FINAL RESULTS

2014 Sonatype Open Source Development and Application Security Survey

Sonatype CONTRAST SECURITY NEA TSWA RUGGED

MY REFLECTIONS ON THE 2014 RESULTS

Wow! What an amazing turnout we had for our 4th annual survey: 3,353 participants this year brings us to over 11,000 in the four years we've run this survey. I would like to extend a BIG THANK YOU to all who participated!

The survey started with a bang and was quickly followed by a shock wave. Just a week after our 2014 survey kicked off this year, the tech world was thrown off kilter by the announcement of the Open SSL bug dubbed Heartbleed. In this report, we'll share how perceptions of open source components and application security changed before and after the Heartbleed announcement.

In many ways, I believe this year's survey results will mark an inflection point for open source development and application security. With 90% of a typical application now assembled using open source components, and enterprise architects teaming with application security to boost their focus on tracking and governing known component vulnerabilities, I believe we will mark post-Heartbleed 2014 as an important turning point toward trusted application development. This includes an increased vigilance toward use and maintenance of components across our software supply chain.

While we celebrated the 34 survey participants who scored those kool LEGO programmable robots or the $100 Amazon gift cards, we also had some fun this year finding out what your pizza and drink preferences were (spoiler alert: beer edged out soda by 1%). And yes, due to popular demand, we'll be sure to add in "bacon" next year as one of the preferred pizza toppings.

As a good friend once reminded me, "it's not the stats that count". So, while the 2014 results might astound, motivate, or frustrate you, remember that the actions you take after seeing the results will be much more valuable to your organization than the stats themselves. Consider sharing these results with your colleagues over lunch or at your next staff meeting. You might even present them at your next local JUG, OWASP, or DevOps meet up to gauge perspectives or share best practices with others across the community.

Finally, I would like to thank this year's co-sponsors of the survey: NEA, Contrast Security, Rugged Software, and the Trusted Software Alliance. They all helped us refine this year's survey questions and broadened participation in this year's survey.

Now, dive into the results and let the discussions begin!

Sincerely,

Wayne Jackson
CEO, Sonatype

Wayne Jackson, CEO
Sonatype, Inc.

FINAL RESULTS
2012 Sonatype Open Source Development Survey

Previous 2013 Survey
bit.ly/sonatype13

FINAL RESULTS
2013 Sonatype Open Source Development Survey

Previous 2012 Survey
bit.ly/sonatype12

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

THIS YEAR

3,353

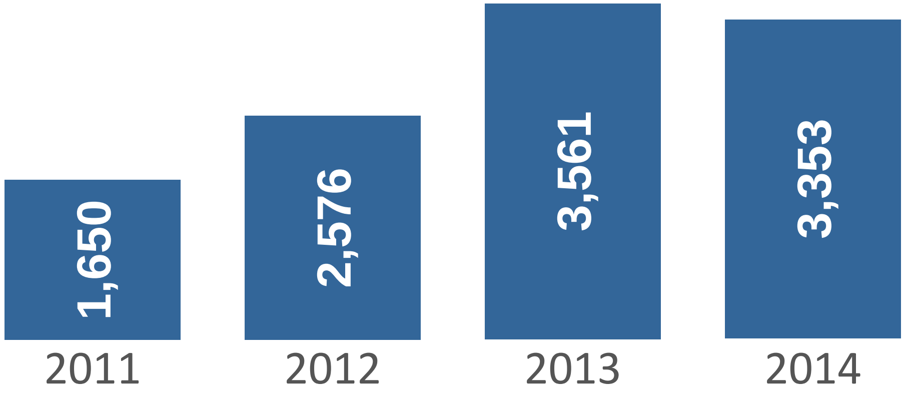
Thank you!

PEOPLE SHARED THEIR VIEWS

OVER THE FOUR YEAR STUDY

11,140

PEOPLE HAVE PARTICIPATED



The TRUE State of Open Source Security

Source: 2014 Sonatype Open Source and Application Security Survey

STATE OF THE INDUSTRY

Applications are the #1 attack vector leading to breach

13 billion open source component requests annually

11 million developers worldwide

90% of a typical application is is now open source components

46 million vulnerable open source components downloaded annually

PRACTICES

76% don't have meaningful controls over what components are in their applications.

21% must prove use of secure components.

63% have incomplete view of license risk.

COMPONENTS

The Central Repository is used by 83%.

Nexus component managers used 3-to-1 over others

84% of developers use Maven/Jar to build applications.

APP SECURITY

6 in 10 don't track vulnerabilities over time.

77% have never banned a component.

31% suspected an open source breach.

OSS POLICIES

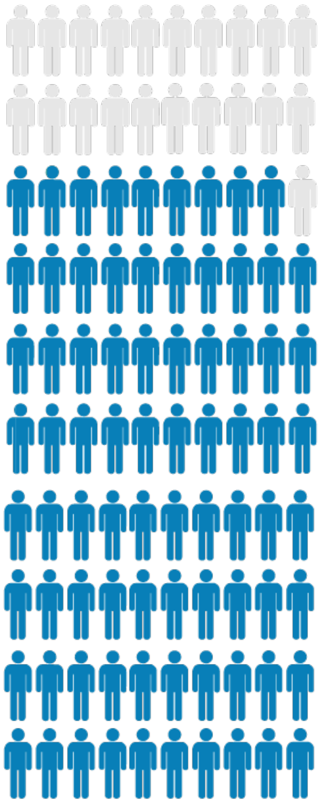
56% have a policy and 68% follow policies.

Top 3 challenges no enforcement/workaround are common, no security, not clear what's expected

Who took the survey?

Participants from companies such as…

Adobe
Bank of America
RSA SECURITY
ERICSSON
BOSTON UNIVERSITY
Capital One
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
UNIVERSITY OF TORONTO
Liberty Mutual
TimeWarner

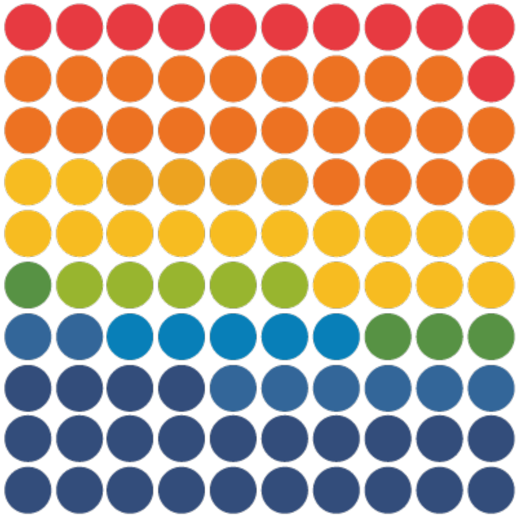


79% OF THE RESPONSES CAME FROM DEVELOPERS, MANAGERS AND ARCHITECTS

Source: 2014 Sonatype Open Source Development 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/SI

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 Development and Application Security Survey

A LITTLE BIT OF BACKGROUND:

