Sonatype

2013 SONATYPE SURVEY FINDINGS

The Component Lifecycle Management Company

OUR WORLD RUNS ON SOFTWARE, AND **SOFTWARE RUNS ON OPEN SOURCE COMPONENTS**. EVERY YEAR, WE ASK THOSE ON THE FRONT LINES—DEVELOPERS, ARCHITECTS, AND MANAGERS, ABOUT HOW THEY'RE USING COMPONENTS, AND HOW THEY'RE BALANCING THE NEED FOR SPEED WITH THE NEED FOR SECURITY.

THIS YEAR

3,500

PEOPLE PROVIDED THEIR VIEWS

Who took the survey?

Just some of the organizations represented

NETFLIX
HSBC
Disney
Adobe
FedEx
SIEMENS
Goldman Sachs
facebook
BARCLAYS
THOMSON REUTERS
Alcatel·Lucent
LinkedIn
ebay
JPMorgan Chase & Co.
Deutsche Bank
GE
RSA SECURITY

85% OF THE RESPONSES CAME FROM DEVELOPERS, MANAGERS AND ARCHITECTS

25% OF THE RESPONDANTS HAVE

MORE THAN

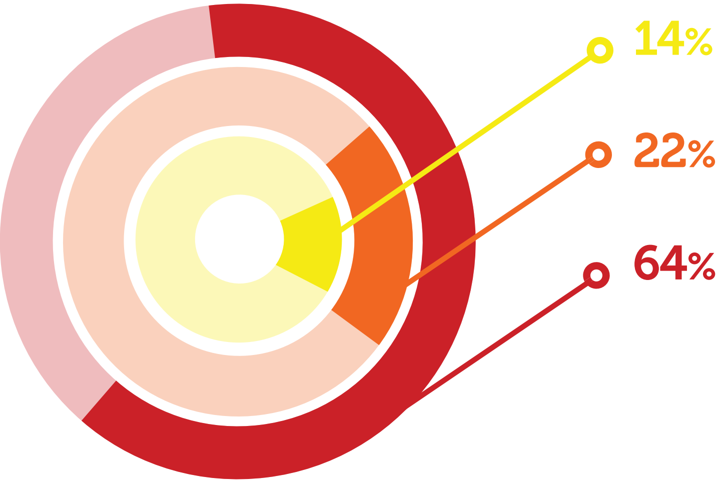
500 DEVELOPERS

IN THEIR ORGANIZATION

> 50 COUNTRIES, CONCENTRATION US/EMEA

At least 80% of a typical java application is assembled from open source components and frameworks.

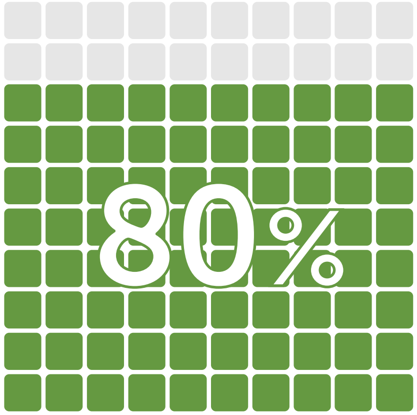
Question: Would it surprise you to know that 80% of a typical Java application is now assembled from open source components and frameworks?



14% Believe that 80% seems a bit high

22% Feel that 80% seems a bit low

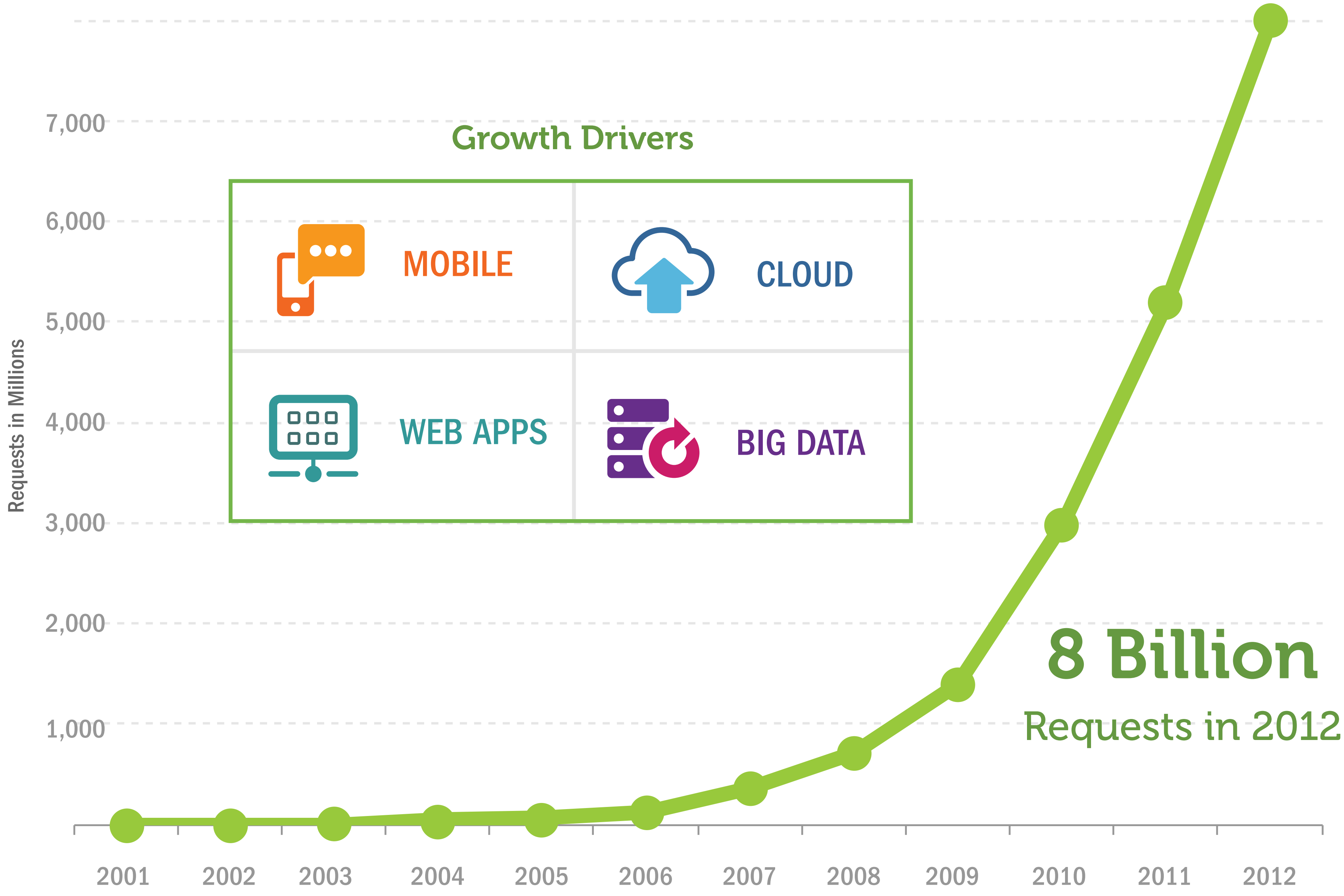
64% Think that 80% seems about right



Yes, It’s True!

