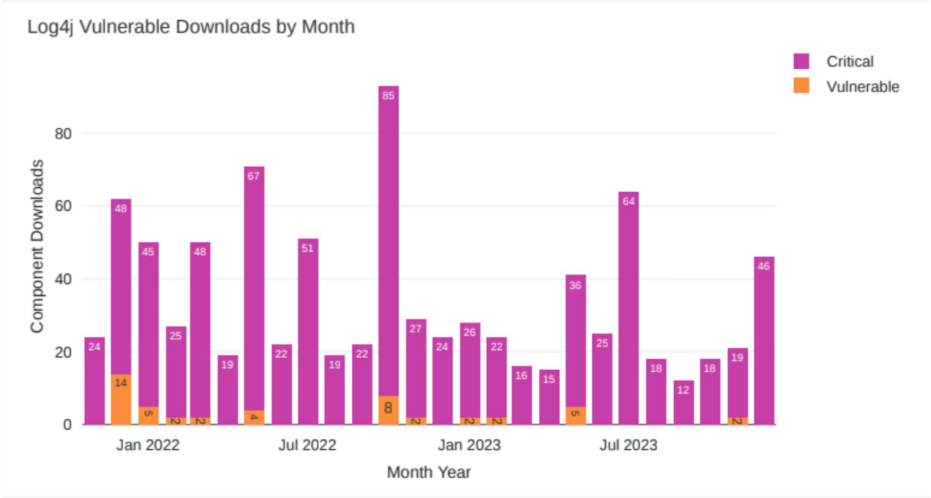
5,434

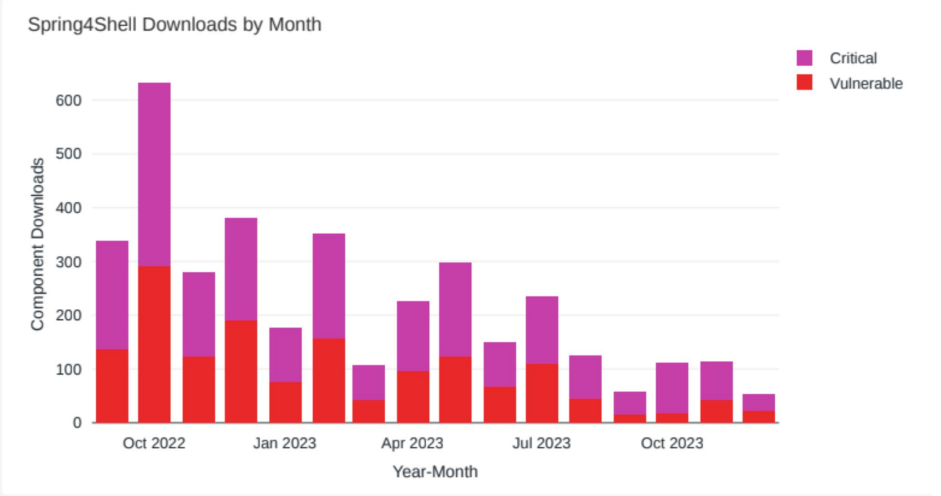
Downloads via unsupported instances:

