FINAL RESULTS

2014 Sonatype Open Source and Application Security Survey

Sonatype CONTRAST SECURITY NEA TSWA RUGGED

"I will share the ***DEVELOPMENT*** *perspective"*

Brian Fox
VP Product Management
Sonatype
@Brian_Fox

Sonatype

"I will offer the ***APPLICATION SECURITY*** *perspective"*

Adrian Lane
CTO & Analyst
Securosis
@AdrianLane

Securosis

A BIG THANK YOU TO THE

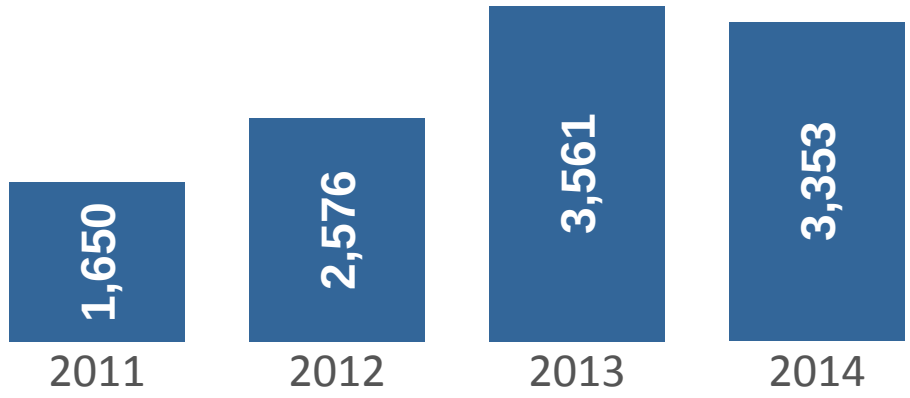
3,353

PEOPLE WHO SHARED THEIR VIEWS

OVER THE FOUR YEAR STUDY

11,140

PEOPLE SHARED THEIR VIEWS



Who took the survey?

3,353 participants at companies such as...

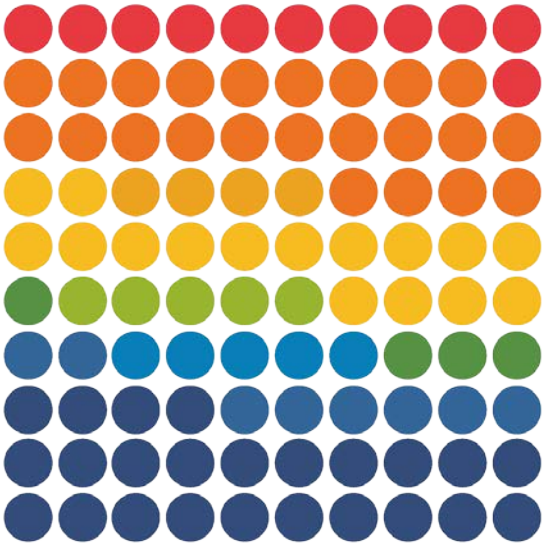
Adobe
Bank of America
RSA SECURITY
ERICSSON
BOSTON UNIVERSITY
CapitalOne
ebay
hp
cisco
FedEx
ESPN
HARVARD MEDICAL SCHOOL
comcast
GM
IBM
THE LINUX FOUNDATION
sears
WELLS FARGO
YAHOO!
TNT express
WeightWatchers
NYSE
UNION PACIFIC
TOMTOM
Liberty Mutual
TimeWarner
UNIVERSITY OF TORONTO

79% OF THE RESPONSES CAME FROM DEVELOPERS, MANAGERS AND ARCHITECTS

Source: 2014 Sonatype Open Source and Application Security Survey

Who took the survey?

Q: In what industry is your company?



- 11% Banking and finance
- 23% Technology/ISV
- 4% Insurance
- 16% Consulting/Systems
- 5% Telecommunications
- 4% Manufactutring
- 5% Media and entertainment
- 8% Government/Military
- 24% Other

58% OF THE RESPONDENTS HAVE MORE THAN 25 DEVELOPERS IN THEIR ORGANIZATION

OVER 700 OF THE RESPONDENTS HAVE MORE THAN 500 DEVELOPERS

Source: 2014 Sonatype Open Source and Application Security Survey

It is *not* the
stats that count

(it’s the action you take)