Many of the applications you use today are now assembled from hundreds of open source components.

Component downloads from the Central Repository have exploded.



Growth Drivers

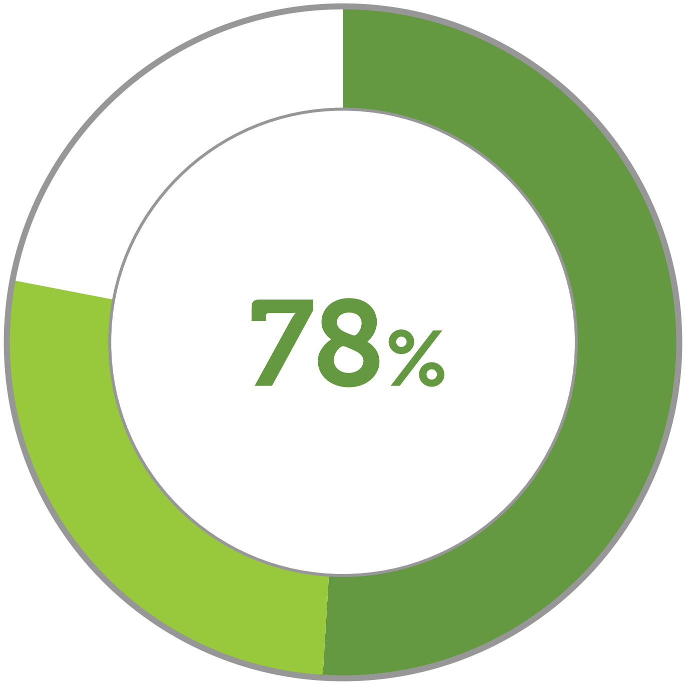
MOBILE	CLOUD
WEB APPS	BIG DATA

8 Billion

Requests in 2012

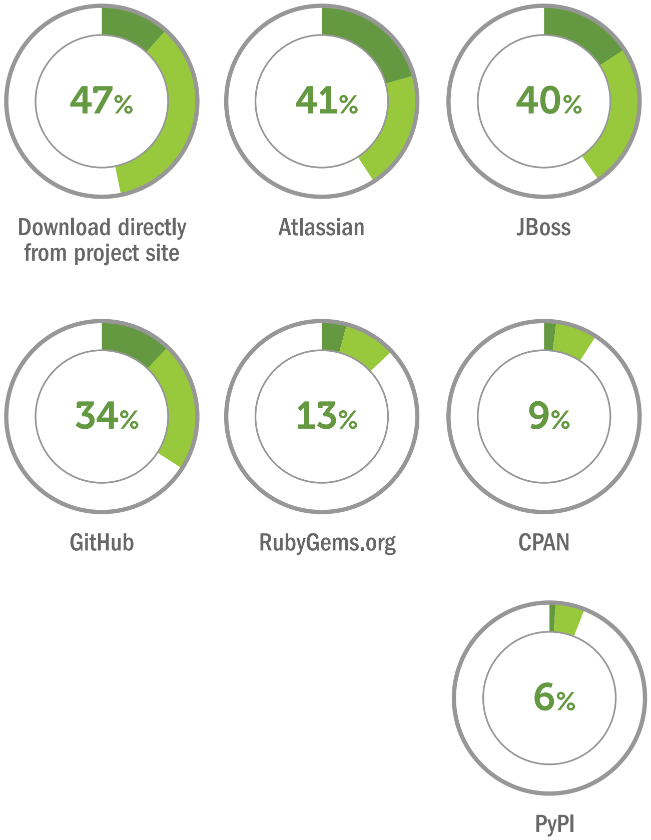
Nearly 80% of organizations report that the components of The Central Repository (Maven Central) are important to their development efforts.

Question: For your organization, please rate the following sources of open source components. (Percentage reporting critical and important.)



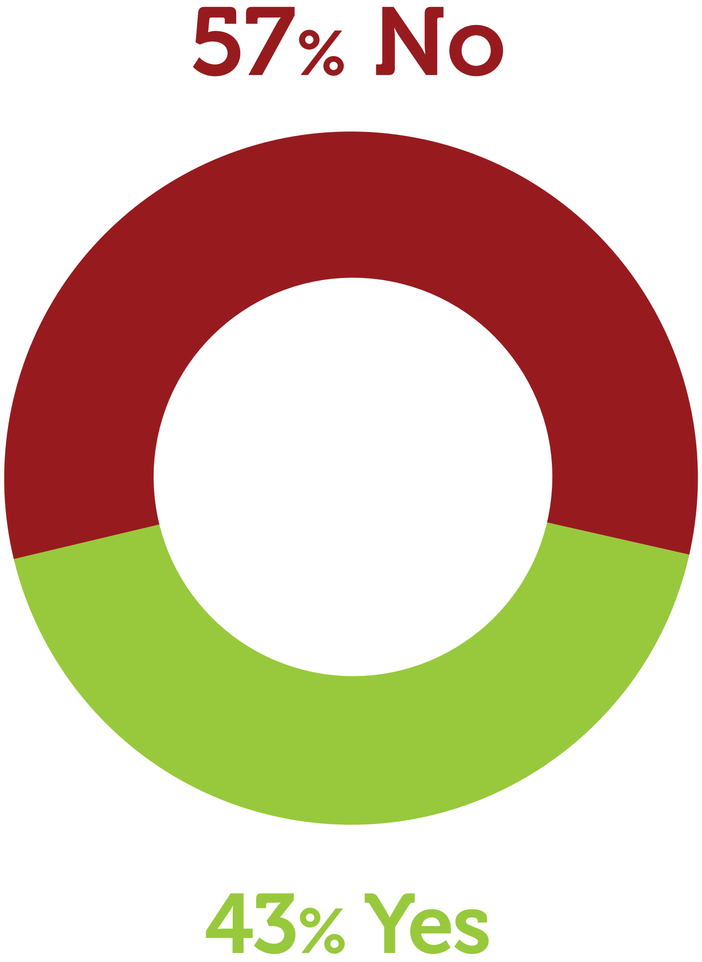
The Central Repository (Maven Central)

This is nearly double the popularity of any other source of components.