OPEN SOURCE IS ON THE RISE

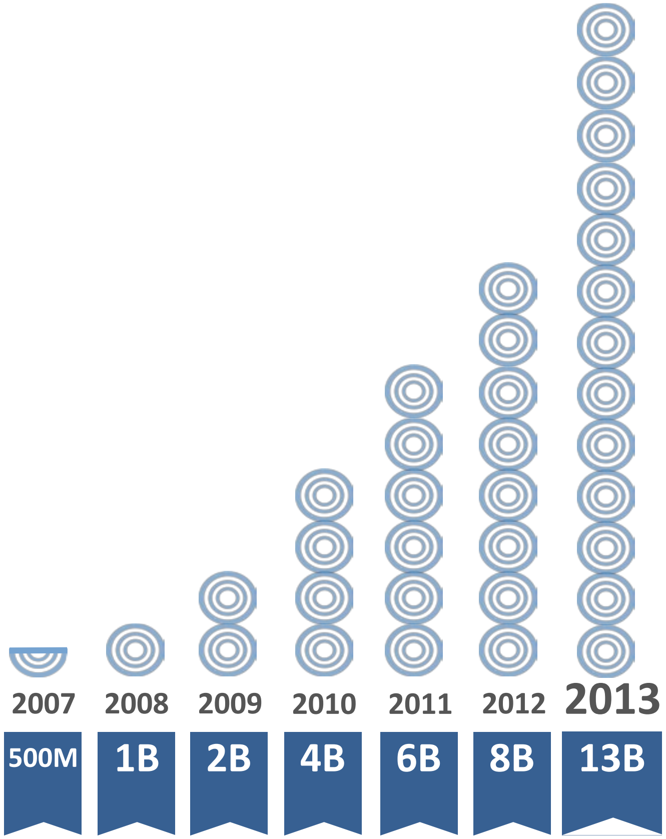
Open source component use has exploded

13 BILLION[1]

OPEN SOURCE SOFTWARE
COMPONENT REQUESTS

11 MILLION[2]

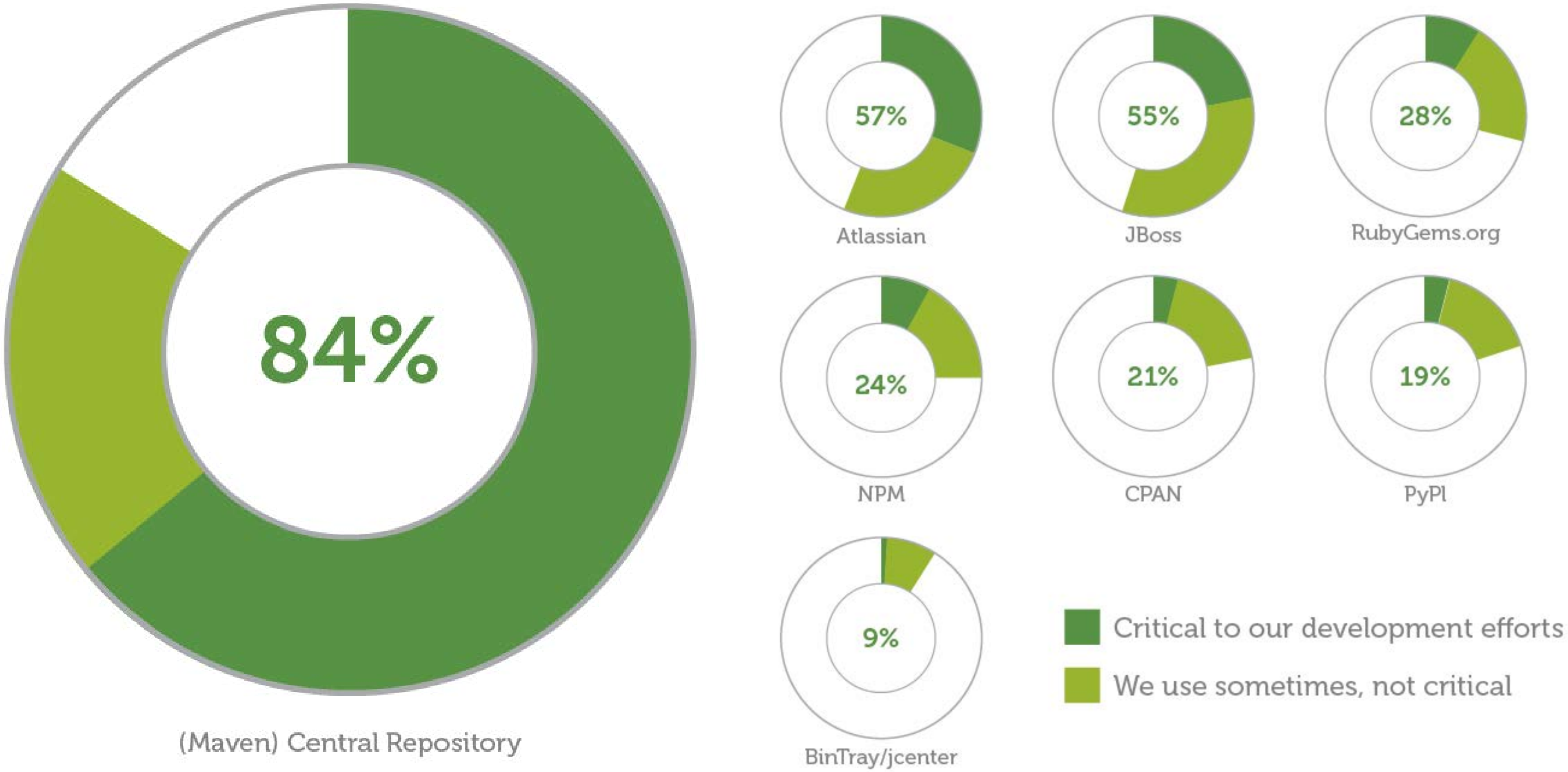
DEVELOPERS WORLDWIDE



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

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

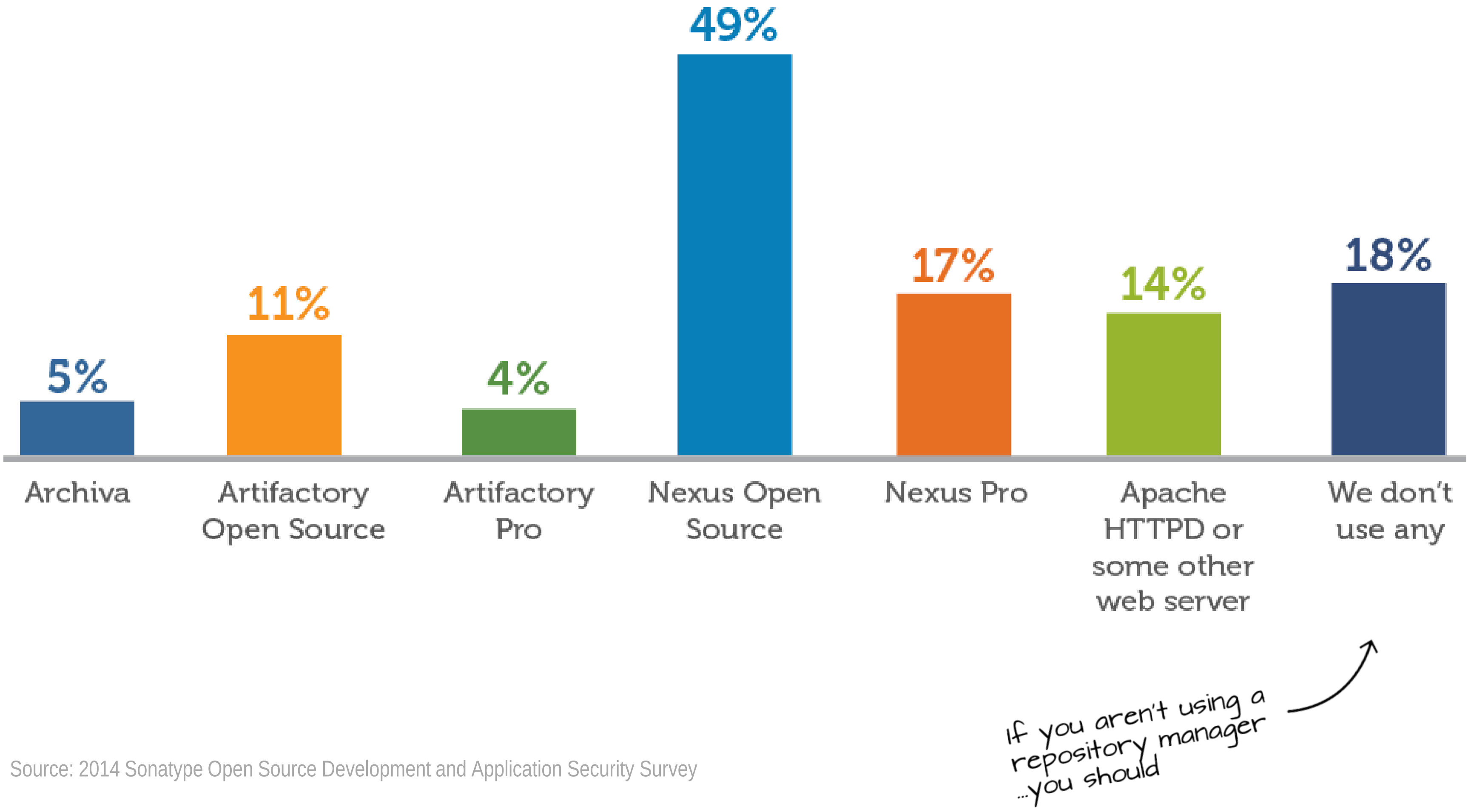
Q: For your organization, please rate the following sources of open source components.



Source: 2014 Sonatype Open Source Development and Application Security Survey

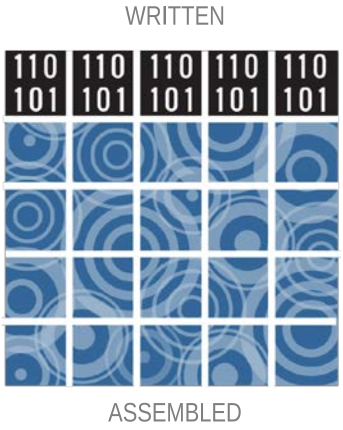
Local component management provides an opportunity for improved visibility and control.

Q: Which local component repository manager does your organization use? (multiple selections possible)



Source: 2014 Sonatype Open Source Development and Application Security Survey

Open source software (OSS) is essential



MOBILE

BIG DATA

WEB APPS

INTERNET OF THINGS

DEV OPS

AGILE DEV

...to help build your applications

Most applications are now assembled from hundreds of open source components…often reflecting as much as 90% of an application.

...and satisfy demand.

Open source helps meet accelerated development demand required for these growth drivers.

HOW PREPARED WERE WE FOR HEARTBLEED?

THE 2014 RESULTS HOLD SIGNIFICANT IMPORTANCE FOR THOSE OF US IN THE OPEN SOURCE DEVELOPMENT AND APPLICATION SECURITY COMMUNITY. WE BELIEVE THIS SURVEY REPRESENTS THE MOST COMPREHENSIVE PERSPECTIVES ON THE STATE OF OPEN SOURCE SECURITY AT THE TIME OF THE CATASTROPHIC HEARTBLEED BUG ANNOUNCEMENT.

APRIL 1ST
SURVEY
INITIATED

1,513
PRE-HEARTBLEED
RESPONSES

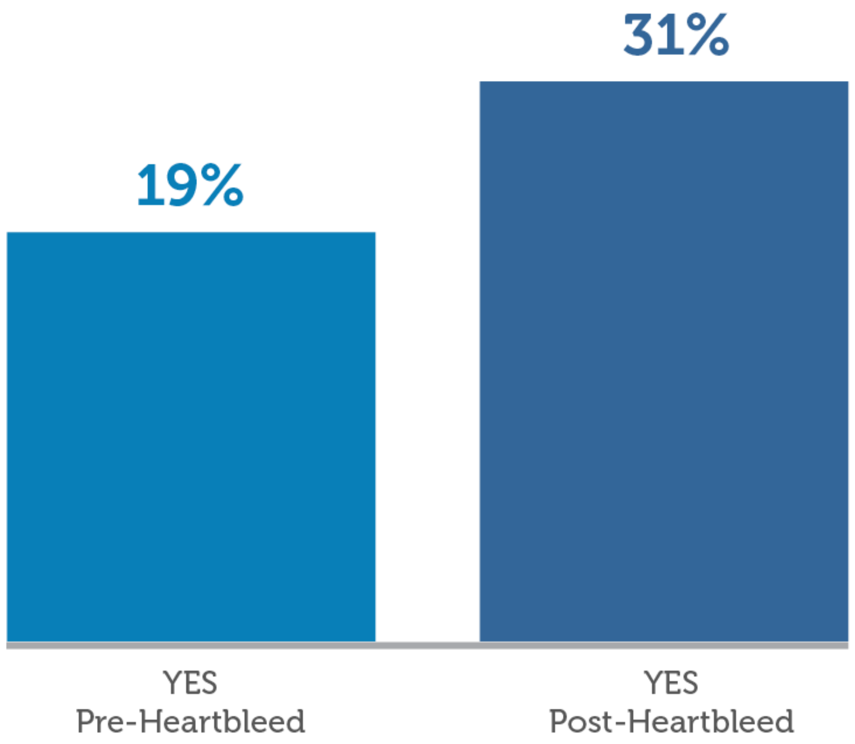
APRIL 7TH
HEARTBLEED
ANNOUNCED

1,839
POST-HEARTBLEED
RESPONSES

APRIL 30TH
SURVEY
CLOSED

Heartbleed heightened concerns over open source-related breaches.