99.7%

sonatype

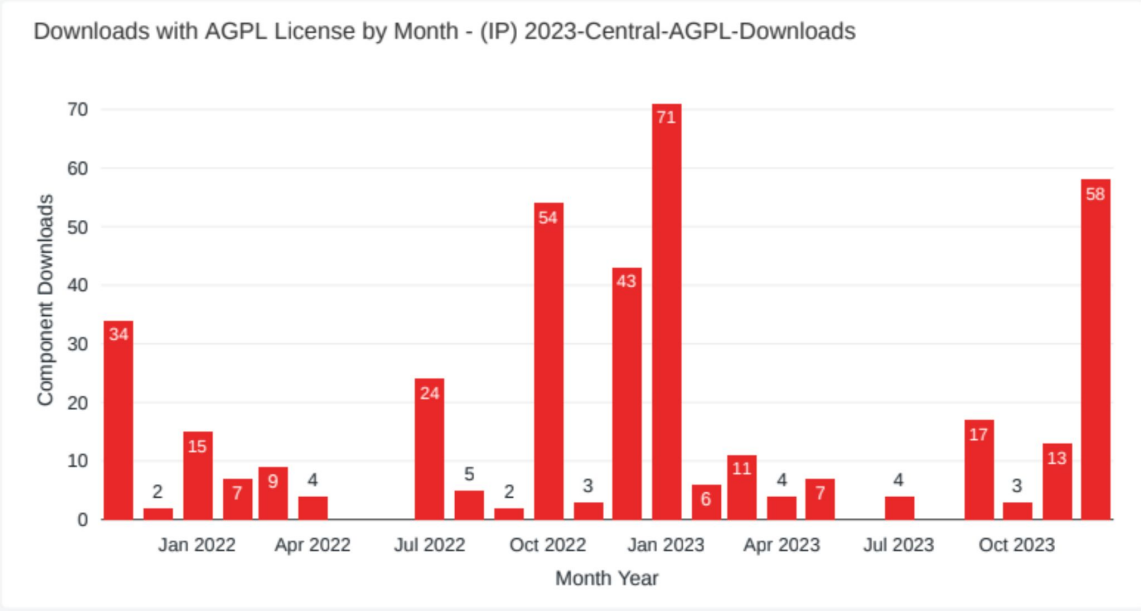
Interesting Observations





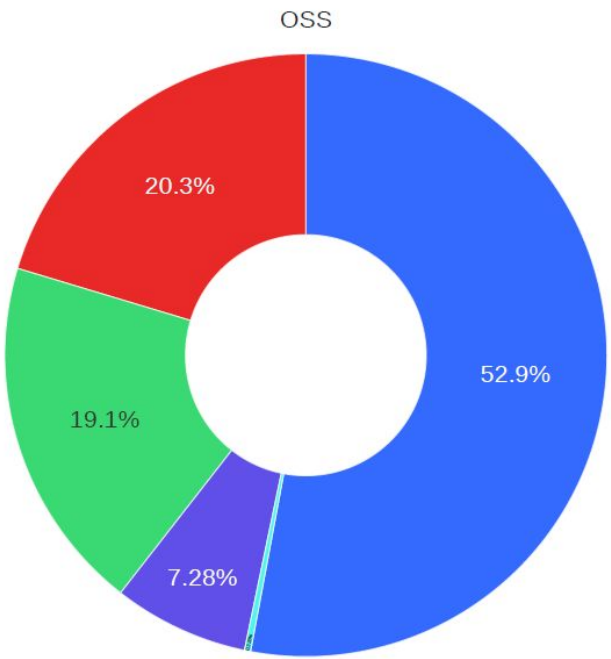
sonatype

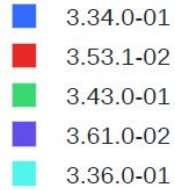
Interesting Observations



sonatype

Starting Observations





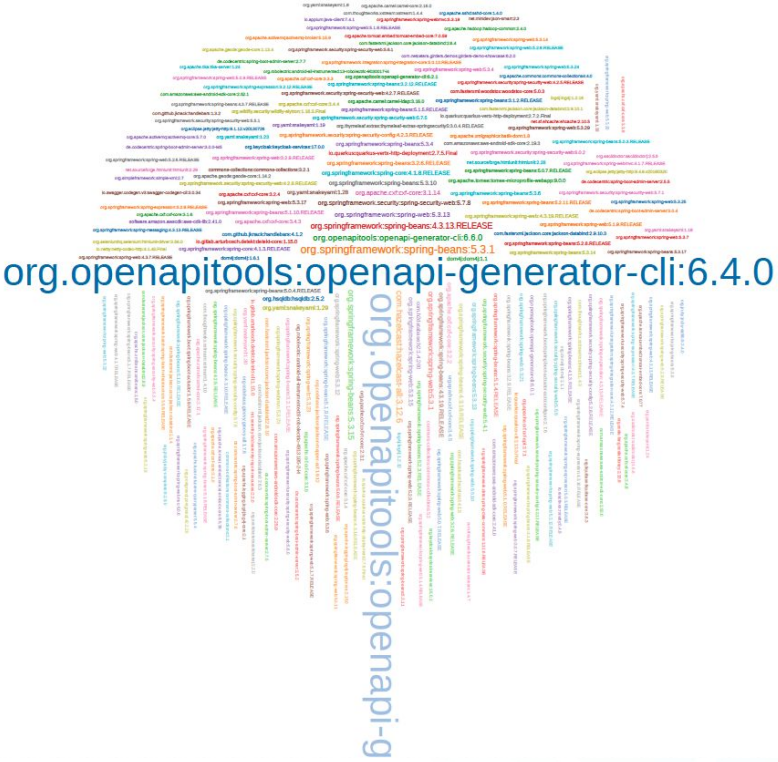
- 3.34 – Sep. 2021
- 3.36 – Oct. 2021
- 3.43 – Nov. 2022
- 3.53 – May 2023
- 3.61 – Oct. 2023