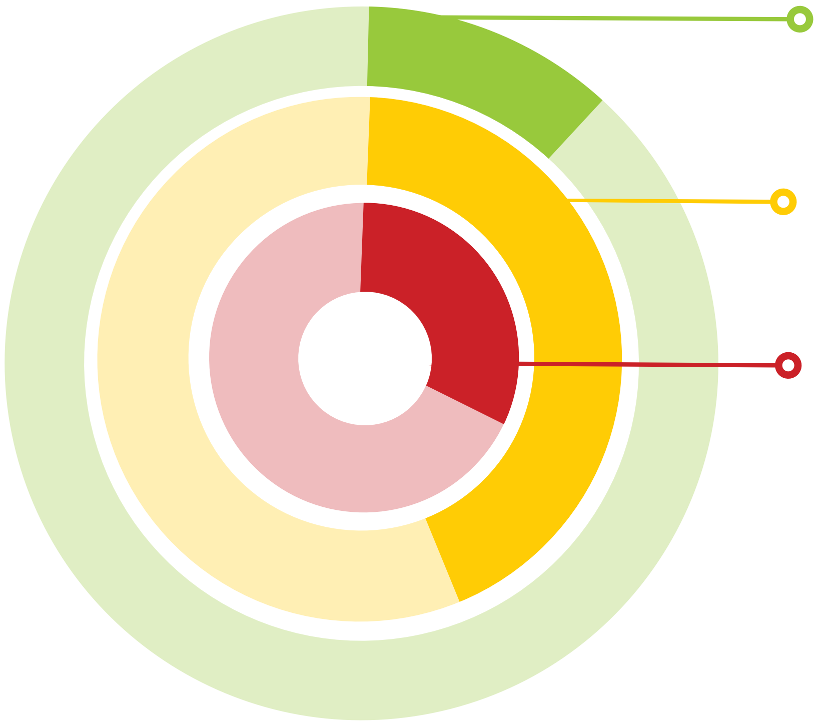
Even given all this usage, 57% of organizations lack any policy governing open source usage.

Question: Does your company have an open source policy?



76% of Organizations Lack Meaningful Controls Over their Open Source Usage

Question: How well does your organization control which components are used in software development projects?



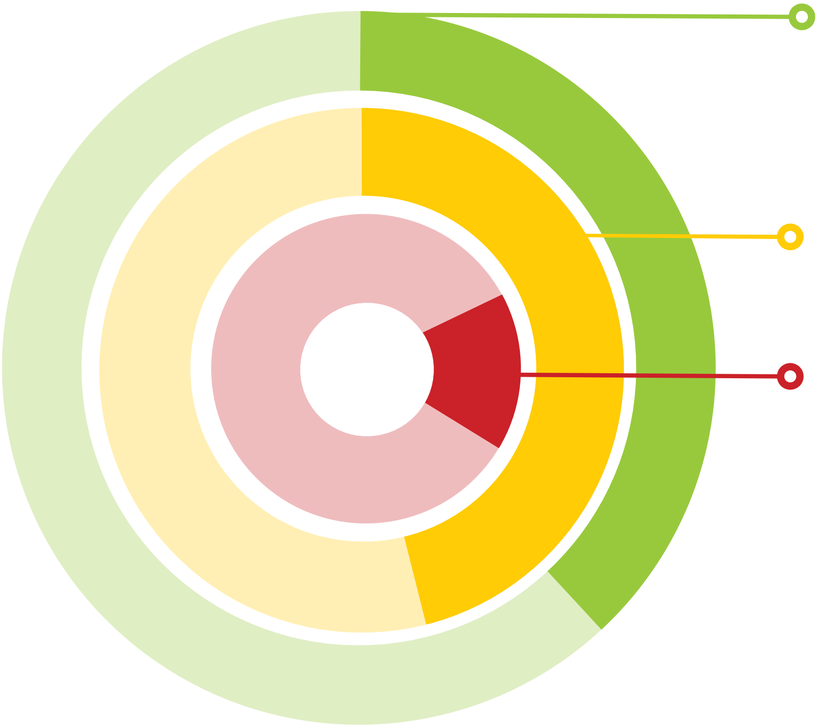
24% We're completely locked down.
We can only use approved components.

44% Yes, We have some corporate standards,
but they aren't enforced

32% There are no standards.
Each developer or team chooses the
components that are best for their project.

Even if they have a policy, only 38% of organizations have control over what components are used in their applications.

Question: How well does your organization control which components are used in software development projects?



38% We're completely locked down.
We can only use approved components.

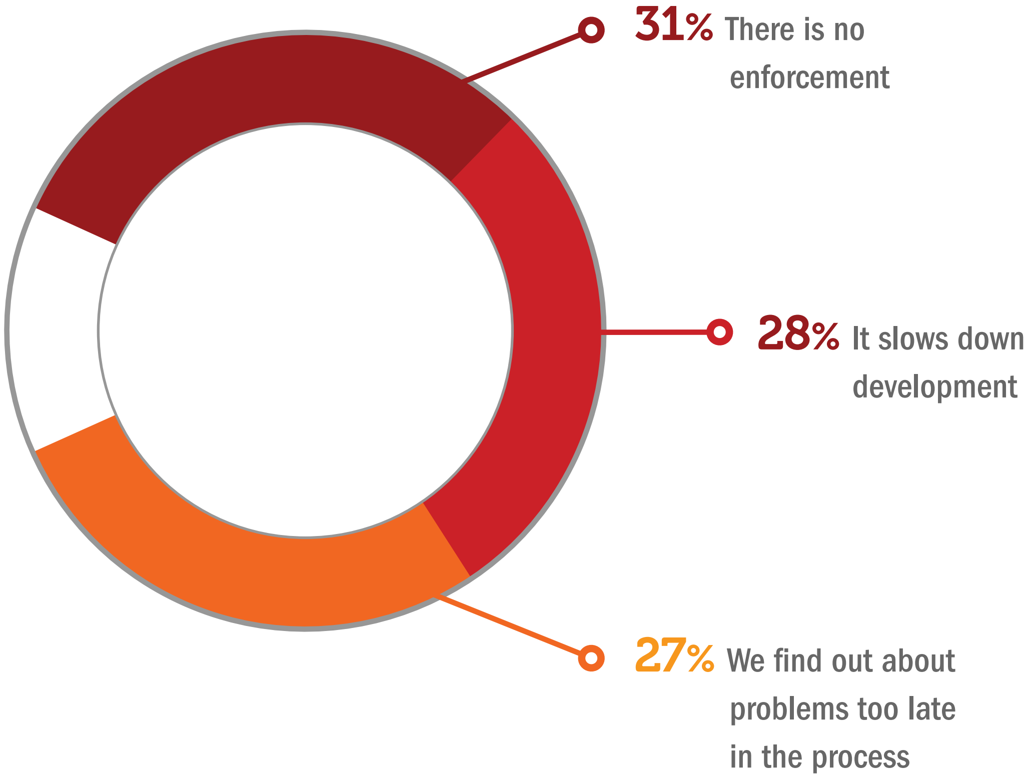
Last year: 33%

46% Yes, We have some corporate standards, but they aren't enforced

16% There are no standards.
Each developer or team chooses the components that are best for their project.