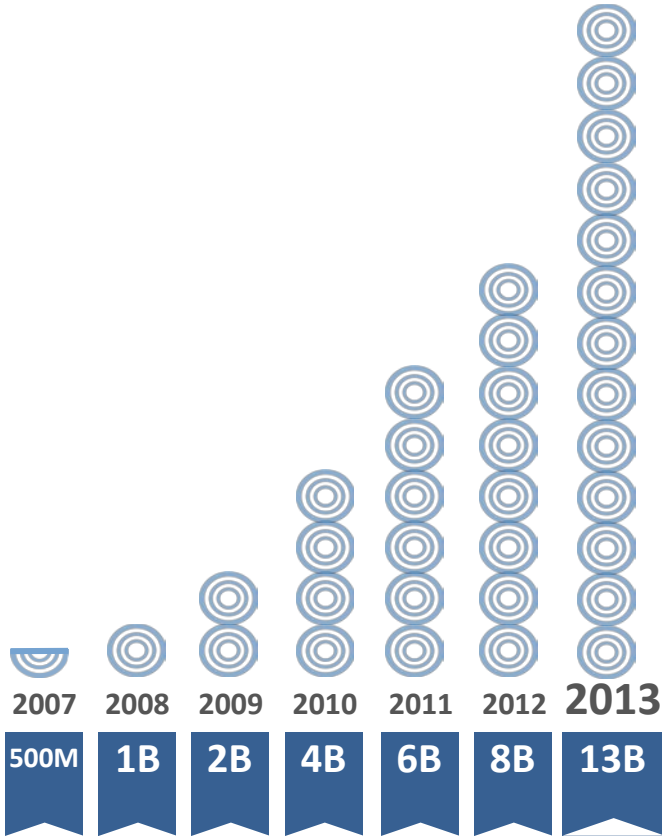
Open source component use has exploded

13 BILLION[1]

OPEN SOURCE SOFTWARE
COMPONENT REQUESTS

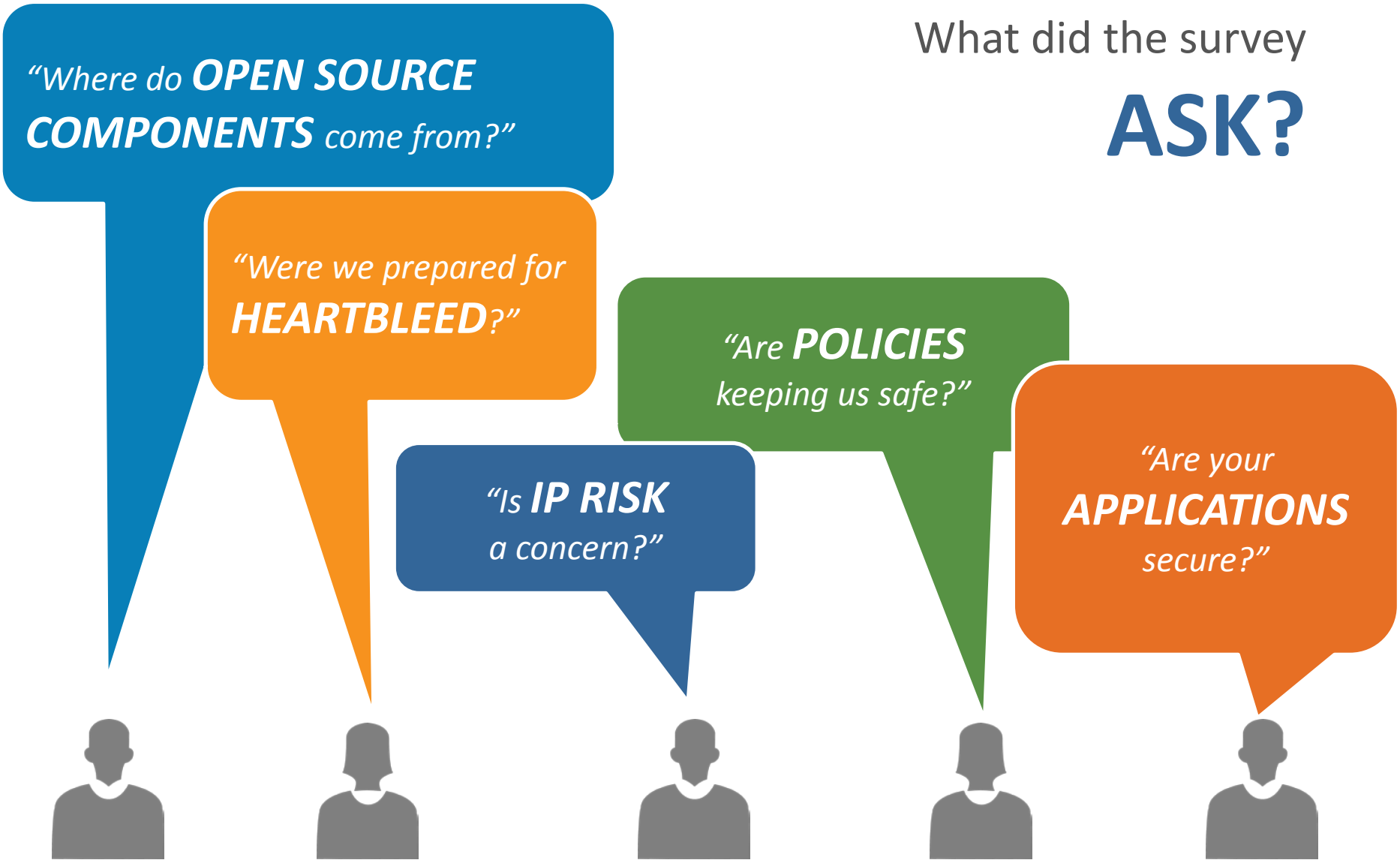
11 MILLION[2]

DEVELOPERS WORLDWIDE



Source: [1]Sonatype, Inc. analysis of the (Maven) Central Repository; [2]IDC

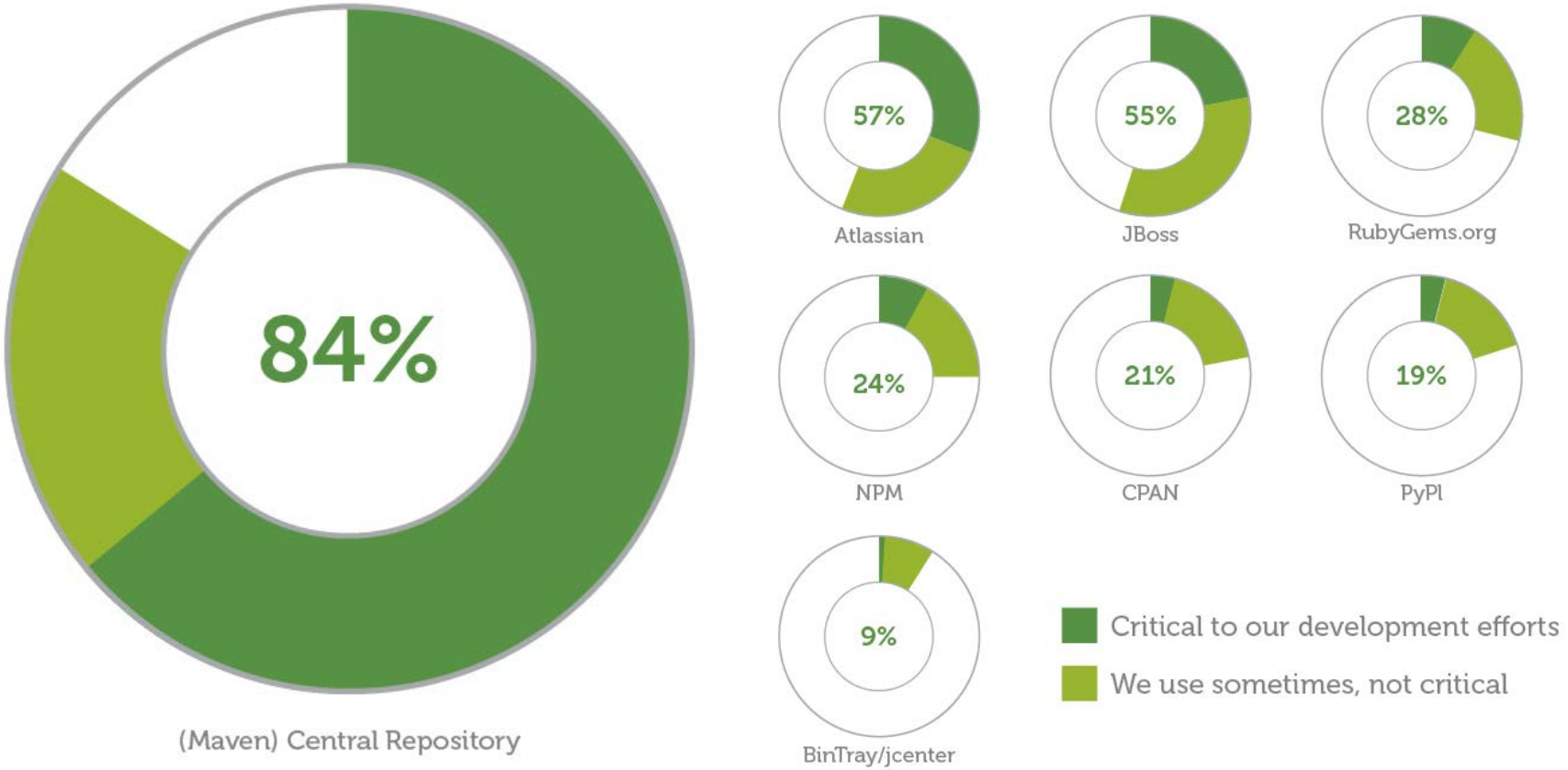
What did the survey **ASK?**



WHERE DO YOU GO FOR COMPONENTS?