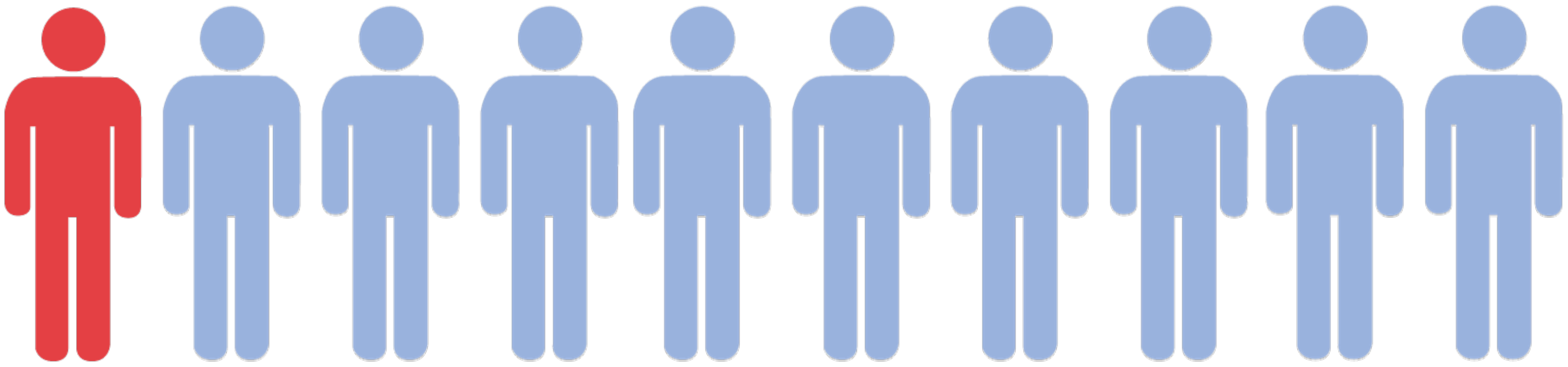
Q: Has your organization had a breach that can be attributed to a vulnerability in an open source component or dependency in the last 12 months?



Heartbleed threw the tech world off kilter

Source: 2014 Sonatype Open Source Development and Application Security Survey

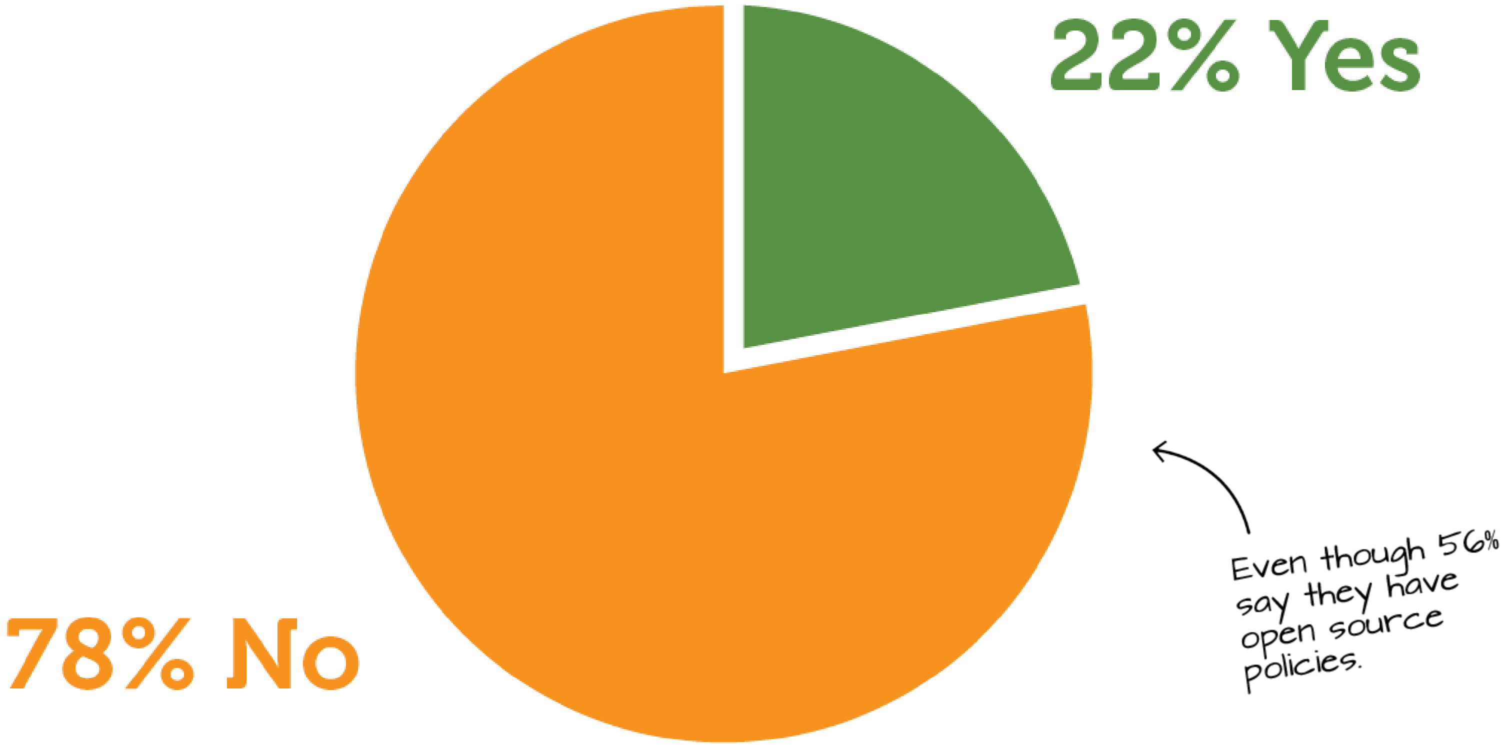
1-in-10 had or suspected an open source related breach in the past 12 months



Source: 2014 Sonatype Open Source Development and Application Security Survey

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?



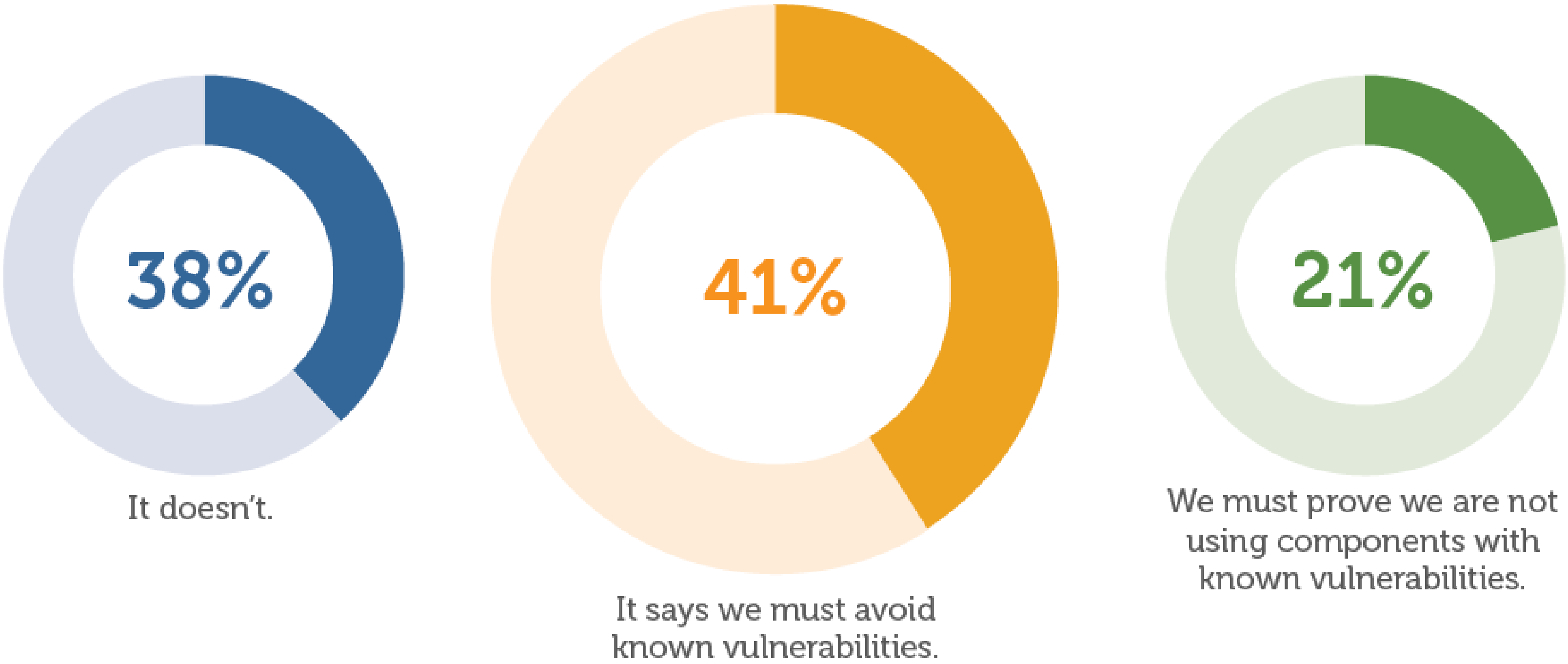
Even though 56% say they have open source policies.