Open source policies are not only unenforced, they get in the way.

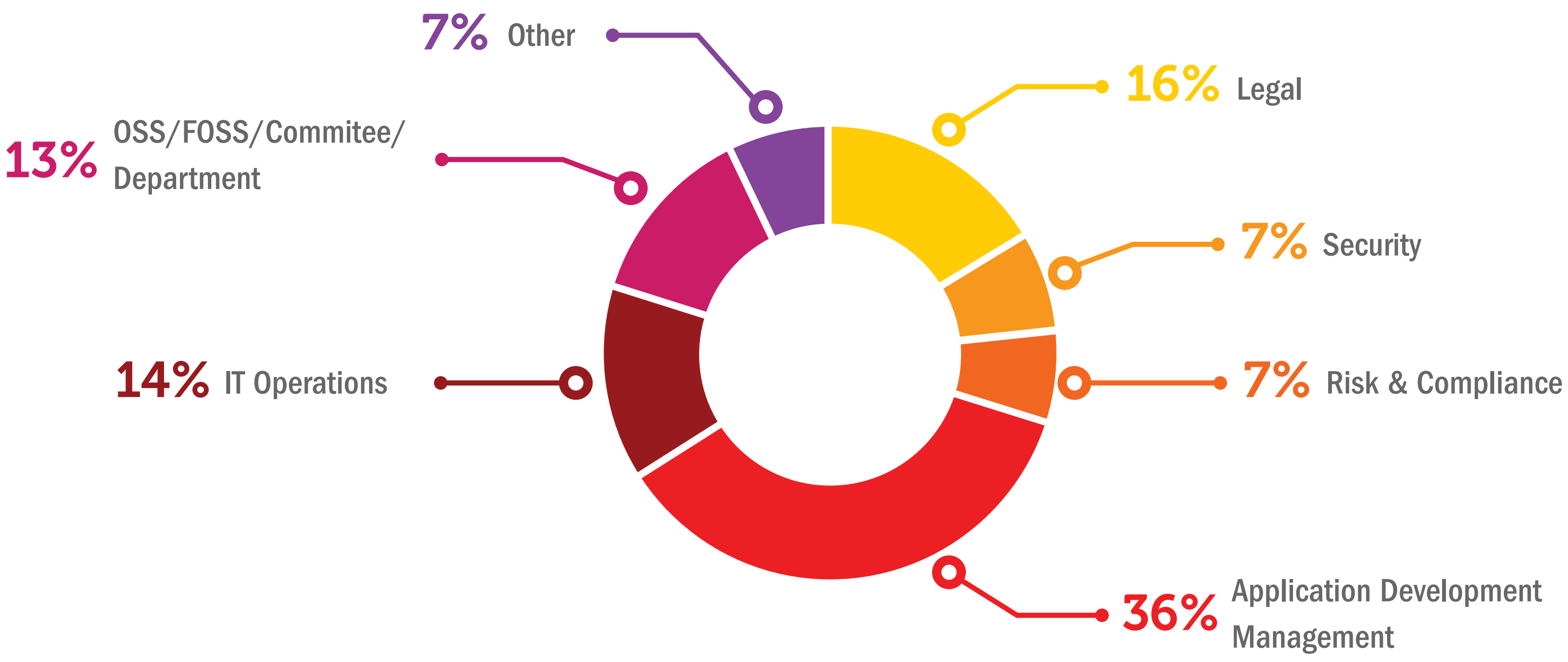
Question: What are the biggest challenges with your open source policy?



> *"There is insufficient information to definitively determine compliance."*
>
> *"A lot of the rules are loose and it's easy to get lazy about stuff."*
>
> *"The people making the policy have no development or technical skills."*
>
> *"Good security design means slower development."*

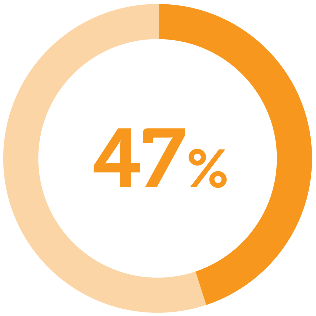
No one and everyone is responsible for open source policy.

Question: Who in your organization has primary responsibility for open source policy/governance?

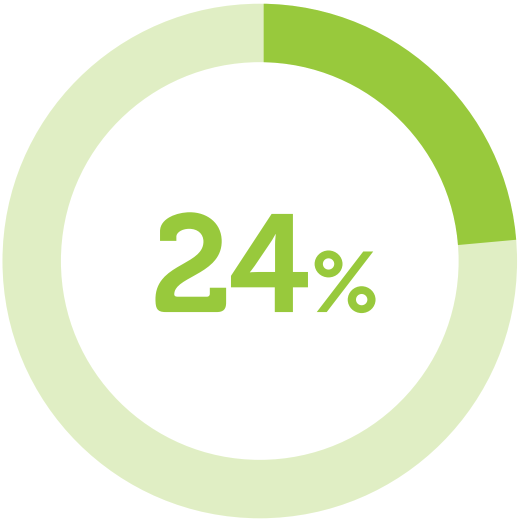


Even organizations with an open source policy are doing little to prevent security vulnerabilities from creeping in.

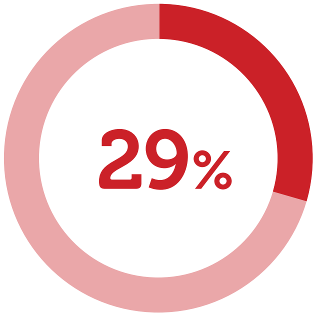
Question: How does your open source policy address security vulnerabilities?