When they need components, more organizations rely on the Central Repository

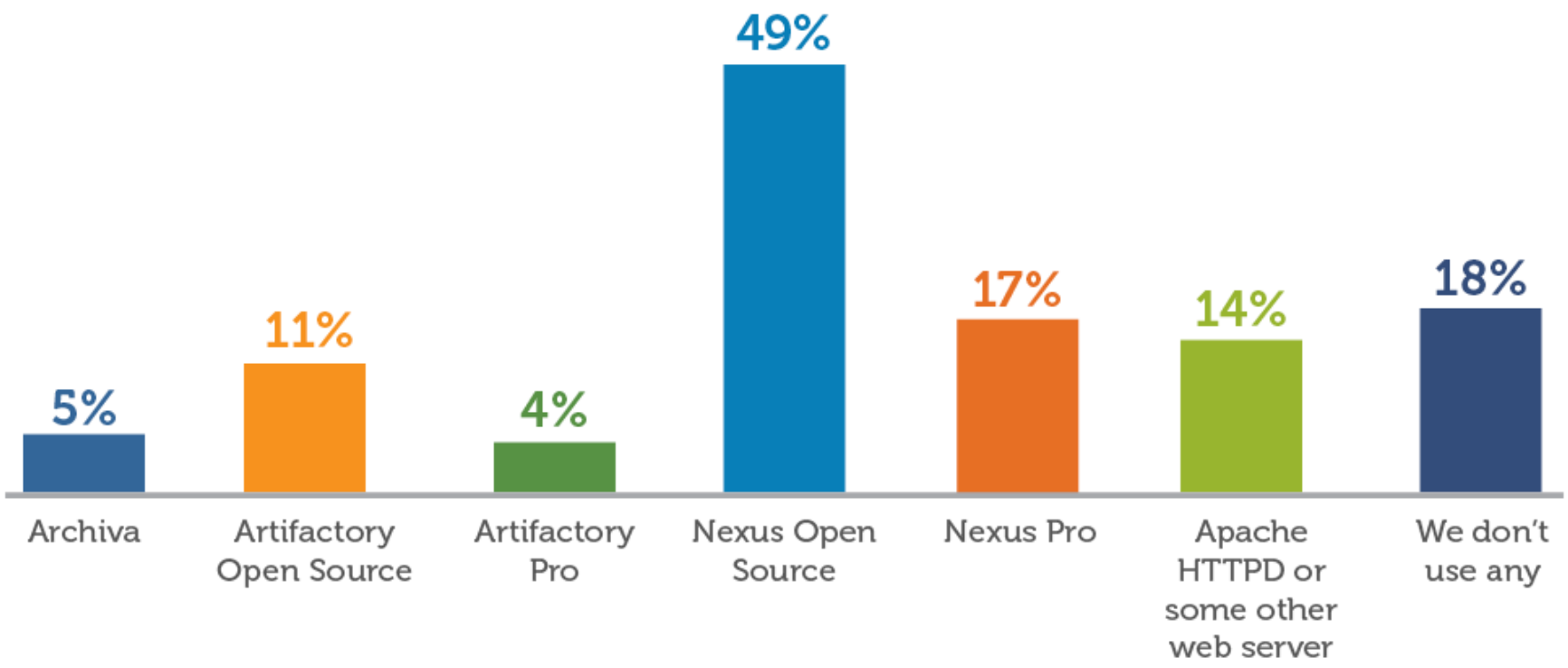
Q: For your organization, please rate the following sources of open source components.



Source: 2014 Sonatype Open Source Development and Application Security Survey

Local component management provides an opportunity for improved visibility and control.

Q: Which local component repository manager does your organization use?

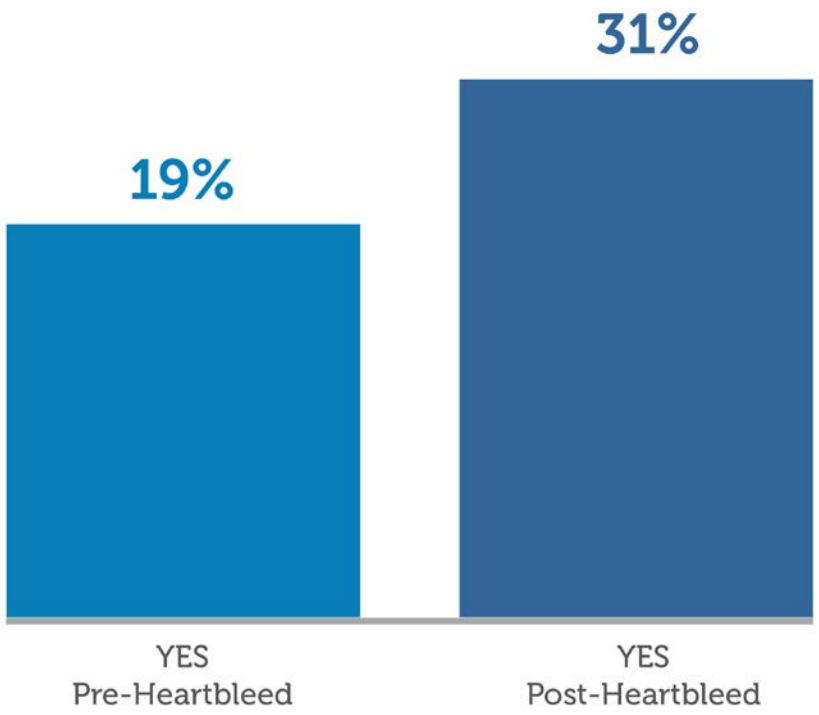


Source: 2014 Sonatype Open Source Development and Application Security Survey

HOW PREPARED WERE WE FOR HEARTBLEED?

Heartbleed heightened concerns over open source-related breaches.

Q: Has your organization had a breach that can be attributed to a vulnerability in an open source component or dependency in the last 12 months?