Source: 2014 Sonatype Open Source Development and Application Security Survey

Only 21% of organizations must prove they are using secure components.

More than 1-in-3 say their open source policy doesn't cover security.

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

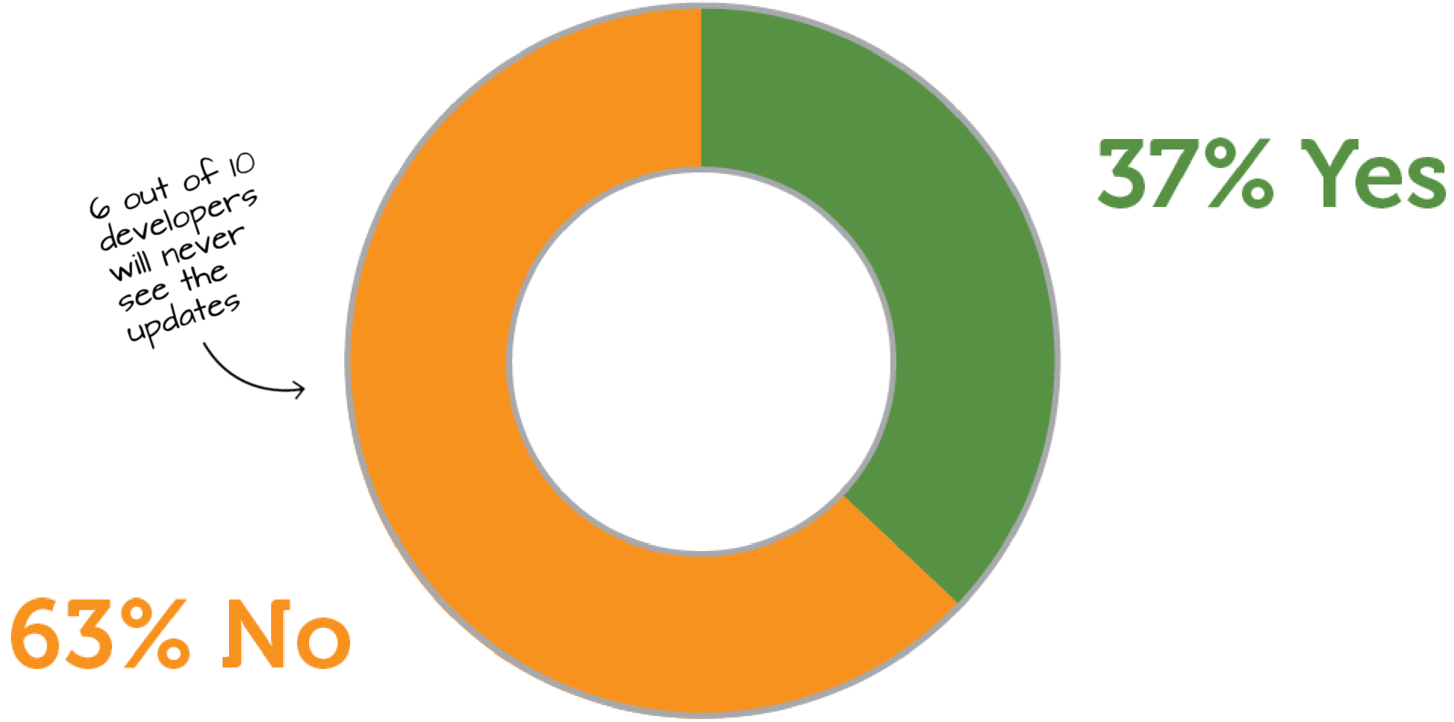


Source: 2014 Sonatype Open Source Development and Application Security Survey

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].

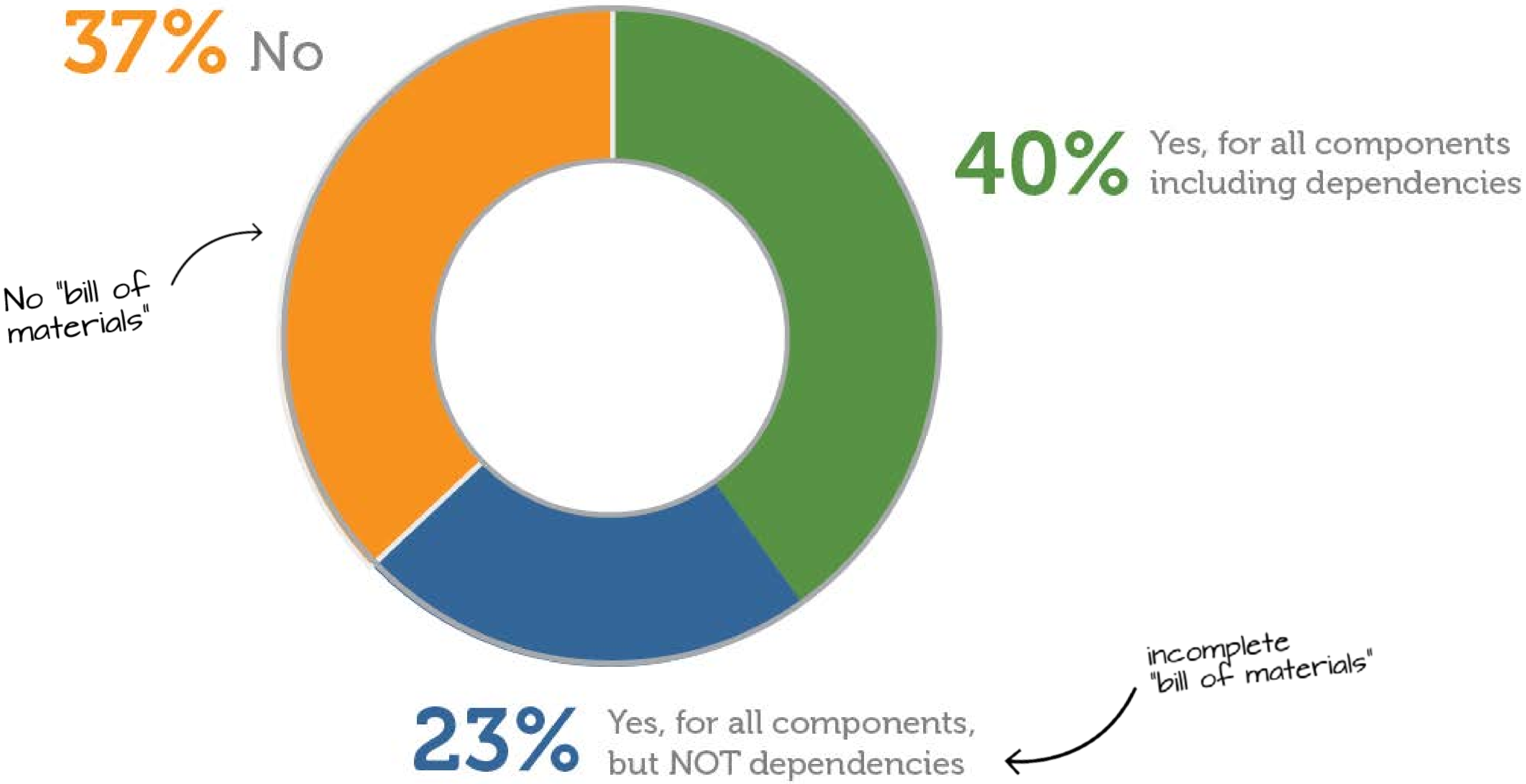
Q: Does someone actively monitor your components for changes in vulnerability data?



Source: 2014 Sonatype Open Source Development and Application Security Survey; [1]Sonatype, Inc. analysis of the (Maven) Central Repository

Even if they monitored new vulnerabilities, 6-in-10 could not track them down in production applications.

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



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

BACKGROUND: HUGE VOLUMES OF VULNERABLE OPEN SOURCE COMPONENTS CONTINUE TO GET DOWNLOADED LONG AFTER PUBLIC DISCLOSURE OF VULNERABILITIES AND AVAILABILITY OF FIXED VERISONS.