Current Version
3.65 – Feb. 2024

sonatype

What we saw

- Components 5+years old
- Multiple versions of same component
- Log4j-Core 1.2.16



sonatype

Landscape of OSS Supply Chain Attacks

sonatype

In less than 12 months Sonatype discovered **350,000+ suspicious & malicious** packages.

POISONING THE WELL —

A new type of supply-chain attack with serious consequences is flourishing

New dependency confusion attacks take aim at Microsoft, Amazon, Slack, Lyft, and Zillow.

New Linux, macOS malware hidden in fake Browserify NPM package

Discord-Stealing Malware Invades npm Packages

Organizations are protecting themselves from next-gen attacks with predictive security.

sonatype

AI-Powered Software Supply Chain Security

Sonatype Repository Firewall

Avoid costly supply chain attacks

Stop known vulnerabilities from being downloaded

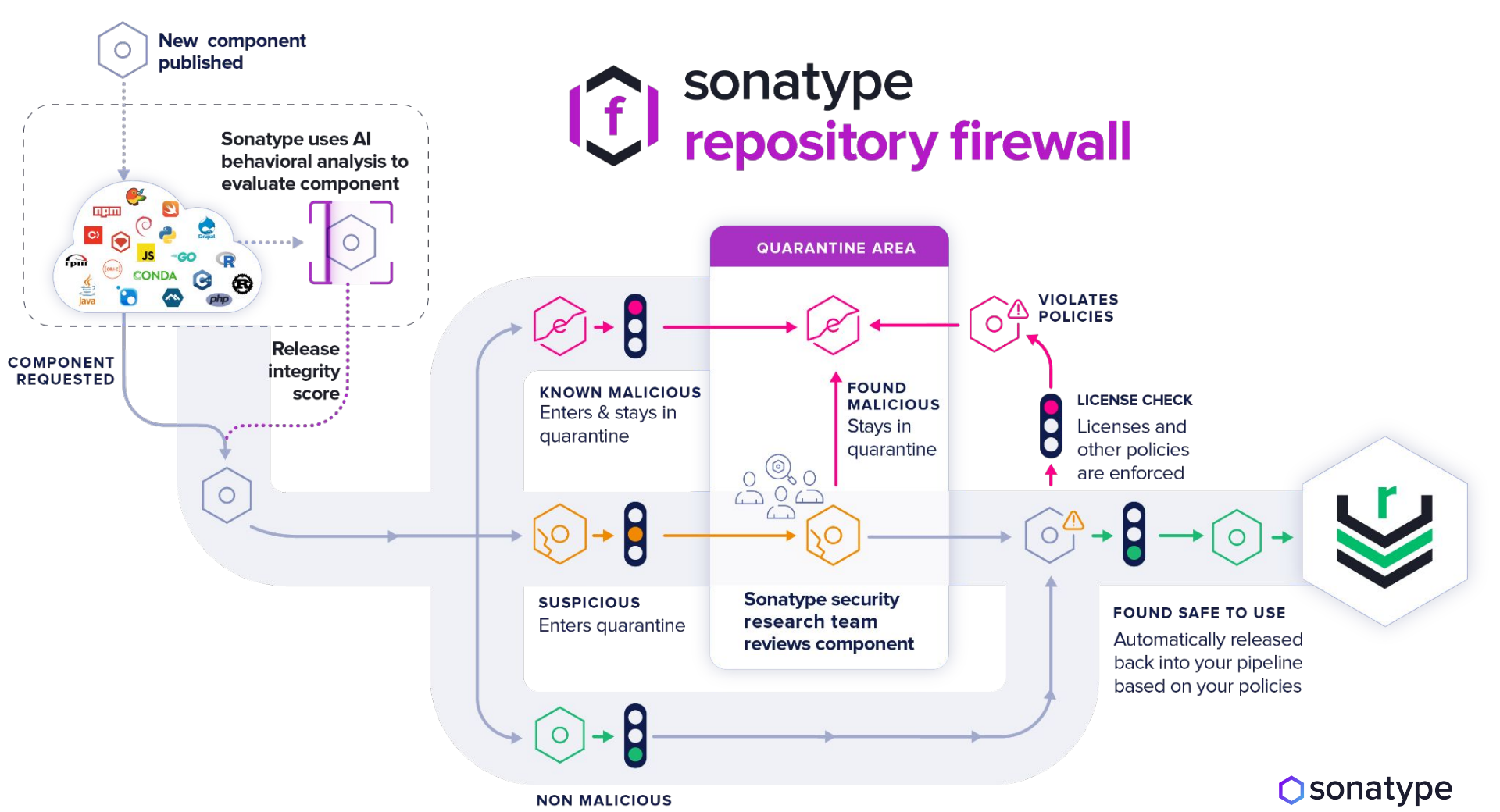
Predict zero-day and suspicious components