twitter

31% confirmed or suspected breaches after Heartbleed. #OpenSourceSurvey

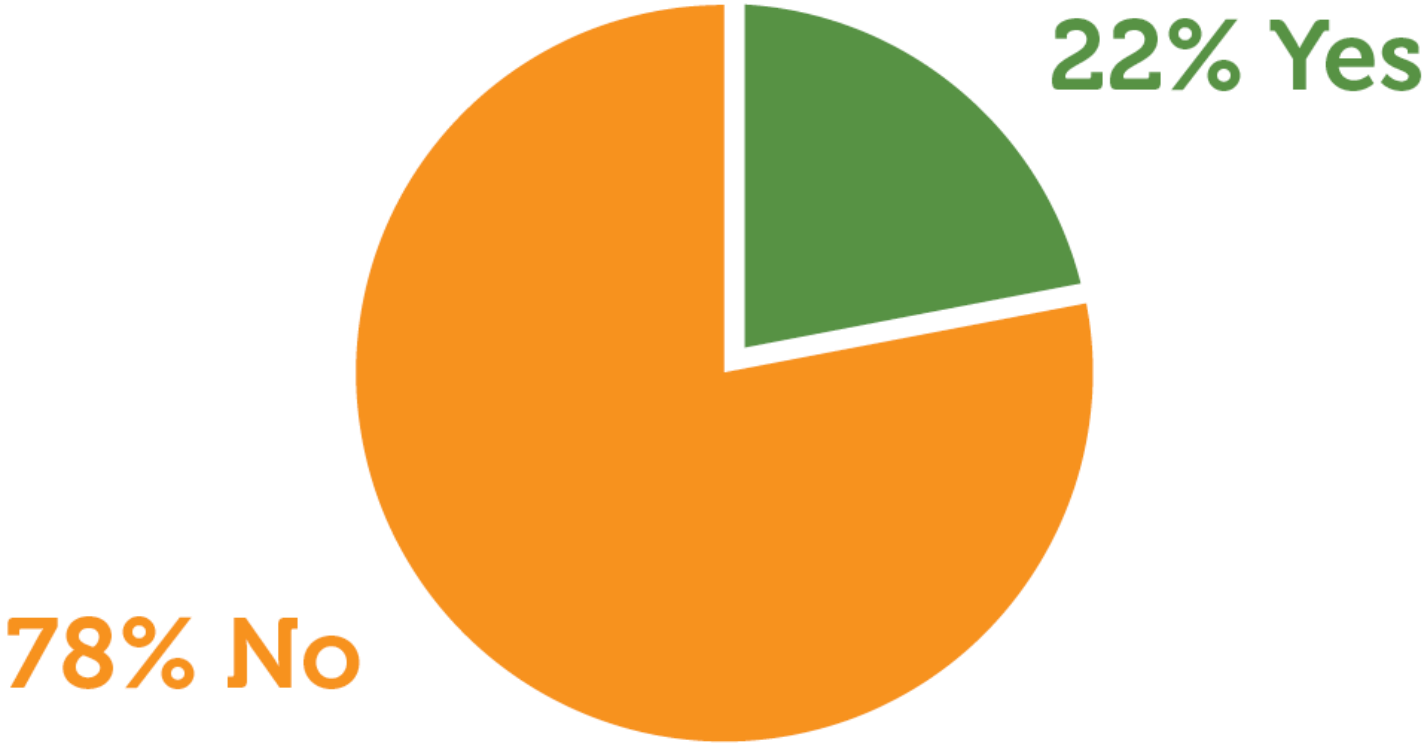
PARTICIPANTS NOTED

373

SUCCESSFUL AND SUSPECTED OPEN SOURCE RELATED BREACHES
IN PAST 12 MONTHS

Yet, 78% have never banned an open source component, library or project.

Q: Has your organization ever banned use of an open source component, library or project?



twitter Agree or Disagree? Should open source policies ban a risky component. #OpenSourceSurvey

The majority of developers don’t track component vulnerability over time.

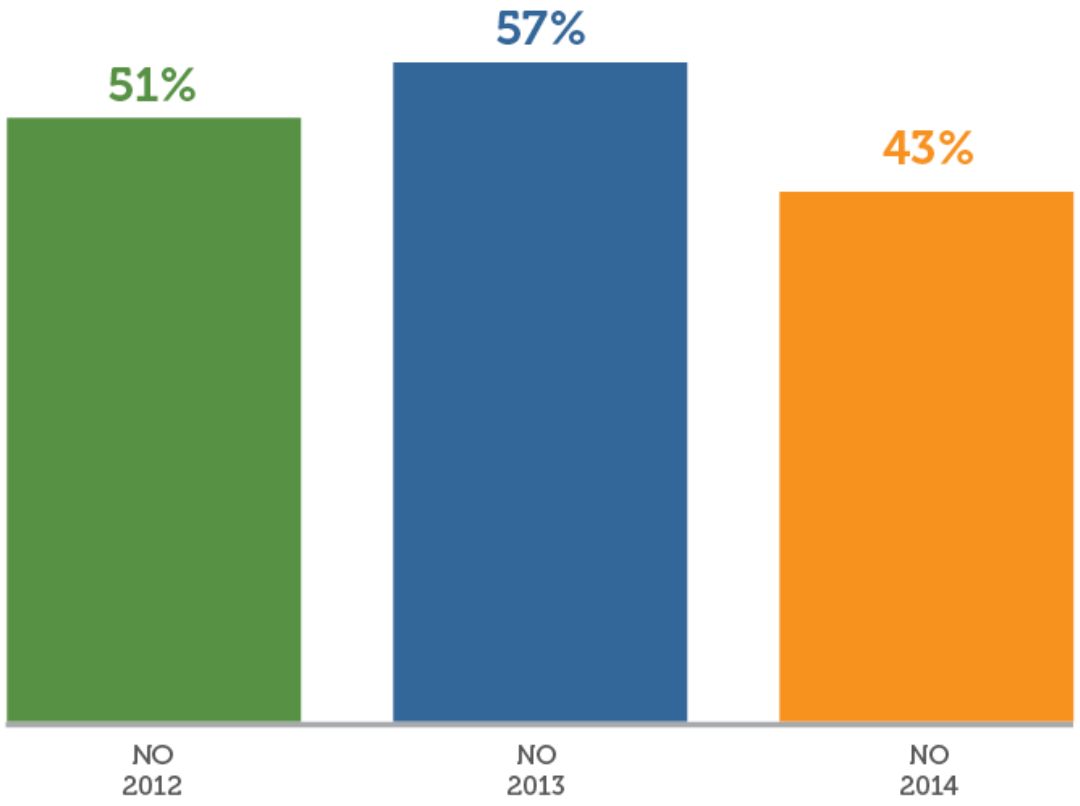
Even when component versions are updated 4-5 times a year to fix known security, license or quality issues[1].

Q: Does someone actively monitor your components for changes in vulnerability data?

ARE OPEN SOURCE POLICIES KEEPING OUR APPLICATIONS SAFE?

Nearly half of organizations continue to run without an open source policy.

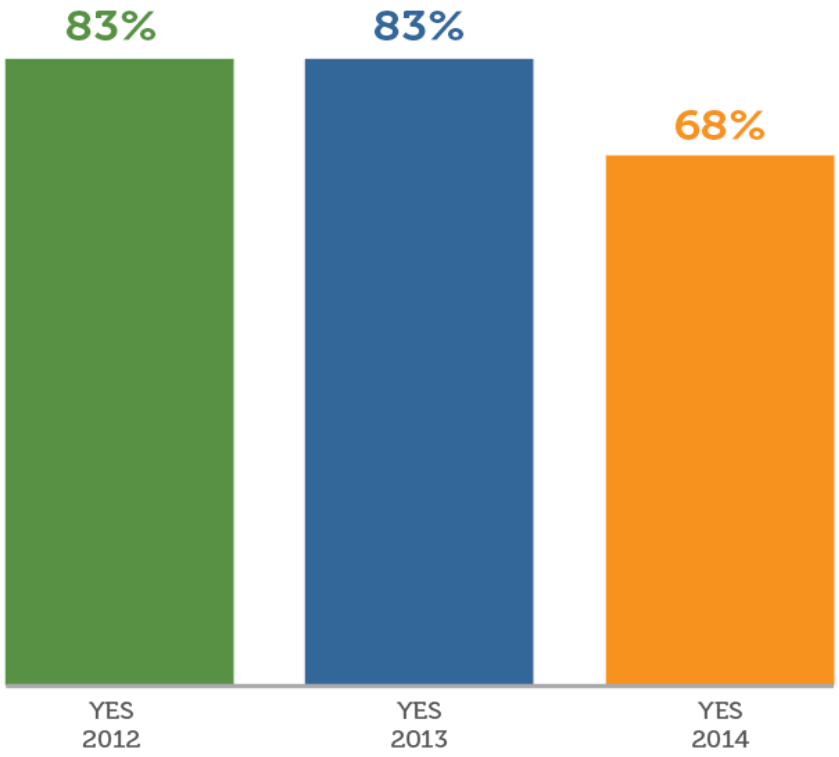
Q: Does your organization have an open source policy?