OUR POLICY SAYS THAT WE MUST AVOID KNOWN VULNERABILITIES



WE MUST PROVE THAT WE ARE NOT USING COMPONENTS WITH KNOWN VULNERABILITIES

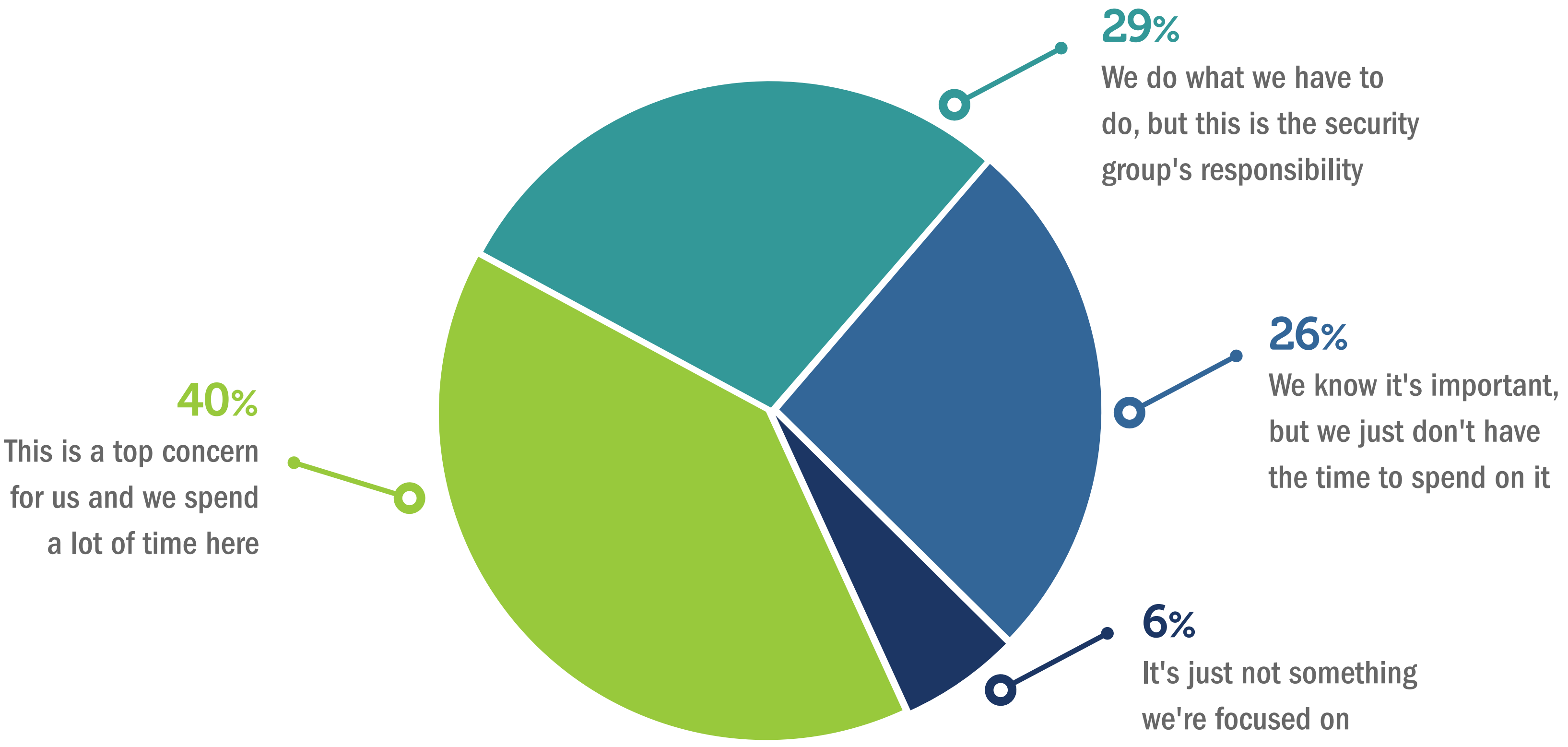


OUR POLICY DOES NOT ADDRESS SECURITY VULNERABILITIES

Only 1 in 4 organizations must prove they're not using components with known vulnerabilites.

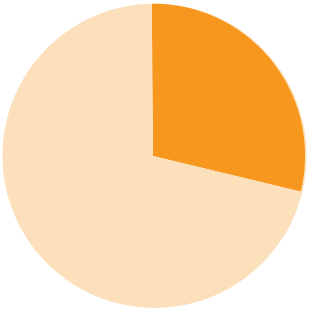
Forget about policy, developers just aren't that interested in security. More than 60% of developers don't spend much time in this area.

Question: How would you characterize your developers' interest in application security?



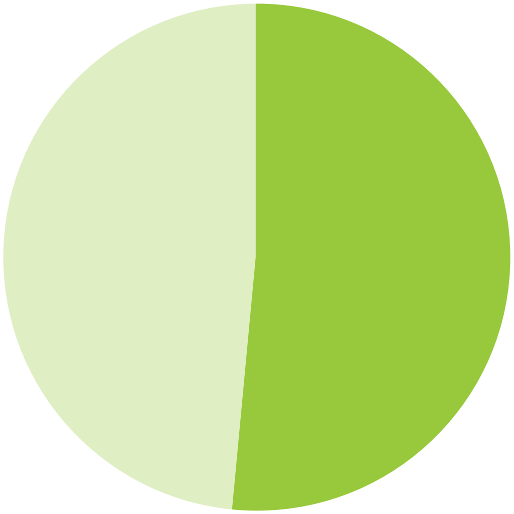
We're a little better at licensing, but still not very good.

Question: Does your policy restrict component usage based on specific licenses or license types?