STRUTS2

WEB APPLICATION FRAMEWORK

CVE -2013-2251
Release Date: July 20, 2013
CVSS v2 Base Score: **9.3 HIGH**
Impact Subscore: **10.0**
Exploitability Subscore: **8.6**

Since then,
4,076 organizations
have downloaded it
179,050 times

HTTP CLIENT

HTTP IMPLEMENTATION FOR JAVA

CVE -2012-5783
Release Date: November 4, 2012
CVSS v2 Base Score: **5.8 MEDIUM**
Impact Subscore: **4.9**
Exploitability Subscore: **8.6**

Since then,
29,468 organizations
have downloaded it
3,749,193 times

BOUNCY CASTLE

CRYPTOGRAPHY API

CVE -2007-6721
Release Date: March 30, 2009
CVSS v2 Base Score: **10.0 HIGH**
Impact Subscore: **10.0**
Exploitability Subscore: **10.0**

Since then,
11,236 organizations
have downloaded it
214,484 times

JETTY

WEB APPLICATION SERVER

CVE -2009-4611
Release Date: January 13, 2010
CVSS v2 Base Score: **5.0 MEDIUM**
Impact Subscore: **2.9**
Exploitability Subscore: **10.0**

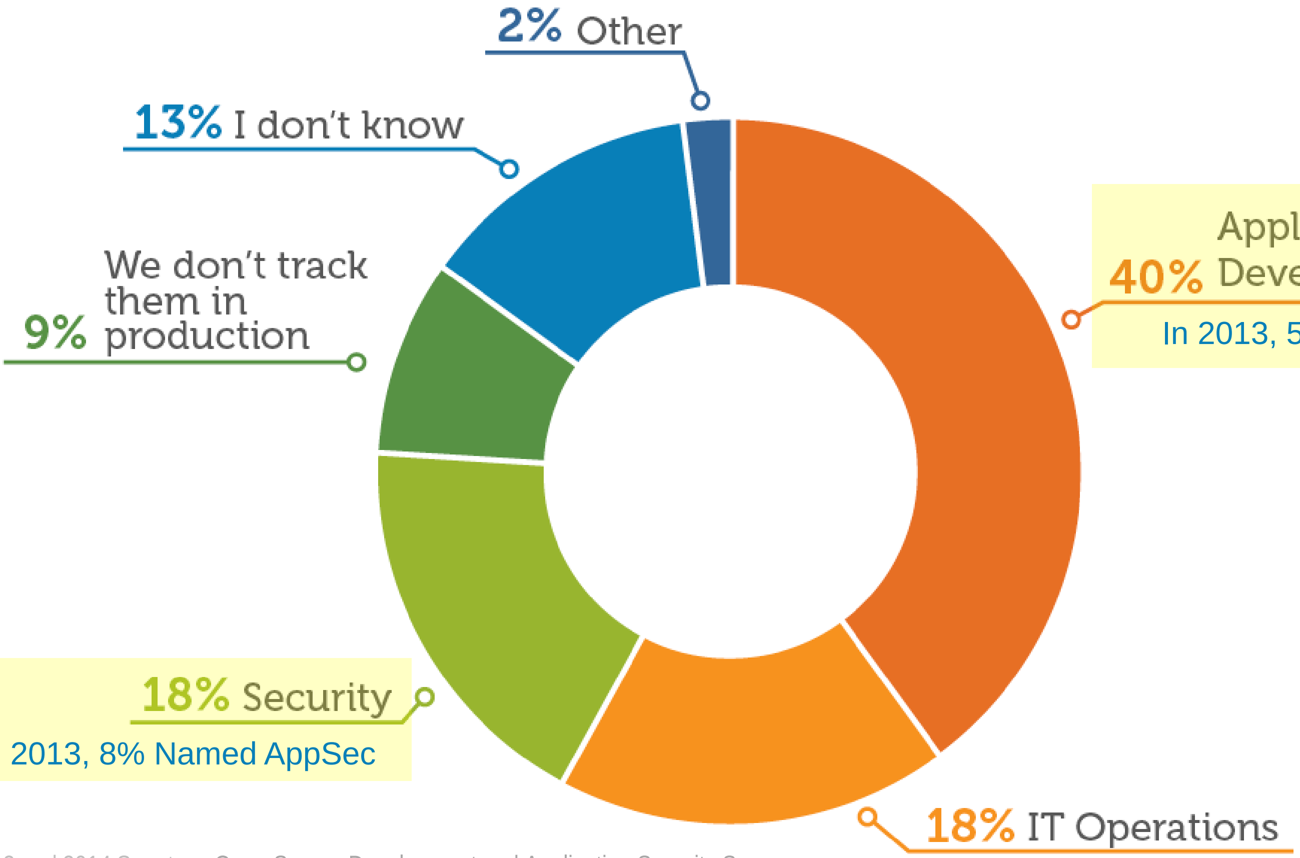
Since then,
36,181 organizations
have downloaded it
5,174,913 times

If you are not using secure components, you're not building secure applications

Source: Sonatype, Inc. analysis of the (Maven) Central Repository

Responsibility for tracking and resolving vulnerabilities is shifting from Application Development to Application Security.

*Q: Who has responsibility for tracking & resolving newly discovered component vulnerabilities in *production* applications?*



In 2013, 50% Named AppDev

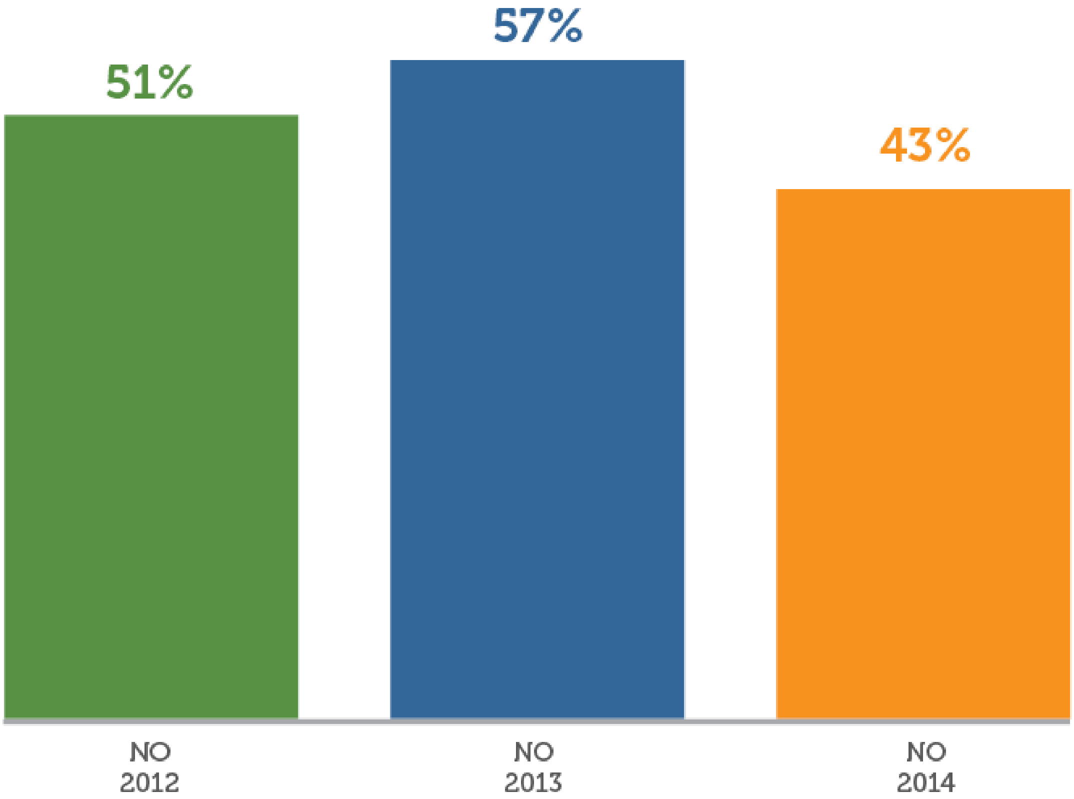
In 2013, 8% Named AppSec

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

ARE OPEN SOURCE POLICIES KEEPING OUR APPLICATIONS SAFE?

Half of organizations continue to run without an open source policy.

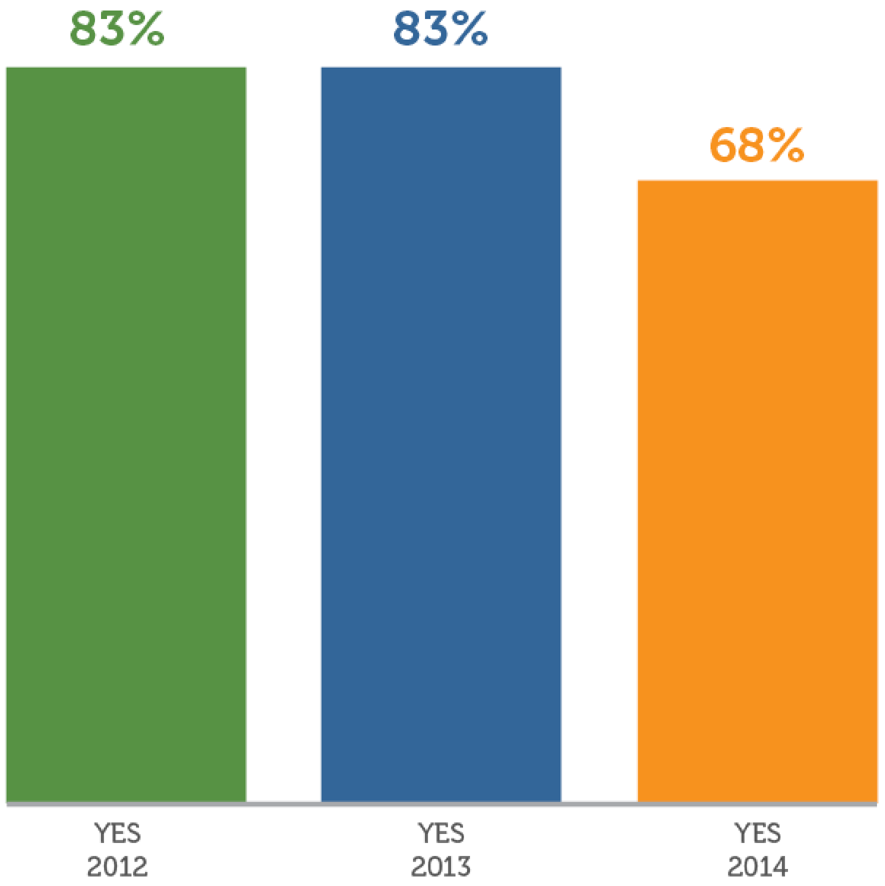
Q: Does your organization have an open source policy?



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?