Source: 2012, 2013, 2014 Sonatype Open Source Development and Application Security Survey

Of those with policies, fewer are following them…

Q: Do you actually follow your company's open source policy?

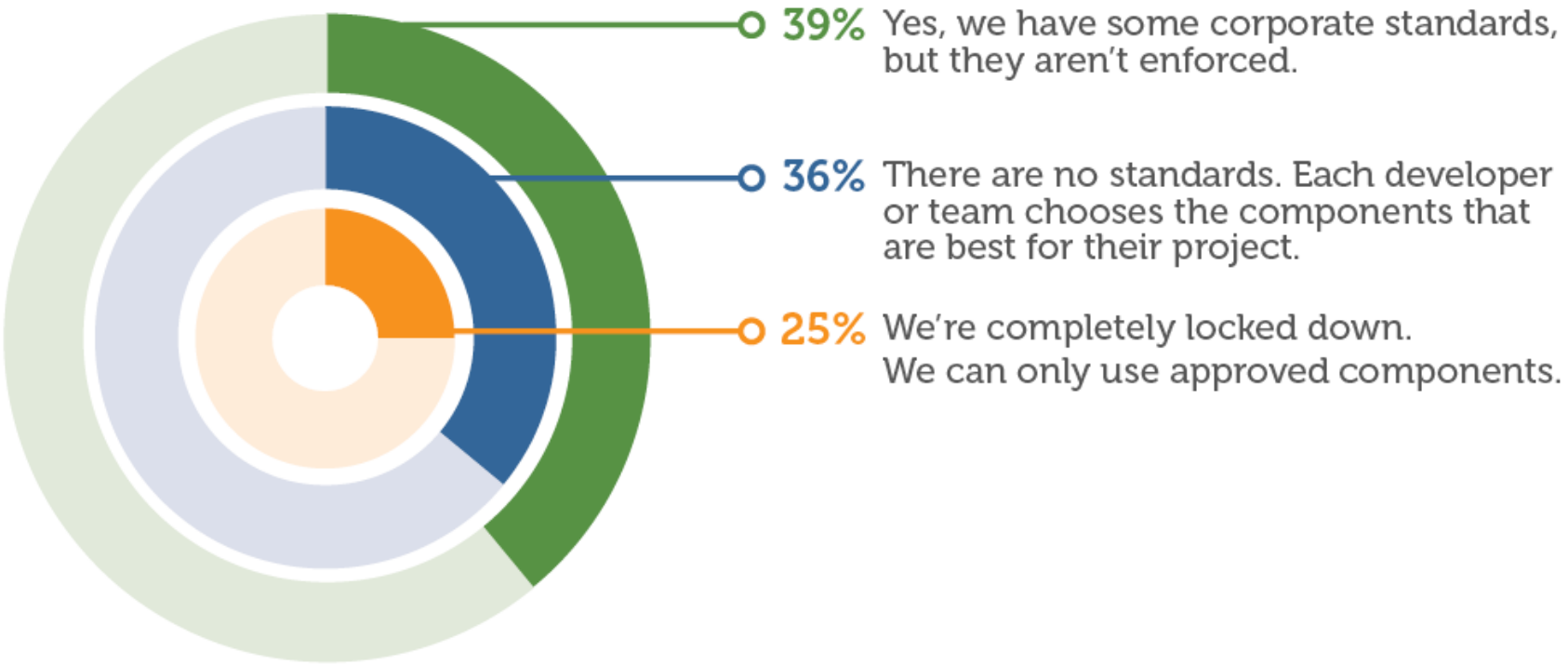


twitter 32% not following policy = No policy. #OpenSourceSurvey

Even if they have a policy, 75% don't have meaningful controls over what components are in their applications.

Is an "Open Source Policy" more than just a document?

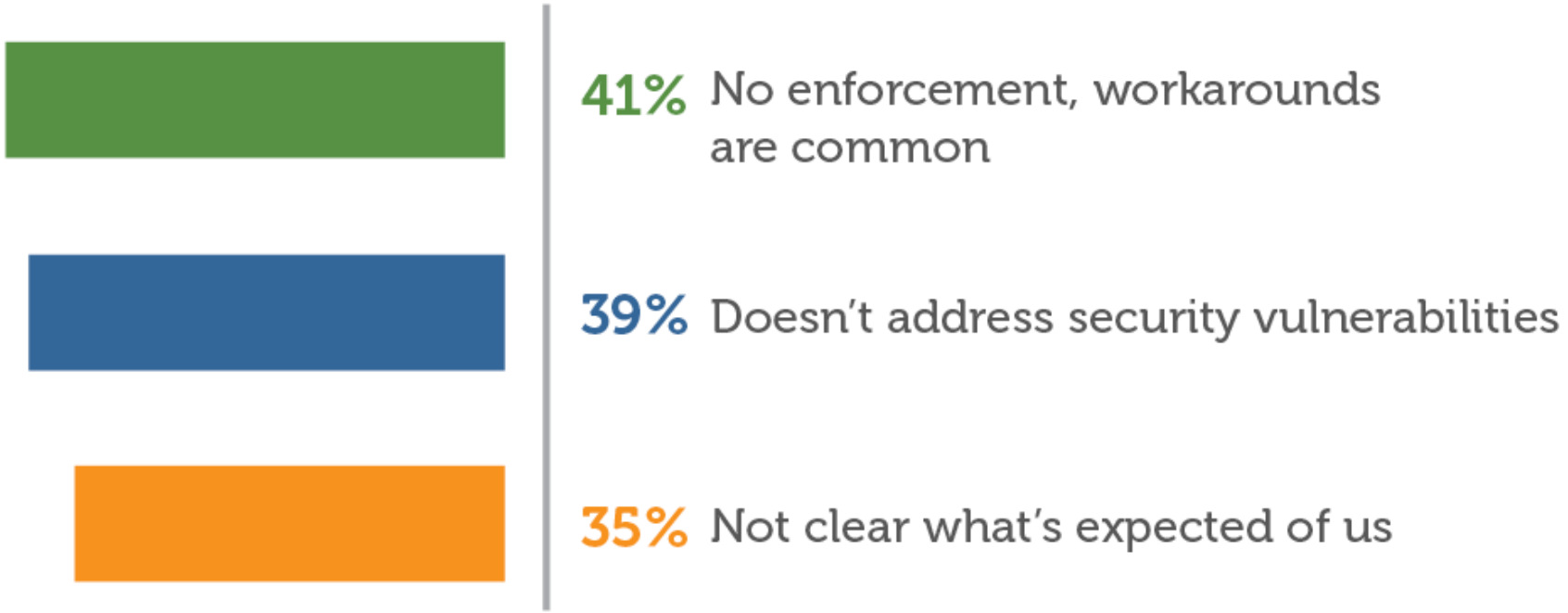
Q: How well does your organization control which components are used in development projects?