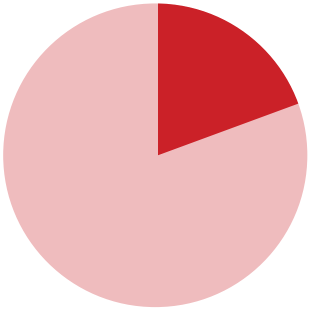
29%

Yes and we examine every component but *not* its dependencies



51%

Yes and and we examine every component and *all* of its dependencies

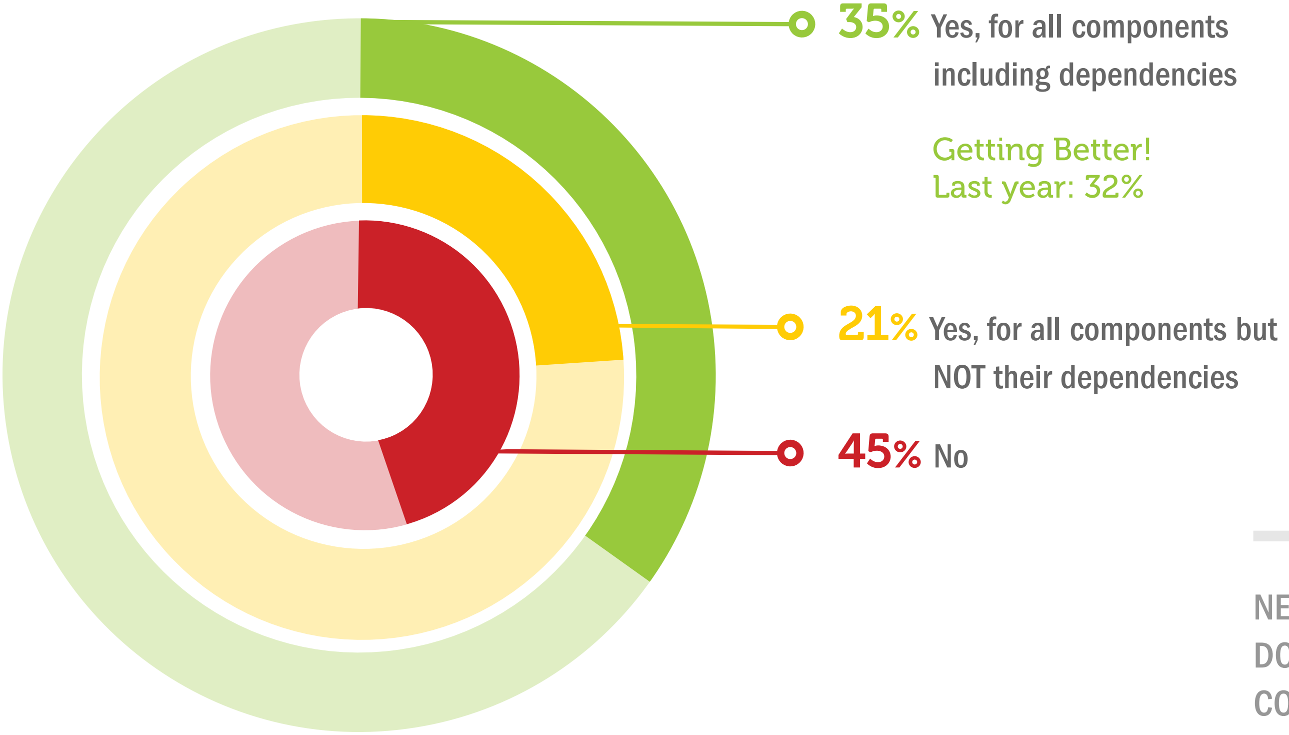


20%

No, our policy does not restrict component usage based on licensing

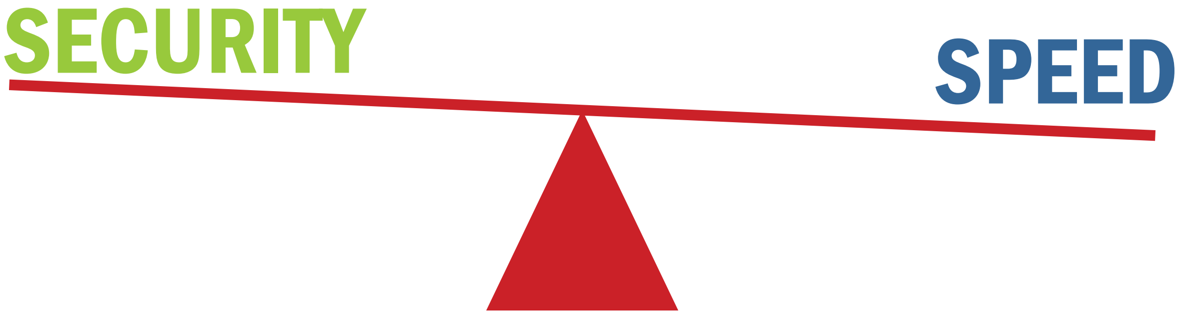
Things don't get much better once applications are in production.

Question: Does your organization maintain an inventory of open source components used in production applications?



NEARLY 2/3 OF ORGANIZATIONS DON'T EVEN MAINTAIN A COMPLETE BILL OF MATERIALS FOR THEIR APPLICATIONS.

The answers to our survey point to a tradeoff.
- a dangerous tradeoff -
between speed and security



Development is agile, component-based, and open source. Security hasn't kept up. There has to be a better way.

FIXING THE RISK:

GOOD COMPONENT PRACTICE

SO WE KNOW THERE'S A RISK. WHAT DO WE DO ABOUT IT?

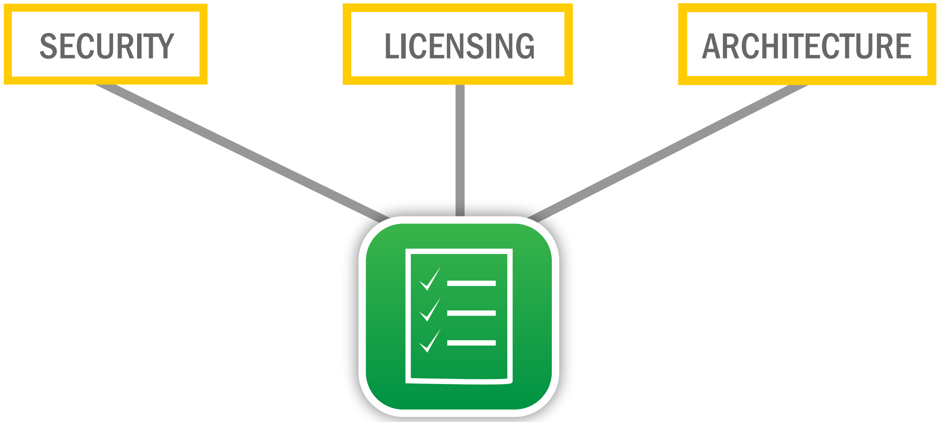
7 STEPS

TO GOOD COMPONENT PRACTICE DESIGNED TO HELP YOUR DEVELOPERS GO FAST, AND YOUR ORGANZIATION TO BE SECURE.

Step 1

CREATE AN OPEN SOURCE POLICY, IF YOU DON'T ALREADY HAVE ONE.
MAKE IT WORK FOR DEVELOPMENT OR IT WON'T WORK AT ALL.

Step 2



SECURITY

LICENSING

ARCHITECTURE

ENSURE YOUR POLICY COVERS ALL ASPECTS OF COMPONENT MANAGEMENT: SECURITY, LICENSING, AND ARCHITECTURE.