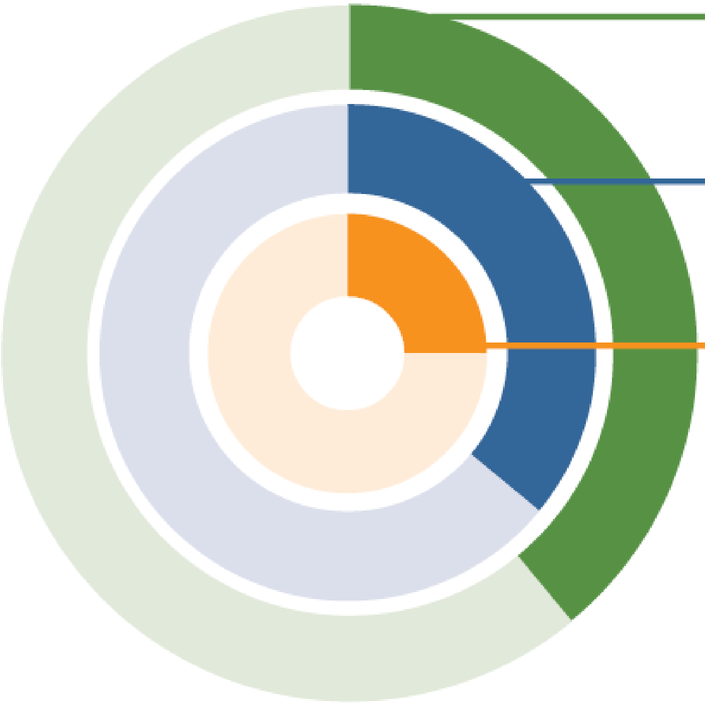


Source: 2012, 2013, 2014 Sonatype Open Source Development and Application Security Survey

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?



39% Yes, we have some corporate standards, but they aren't enforced.

36% There are no standards. Each developer or team chooses the components that are best for their project.

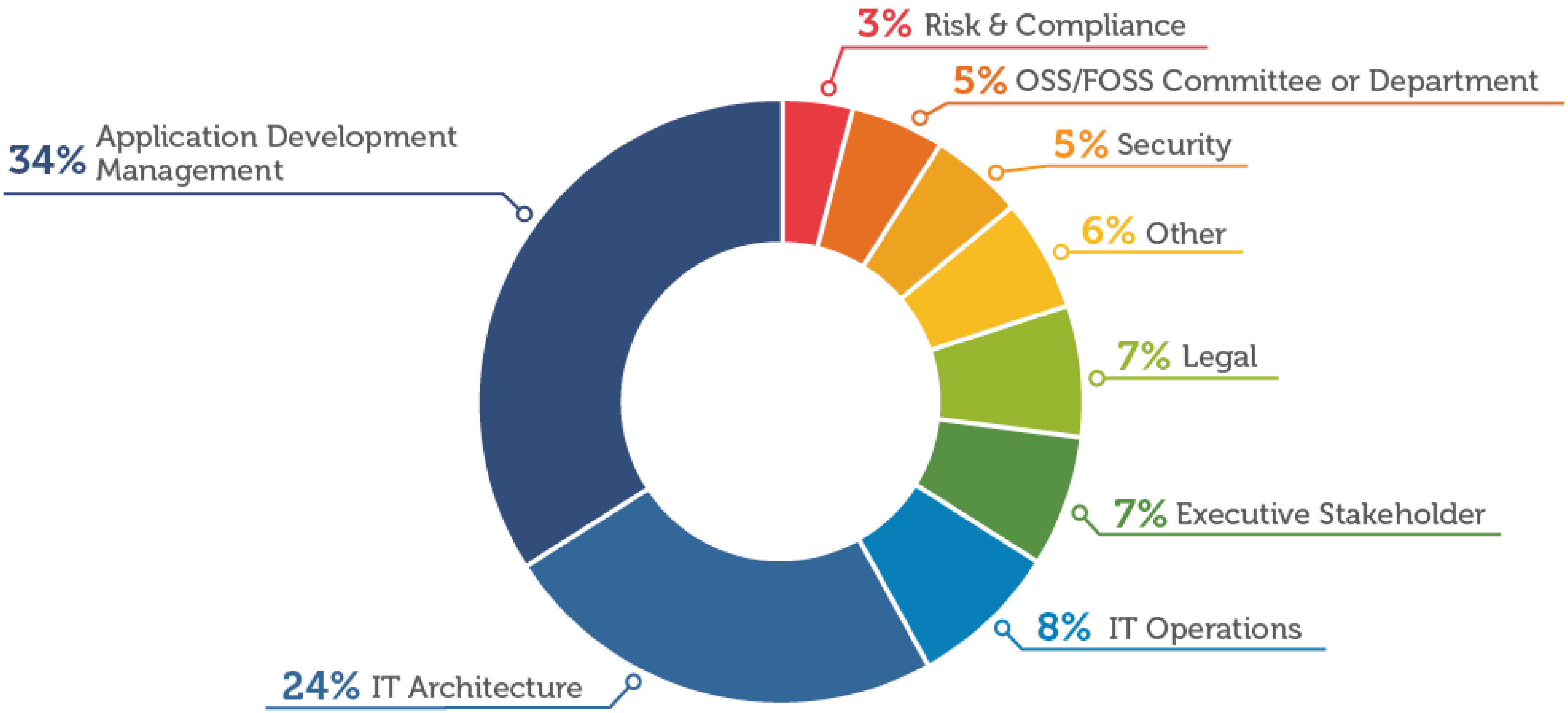
25% We're completely locked down. We can only use approved components.

Source: 2014 Sonatype Open Source Development and Application Security Survey

AppDev and IT architects take the lead in OSS policies & governance.

But control is not unanimous.

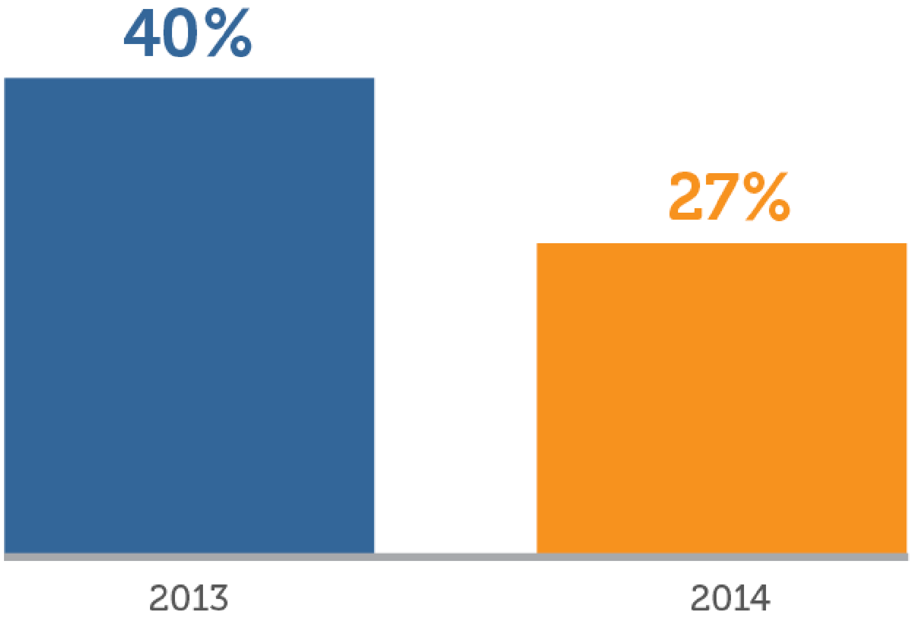
Q: Who in your organization has PRIMARY responsibility for open source policy/governance?



Source: 2014 Sonatype Open Source Development and Application Security Survey

While application development takes the lead in open source policy, only 1-in-4 developers consider it a top concern.

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

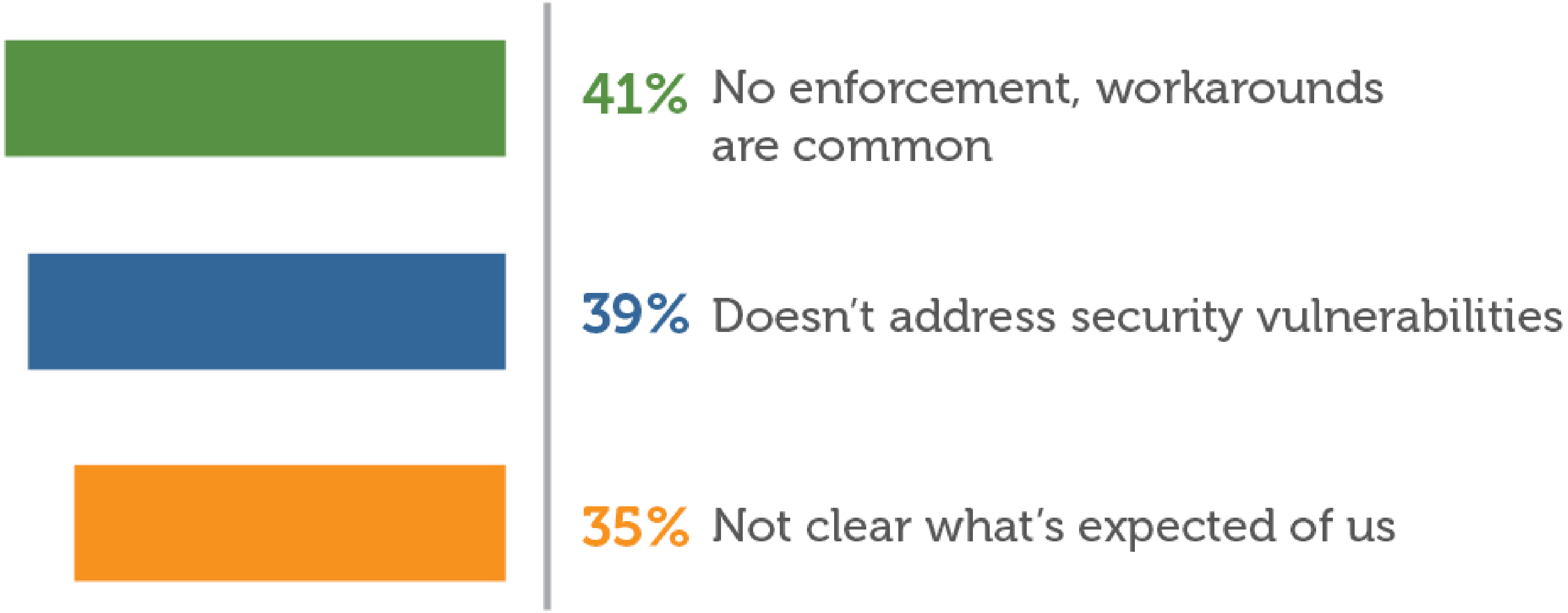


It's a top concern for our developers. They spend a lot of time here.