Happier developers

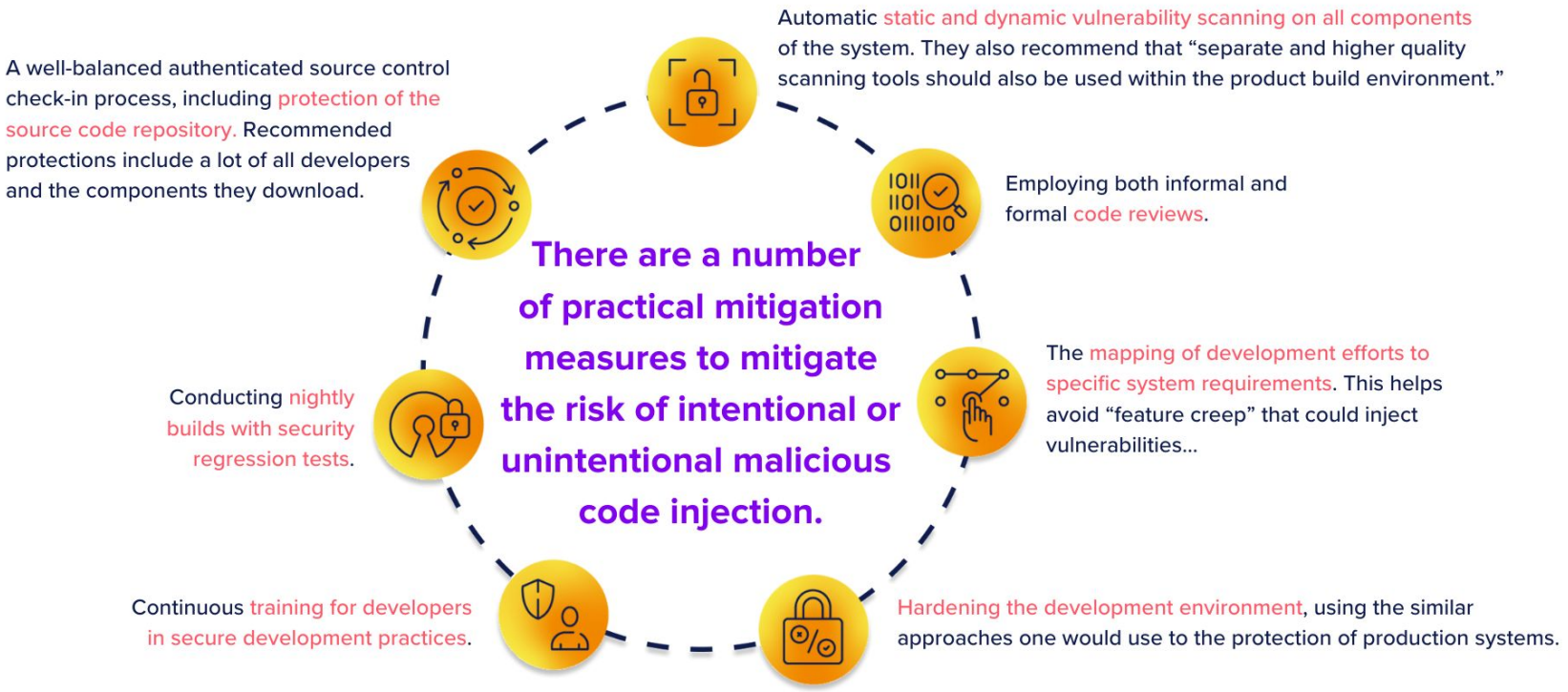
Understand why a component was blocked

Remediation and replacement guidance

sonatype


New component published
Sonatype uses AI behavioral analysis to evaluate component
COMPONENT REQUESTED
Release integrity score
sonatype
repository firewall
QUARANTINE AREA
VIOLATES POLICIES
KNOWN MALICIOUS
Enters & stays in quarantine
FOUND MALICIOUS
Stays in quarantine
LICENSE CHECK
Licenses and other policies are enforced
SUSPICIOUS
Enters quarantine
Sonatype security research team reviews component
FOUND SAFE TO USE
Automatically released back into your pipeline based on your policies
NON MALICIOUS
sonatype

Guidance for Developers



Source: Securing the Software Supply Chain: Recommended Practices Guide for Developers.

Call To Action

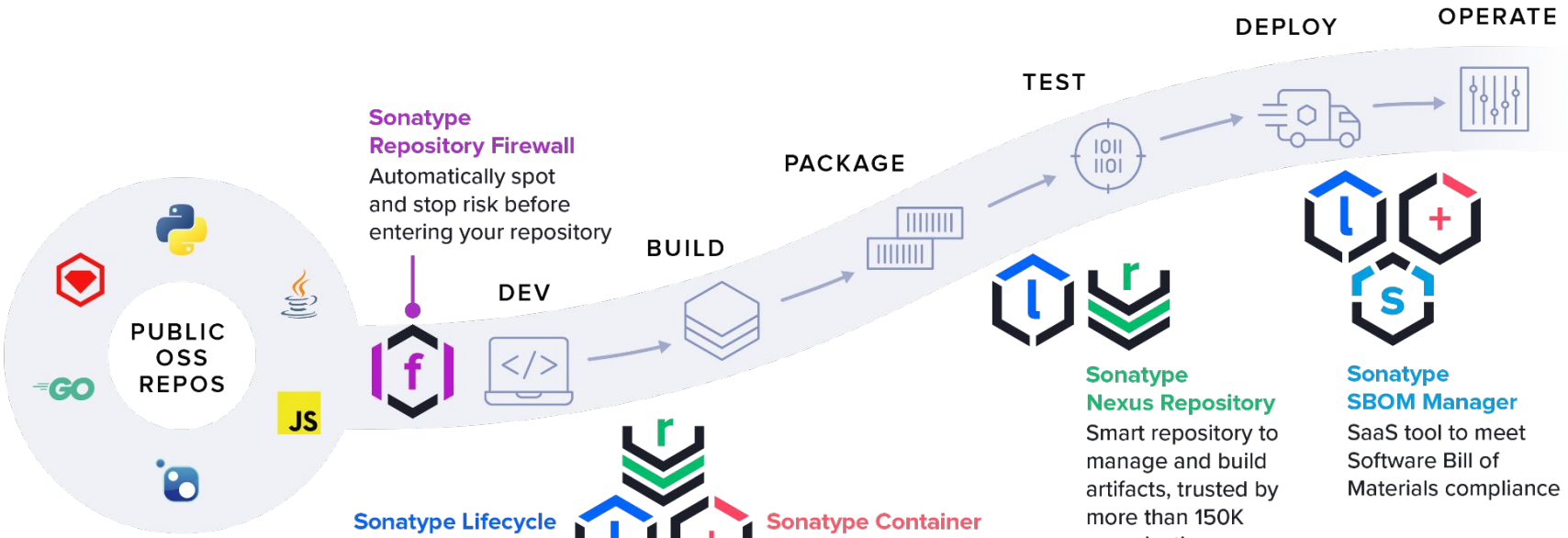
Today ACME Manufacturing are exposing themselves to a large amount of risk through multiple entry points into their SDLC. This problem can often be 10x for other ecosystems such NPM and PyPi as our report only describes the view from Maven Central.

1. Move to a central artifacts management system for proxy and build stages of SDLC. This will improve efficiency of build by not always fetching from public repo.
2. Reduce Technical Debt caused by old components, eg. 5+ years old
3. Eliminate the risk of malicious components entering the CI/CD pipeline from public repositories.
4. Configure and enable policies across the SDLC “cradle to grave”
5. Get control over downloads through your build systems, eg. Apache-Maven
6. Improve your position with ISO 27001 compliance audits
7. Reduce your vulnerable downloads from 11% to 0%.