Source: 2014 Sonatype Open Source Development and Application Security Survey

If you're not enforcing policies, you're not protecting your software.

Q: What are the top challenges with your open source policy? (Top 3)



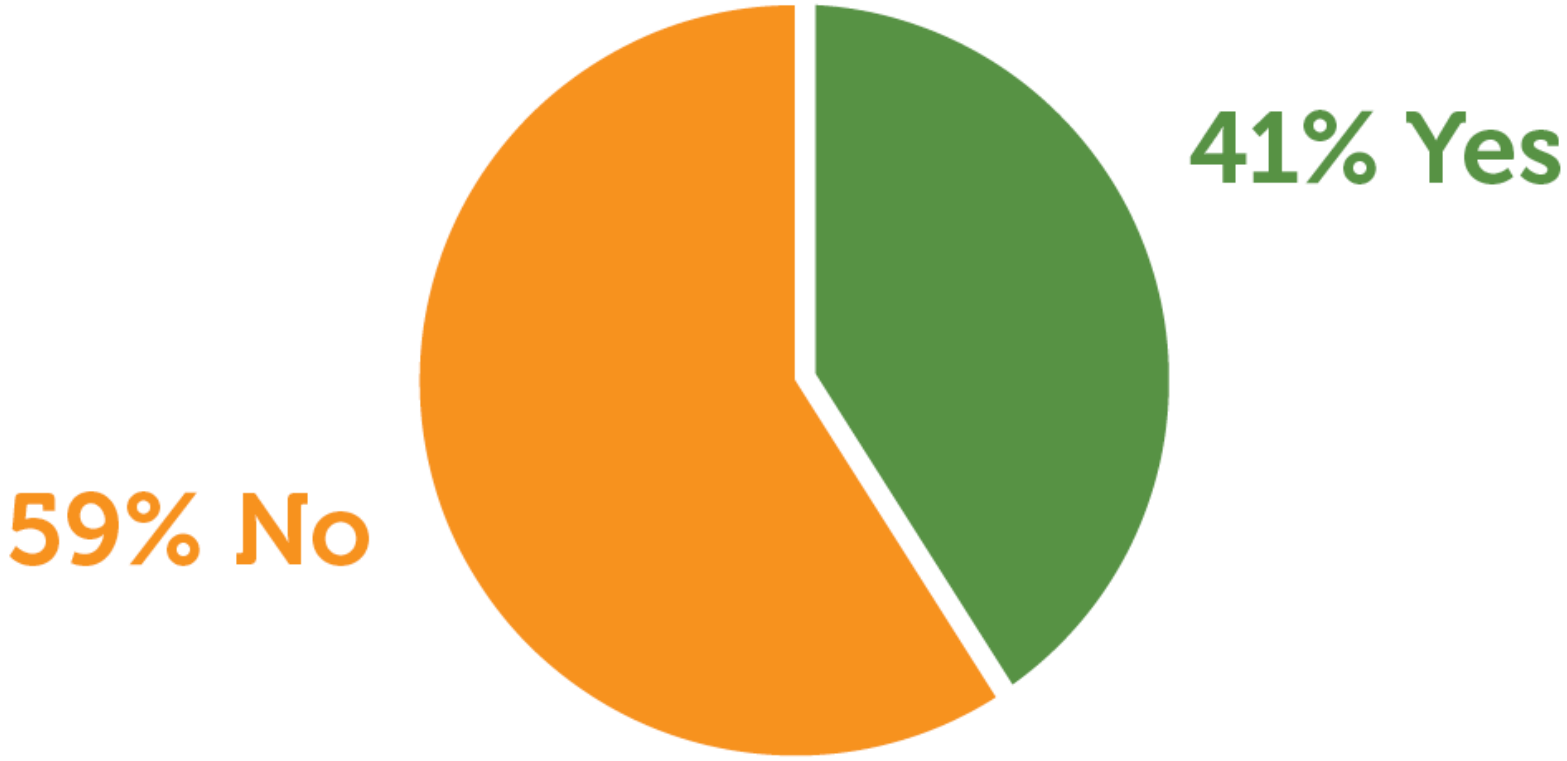
twitter Policies that are not enforced, provide no protection. #OpenSourceSurvey

IP RISK IS ALSO PART OF THE GAME

The majority are not concerned about license risks.

Yet, licensing data is considered helpful to 67% of respondents when selecting open source components to use.

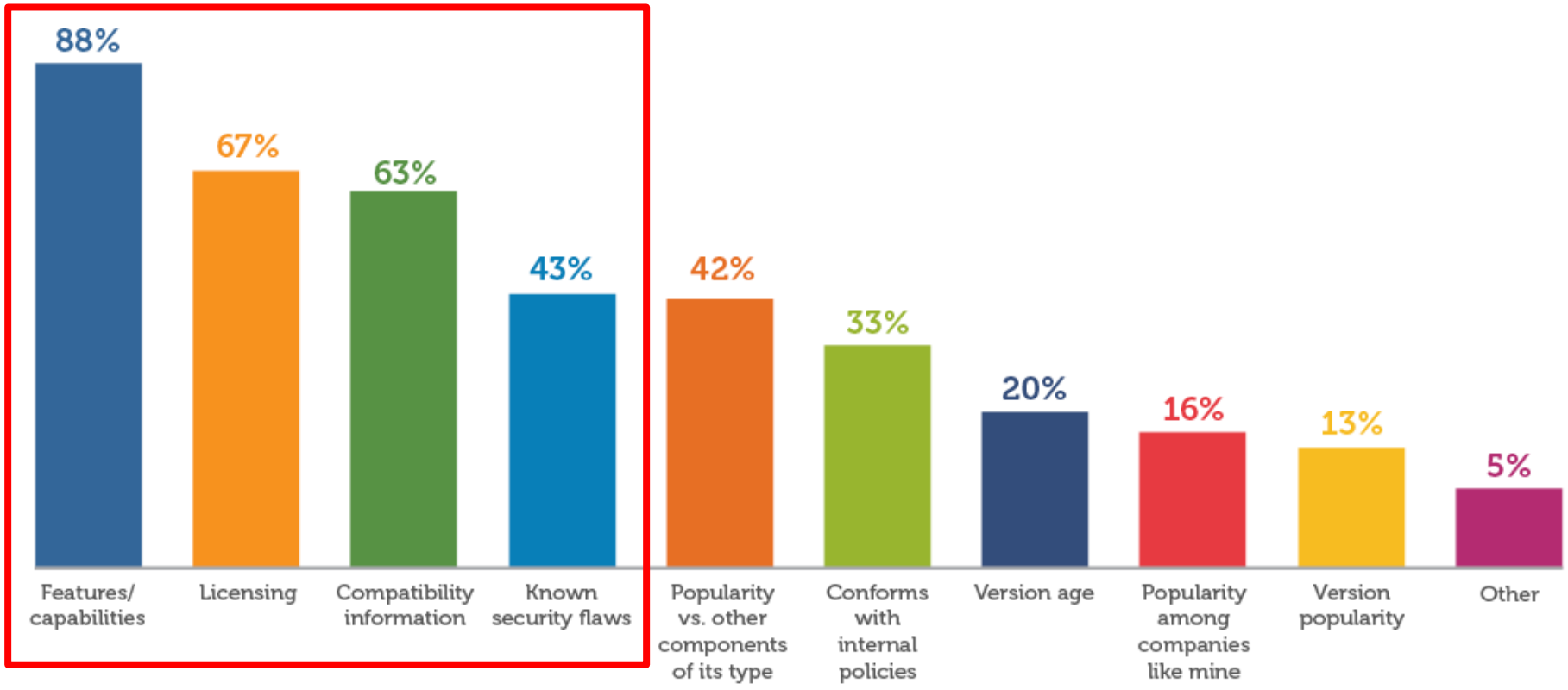
Q: Are open source licensing risks or liabilities a top concern in your position?