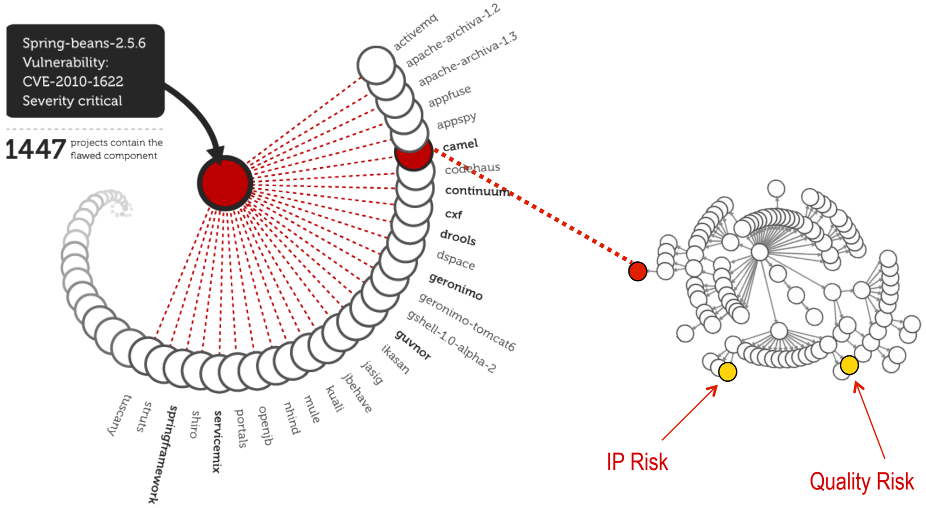
Step 3

GIVE DEVELOPERS THE INFORMATION THEY NEED TO MAKE GOOD DECISIONS UP FRONT.

Step 4

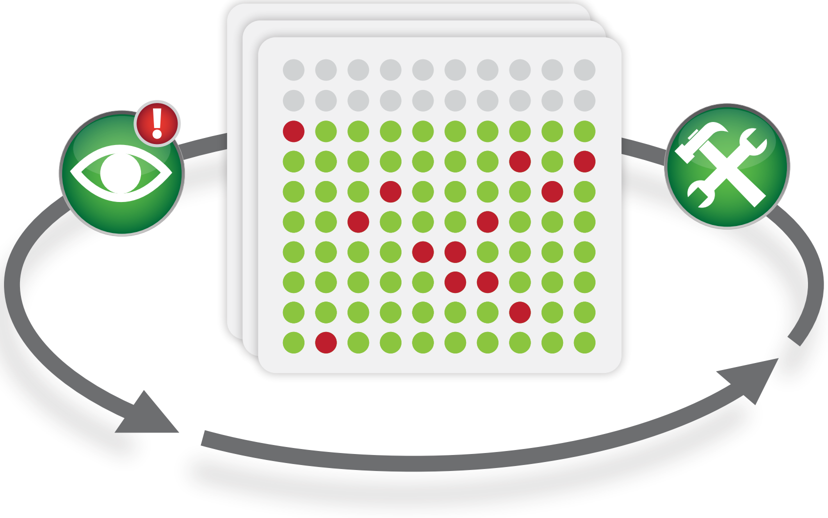
MAKE SURE YOUR POLICY IS AUTOMATICALLY
APPLIED IN THE TOOLS YOUR DEVELOPERS ALREADY USE.

Step 5



BEFORE GOING TO PRODUCTION, CREATE AND MAINTAIN A COMPLETE LIST OF DEPENDENCIES. OTHERWISE, YOU WON'T KNOW WHERE TO LOOK WHEN THERE IS A PROBLEM.

Step 6



WATCH OUT FOR NEW FLAWS.

NEW COMPONENT VULNERABILITIES EMERGE ALL THE TIME.

Step 7

HAVE A REMEDIATION PLAN. HOPE IS NOT A STRATEGY.
KNOW HOW YOU WILL FIX PROBLEMS—REGARDLESS OF WHERE
THEY OCCUR IN THE LIFECYCLE.

Want to learn more?

SONATYPE CLM

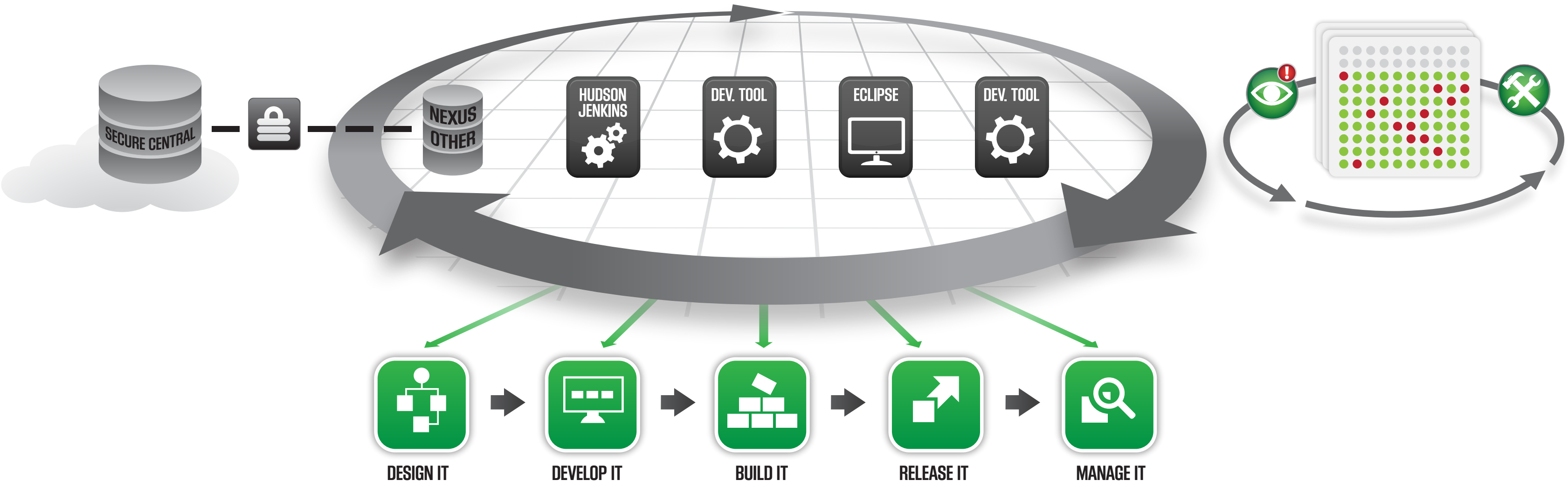
1. Secure Consumption with the use of certified components and integrity checking throughout the lifecycle