SCA for FINOS

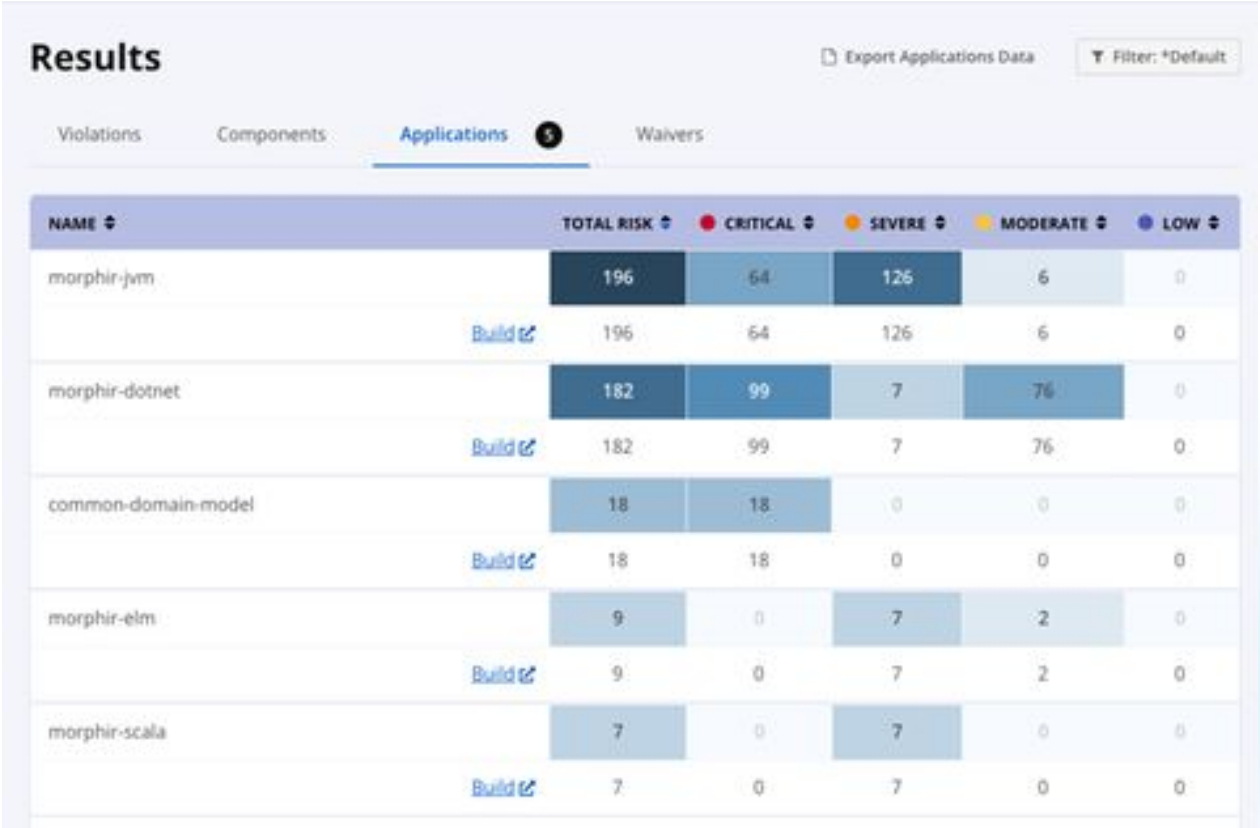
sonatype

Superior open source data service continuously refined by AI, machine learning, and world-class researchers powers our products.