twitter No license = No right to use. #OpenSourceSurvey

Developers want components that work and don't add risk

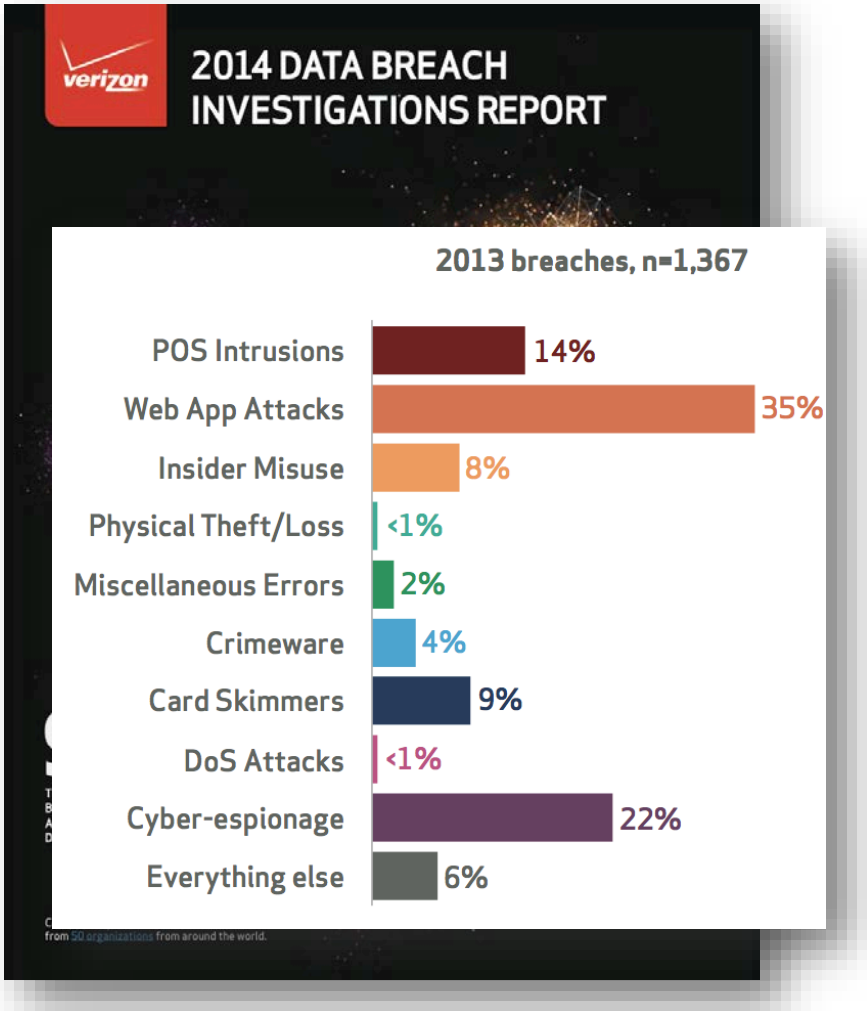
Q: When selecting components, which characteristics would be most helpful to you? (choose four)



Source: 2014 Sonatype Open Source Development and Application Security Survey

APPLICATIONS ARE THE #1 BREACH VECTOR FOR HACKERS

Applications are the #1 Breach Vector…



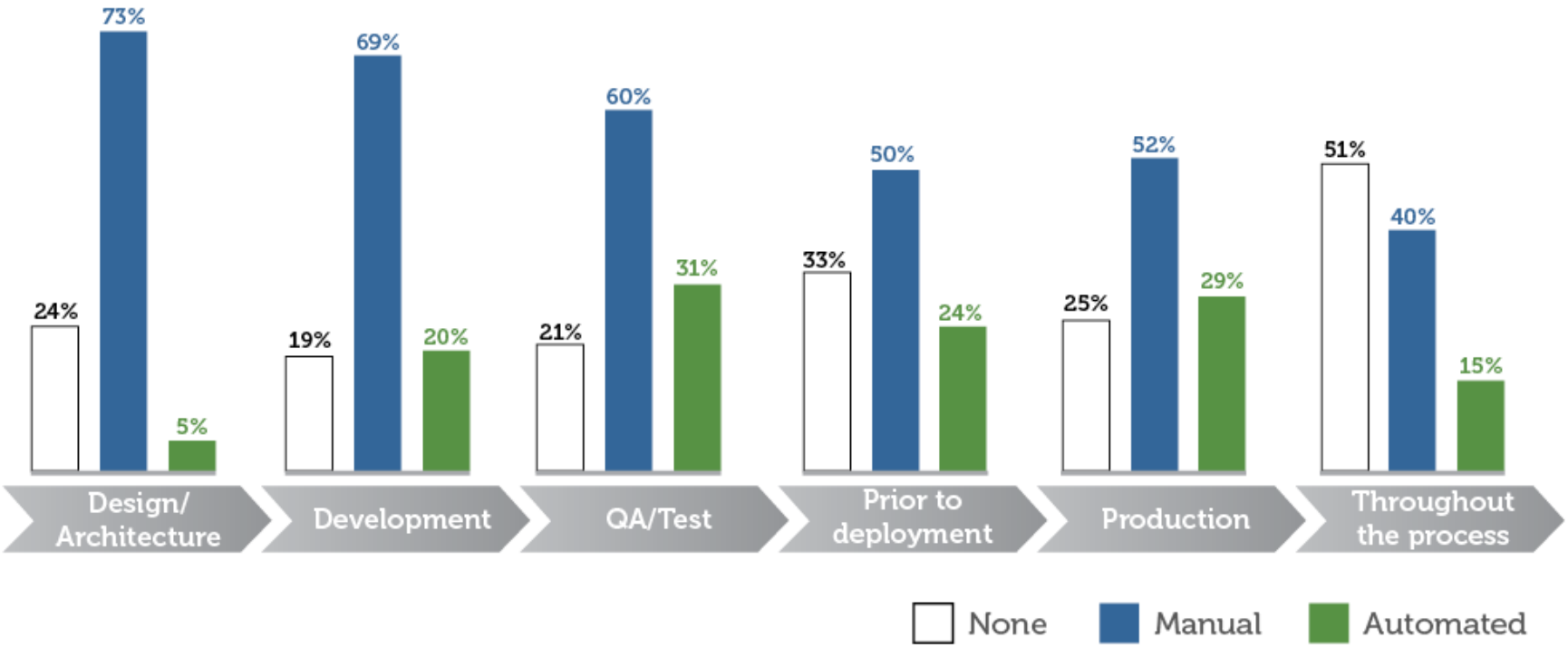
IN APRIL 2014, THE VERIZON DATA BREACH INVESTIGATIONS REPORT NAMED APPLICATIONS AS THE #1 BREACH VECTOR, REPRESENTING ANOTHER SIGNIFICANT, YET SOMBER MILESTONE IN APPLICATION SECURITY.