Source: 2013 and 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)



41% No enforcement, workarounds are common

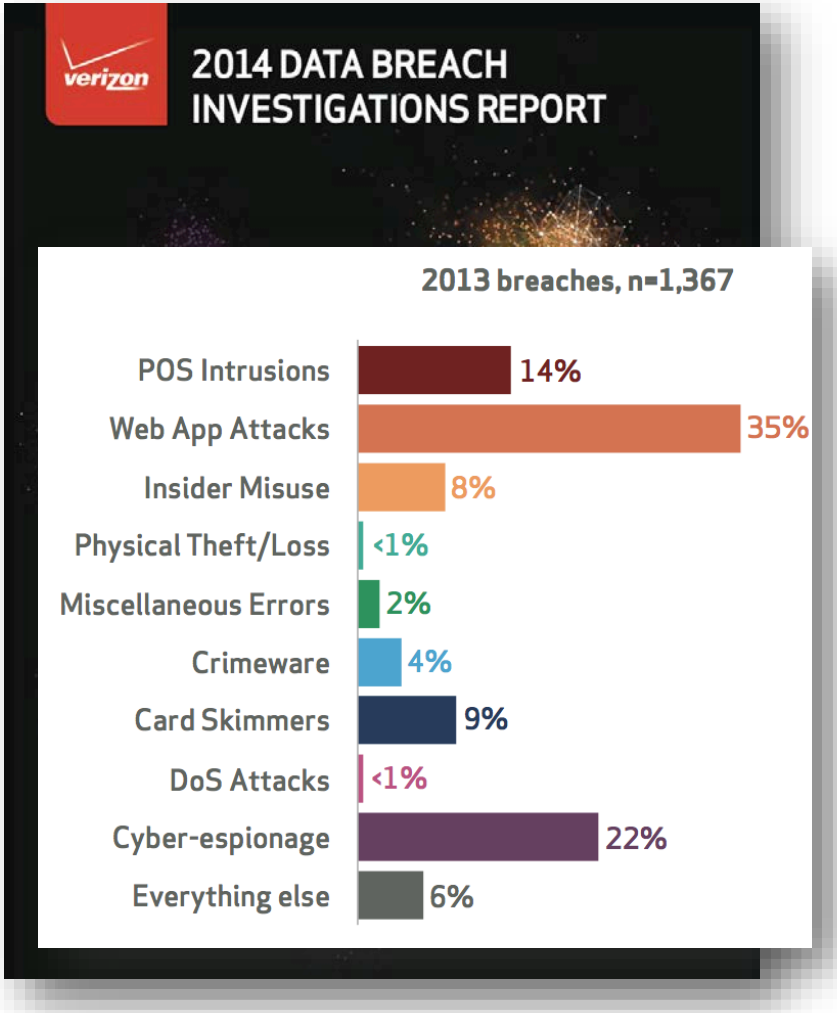
39% Doesn't address security vulnerabilities

35% Not clear what's expected of us

Source: 2014 Sonatype Open Source Development and Application Security Survey

APPLICATIONS ARE THE #1 ATTACK VECTOR LEADING TO BREACHES

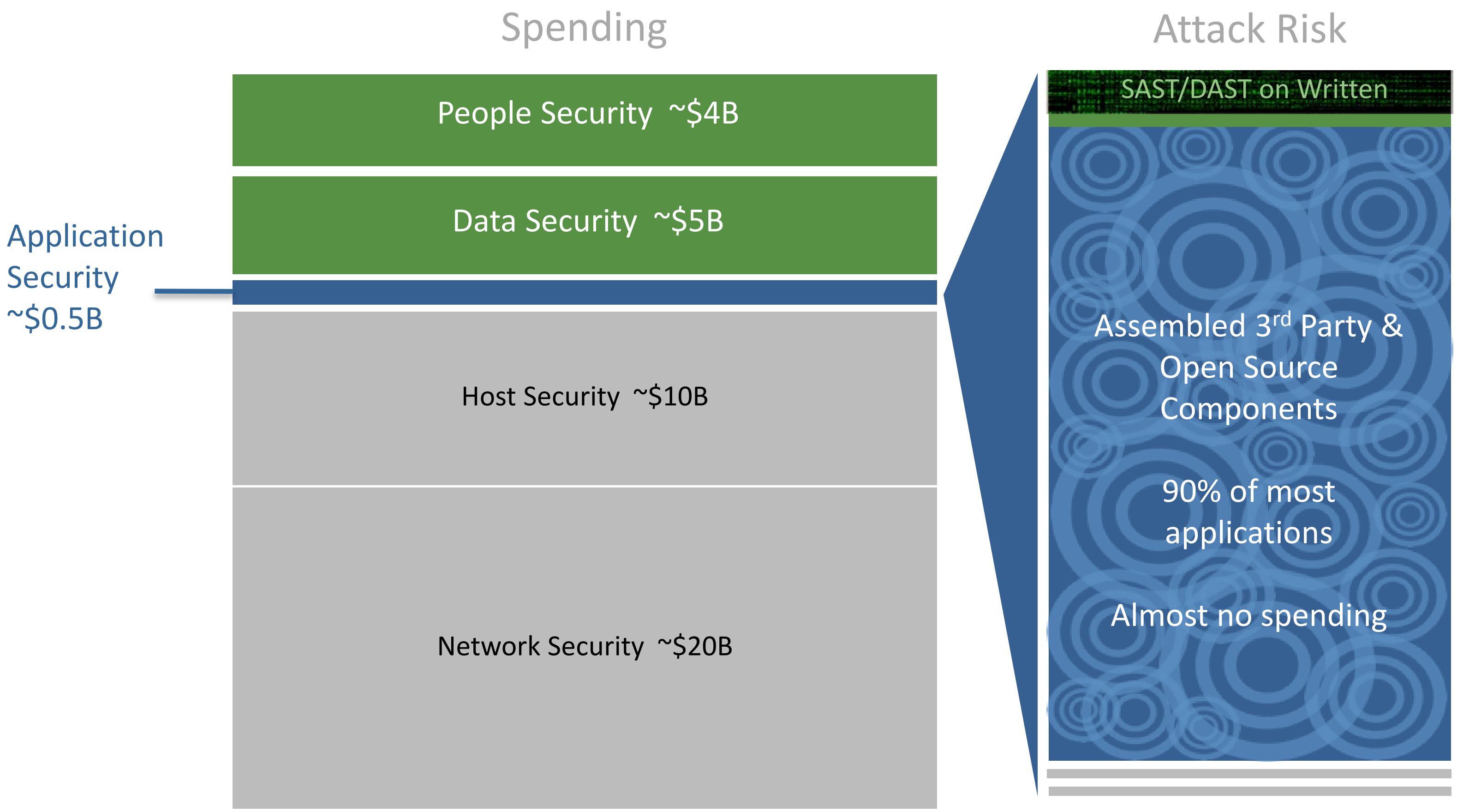
BACKGROUND: APPLICATIONS ACCOUNT FOR MORE BREACHES THAN CYBER-ESPIONAGE, CRIMEWARE, INSIDER MISUSE, AND DOS ATTACKED COMBINED.



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

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

BACKGROUND: SPENDING AND RISK ARE OUT OF SYNC. THE LOWEST PERCENT OF SECURITY BUDGETS ARE ASSIGNED APPLICATION SECURITY. YET, ACCORDING TO THE VERIZON REPORT, APPLICATIONS REPRESENT THE HIGHEST RISK.VECTOR FOR BREACHES. WORSE, WITHIN APPSEC, EXISTING BUDGETS GO TO THE 10% WRITTEN OF APPLICATIONS THAT ARE WRITTEN CODE.