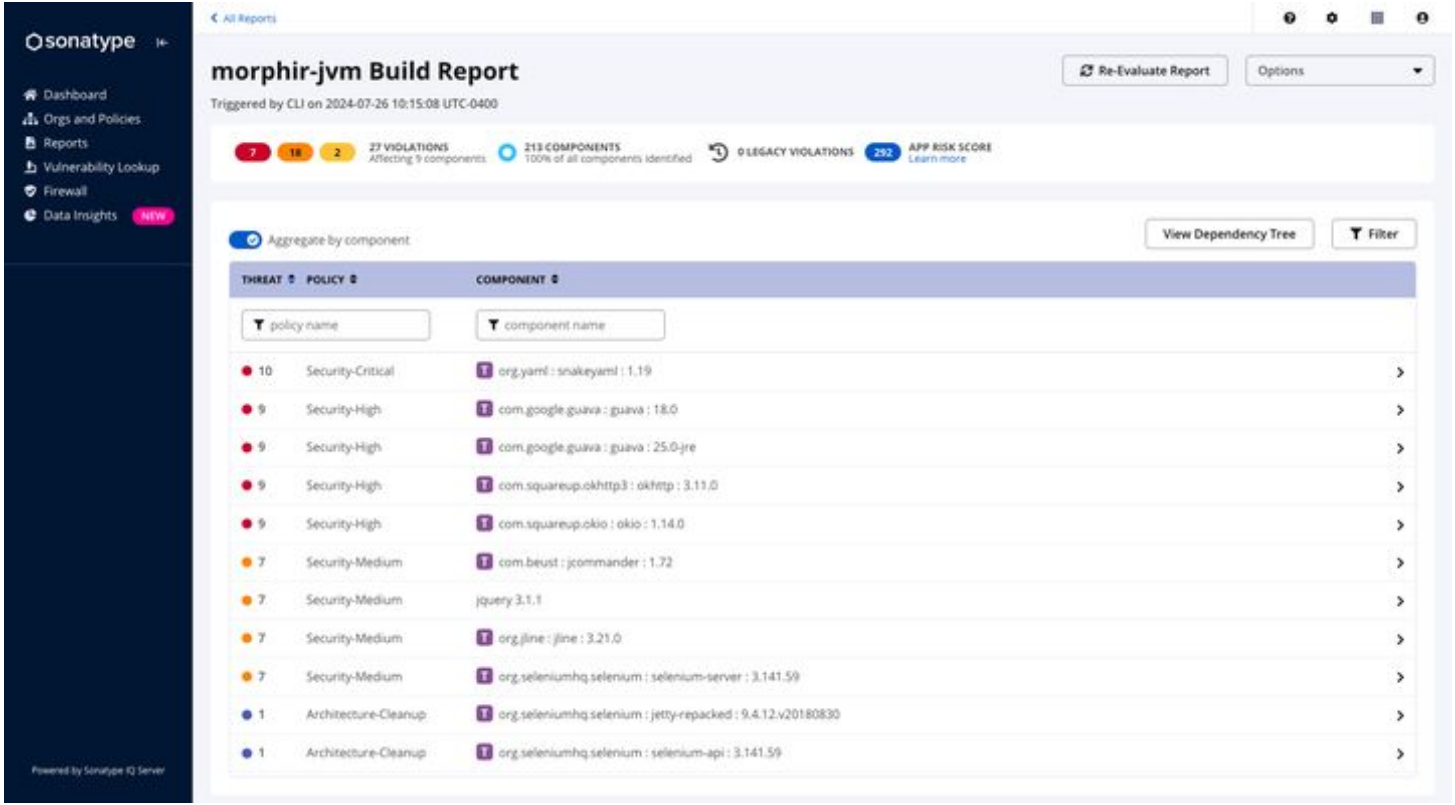
sonatype

Overview



sonatype

Report


sonatype
Dashboard
Orgs and Policies
Reports
Vulnerability Lookup
Firewall
Data Insights
NEW
Powered by Sonatype IQ Server
All Reports
morphir-jvm Build Report
Triggered by CLI on 2024-07-26 10:15:08 UTC-0400
Re-Evaluate Report
Options
7
18
2
27 VIOLATIONS
Affecting 9 components
213 COMPONENTS
100% of all components identified
0 LEGACY VIOLATIONS
292
APP RISK SCORE
Learn more
Aggregate by component
View Dependency Tree
Filter
THREAT
POLICY
COMPONENT
policy name
component name
10 Security-Critical org.yaml : snakeyaml : 1.19
9 Security-High com.google.guava : guava : 18.0
9 Security-High com.google.guava : guava : 25.0-jre
9 Security-High com.squareup.okhttp3 : okhttp : 3.11.0
9 Security-High com.squareup.okio : okio : 1.14.0
7 Security-Medium com.beust : jcommander : 1.72
7 Security-Medium jquery 3.1.1
7 Security-Medium org.jline : jline : 3.21.0
7 Security-Medium org.seleniumhq.selenium : selenium-server : 3.141.59
1 Architecture-Cleanup org.seleniumhq.selenium : jetty-repacked : 9.4.12.v20180830
1 Architecture-Cleanup org.seleniumhq.selenium : selenium-api : 3.141.59

Questions?