WITH COMPONENTS ACCOUNTING FOR 90% OF A TYPICAL APPLICATION, SECURE APPLICATION DEVELOPMENT PRACTICES SHOULD BE A TOP CONCERN FOR THE OPEN SOURCE COMMUNITY.

The majority rely on manual application security analysis.

Application development runs at Agile & DevOps speed. Is security is keeping pace?

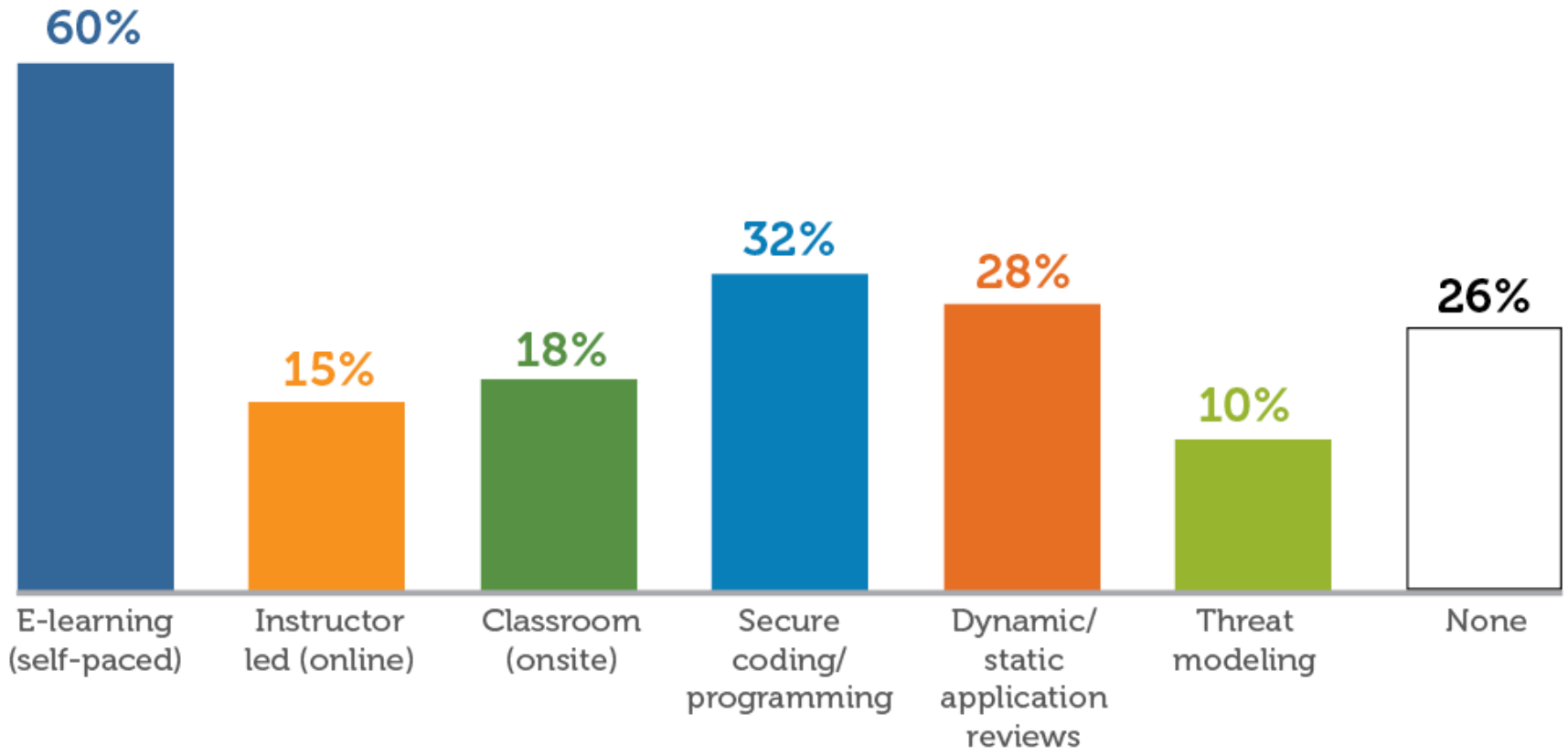
Q: At what point in the development process does your organization perform application security analysis?



twitter Automation is inevitable. Manual security can't keep pace with agile development #OpenSourceSurvey

While applications account for more breaches, 1-in-4 developers don't receive application security training.

Q: What application security training is available to you?



Source: 2014 Sonatype Open Source Development and Application Security Survey

Read the

INDEPENDENT ANALYSIS from **SECUROSIS**

securosis.com/blog

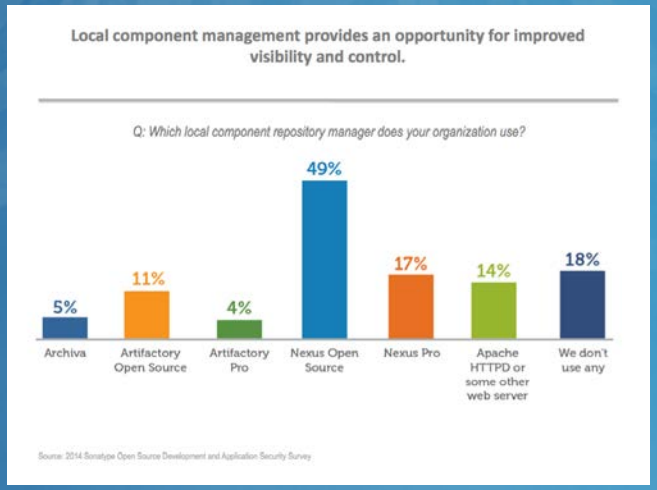
Analysis 1
June 11

Analysis 2
June 18

Analysis 3
June 20

WANT ALL THE JUICY SURVEY RESULTS? VISIT:

www.sonatype.com/2014survey



The 2014 Complete Results
(+30 questions and results covered)

Expert Analysis of Results
(Webinar recording and slides)