2. Govern Development to ensure policy compliance without disrupting developer productivity

3. Profile Exposures to proactively identify and prioritize action

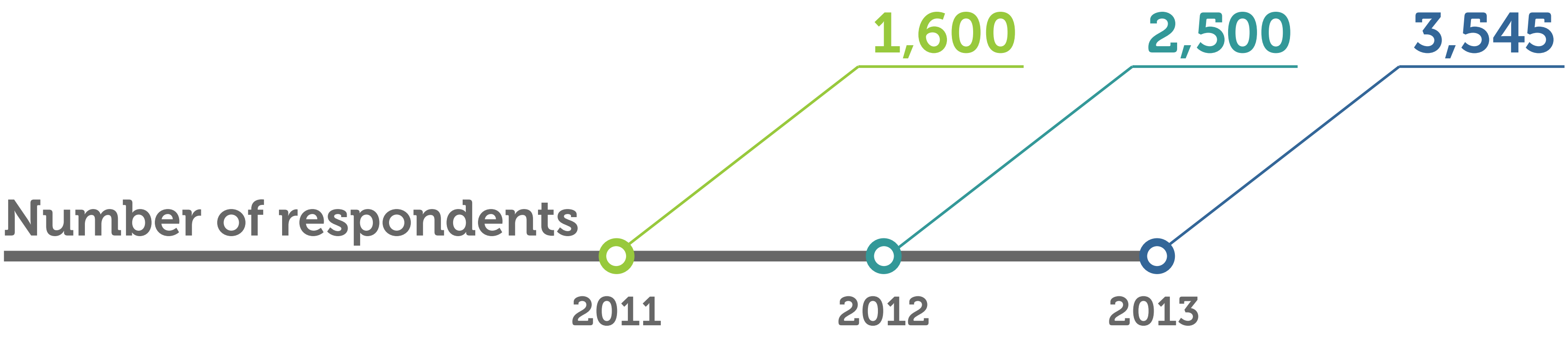
4. Remediate Risk by preventing and quickly fixing security and IP vulnerabilities

5. Monitor Threats in production applications to ensure continuous trust in critical operations



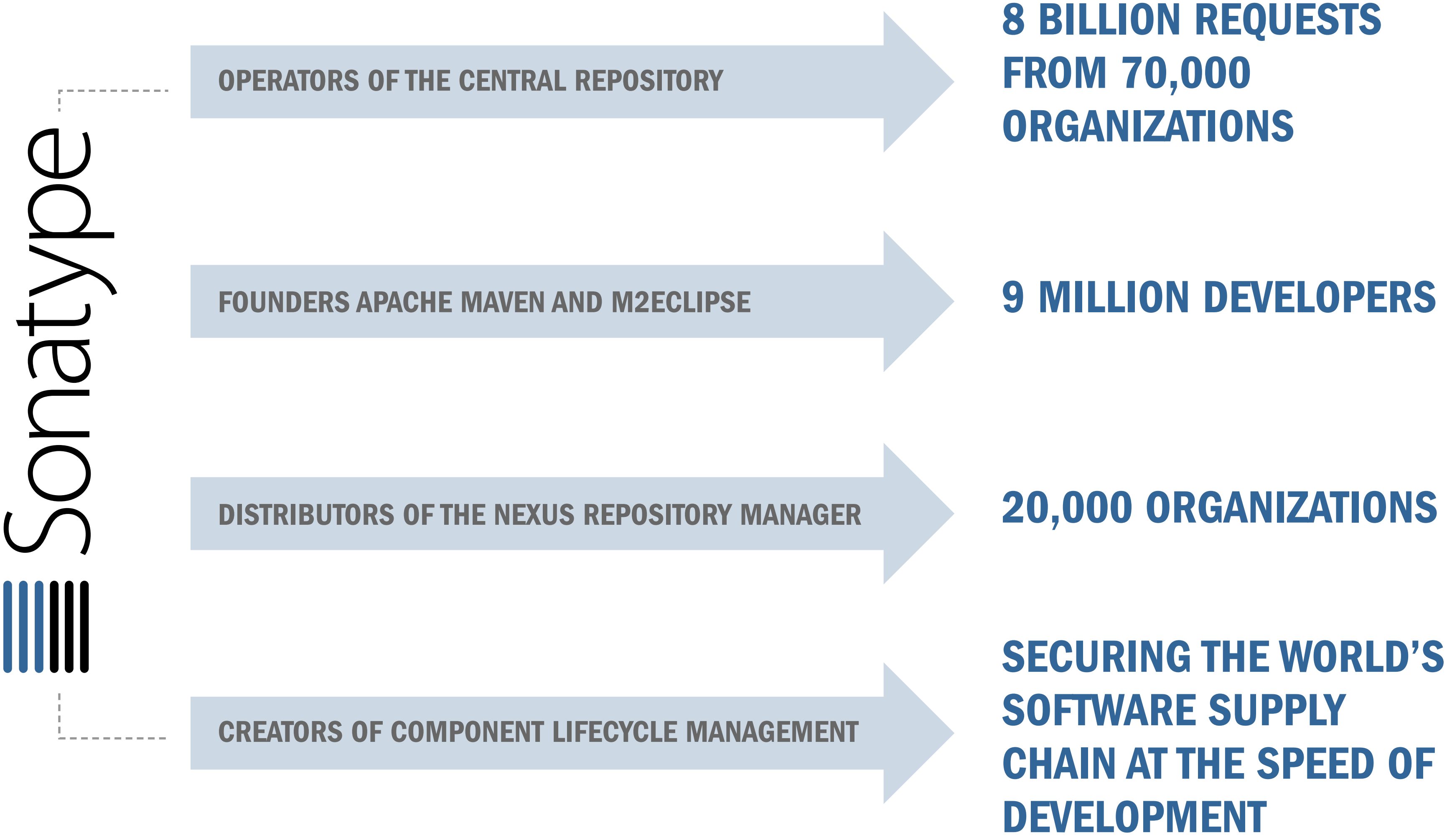
SONATYPE CAN HELP. VISIT WWW.SONATYPE.COM/CLM

Largest Open Source Survey of Its Kind



Sonatype's annual community survey is the industry's largest, most comprehensive primary research on open source usage from a developers point of view. 2013 saw record participation with more than 3,500 participants.

Meet Sonatype,
the Component Lifecycle Management Company



OPERATORS OF THE CENTRAL REPOSITORY → 8 BILLION REQUESTS FROM 70,000 ORGANIZATIONS

FOUNDERS APACHE MAVEN AND M2ECLIPSE → 9 MILLION DEVELOPERS

DISTRIBUTORS OF THE NEXUS REPOSITORY MANAGER → 20,000 ORGANIZATIONS

CREATORS OF COMPONENT LIFECYCLE MANAGEMENT → SECURING THE WORLD'S SOFTWARE SUPPLY CHAIN AT THE SPEED OF DEVELOPMENT