Spending

People Security ~$4B

Data Security ~$5B

Application Security ~$0.5B

Host Security ~$10B

Network Security ~$20B

Attack Risk

SAST/DAST on Written

Assembled 3rd Party & Open Source Components

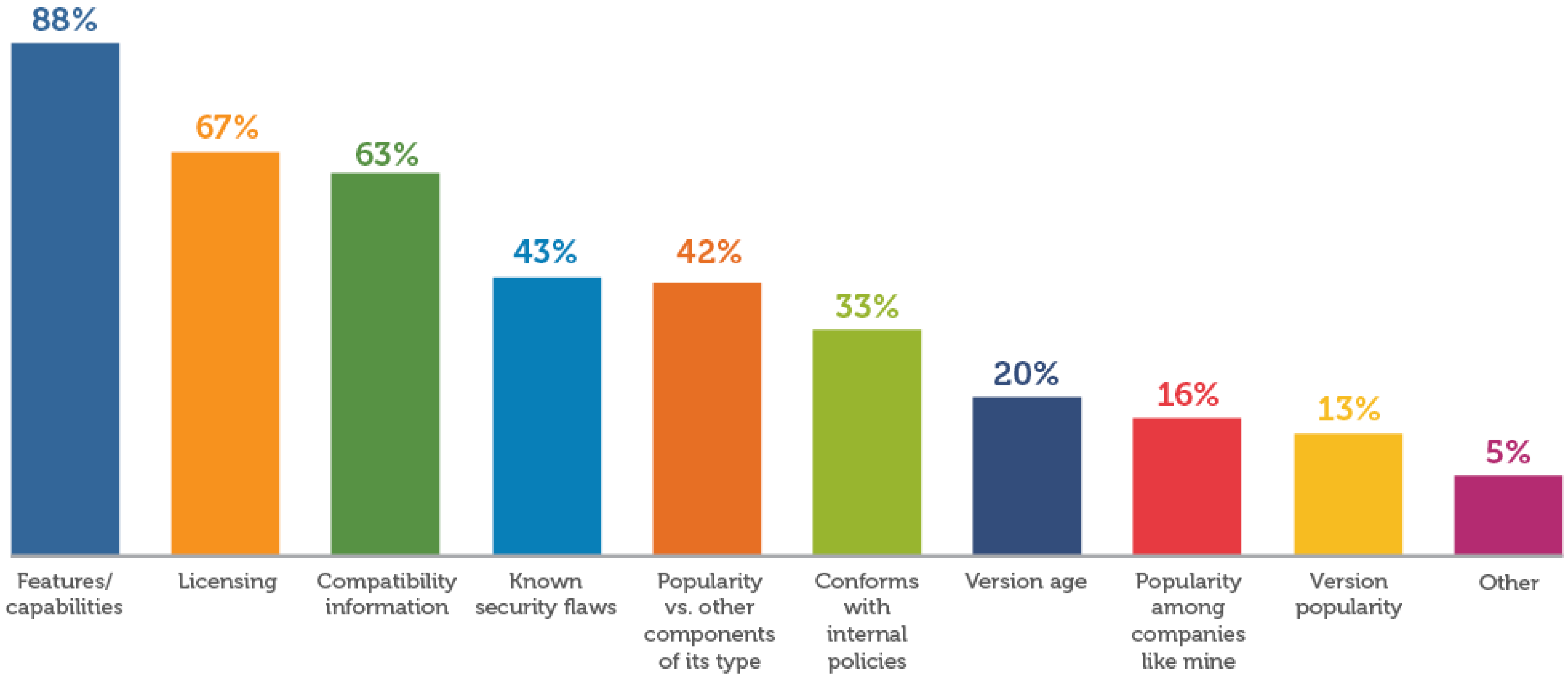
90% of most applications

Almost no spending

Source: Normalized spending numbers from IDC, Gartner, the 451 Group; since groupings vary

Developers want components that work and don't add risk

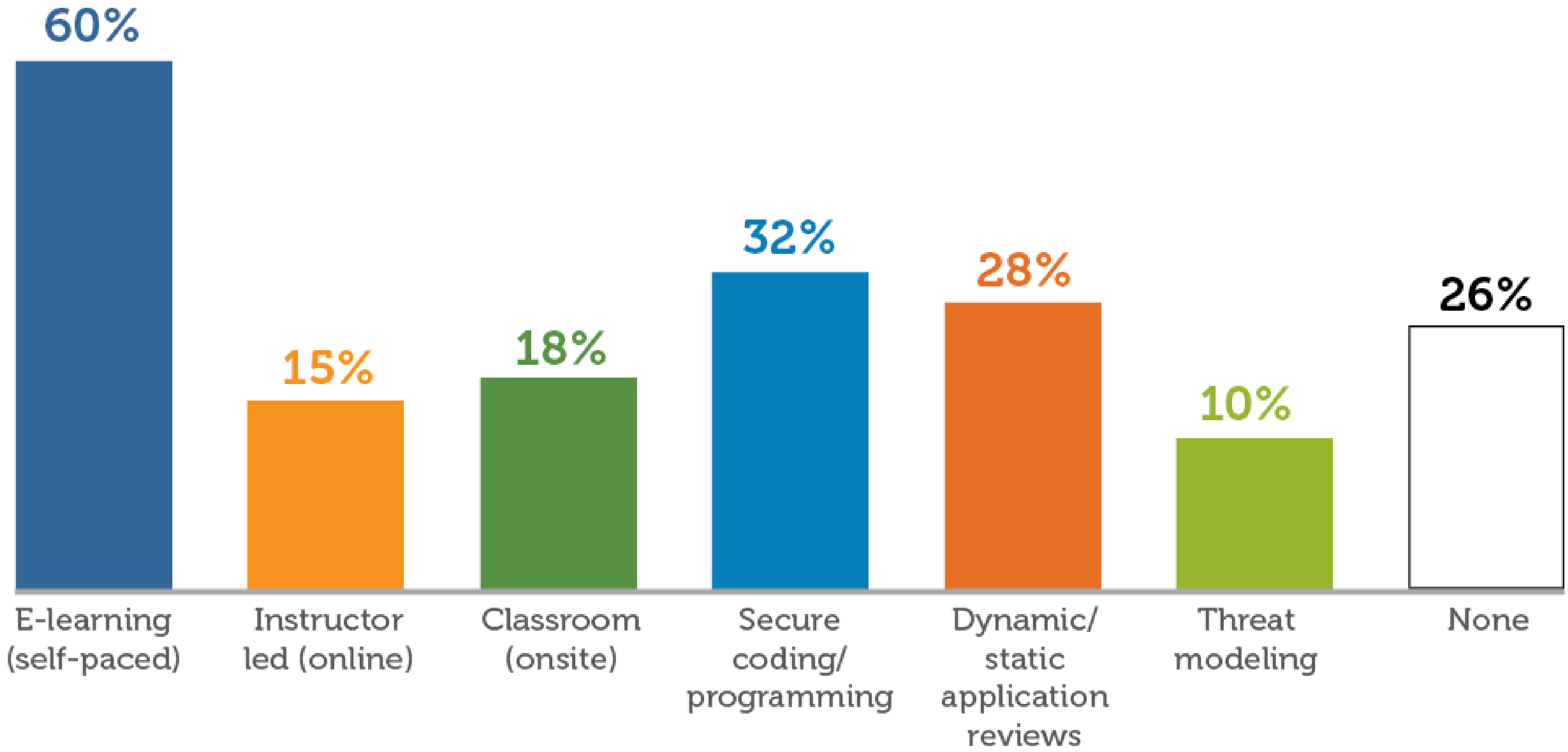
Q: When selecting components, which characteristics would be most helpful to you? (choose four)



Source: 2014 Sonatype Open Source Development and Application Security Survey

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? (multiple selections possible)

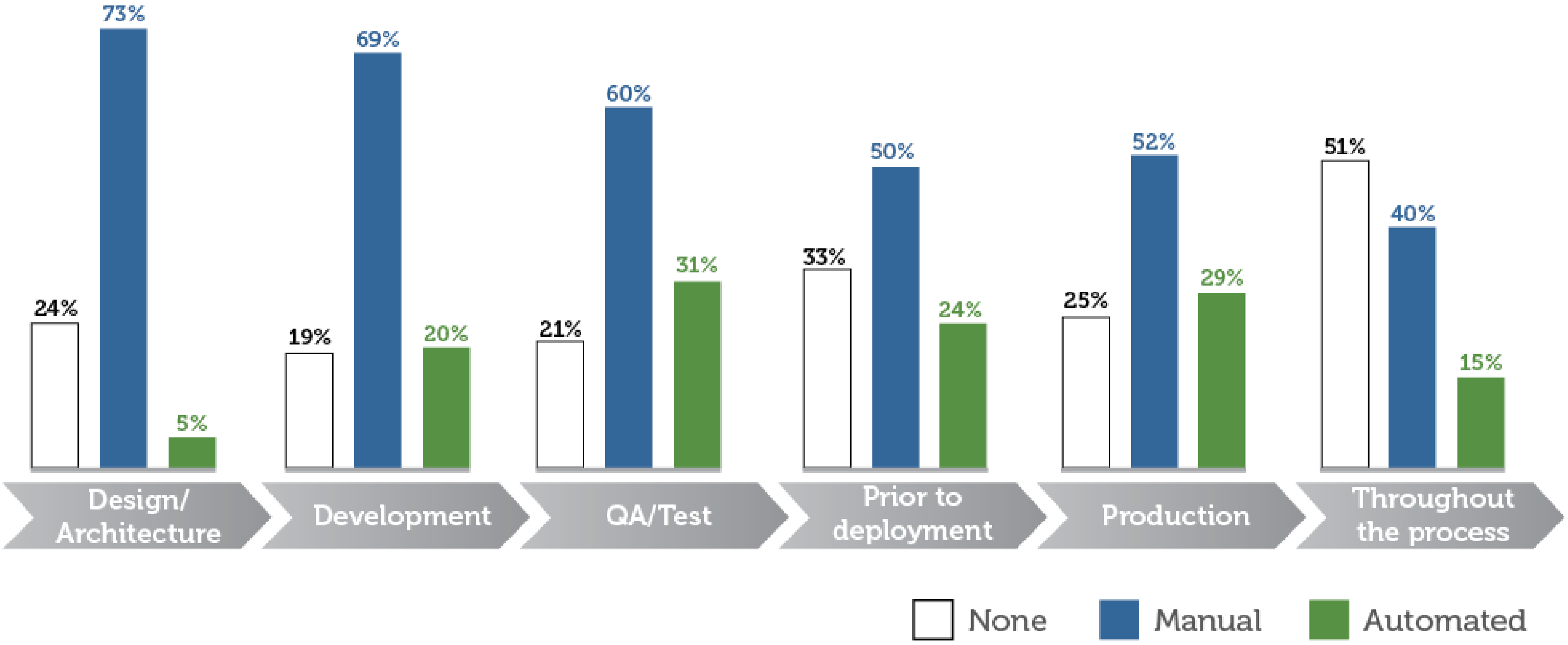


Source: 2014 Sonatype Open Source Development and Application Security Survey

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? Q: (multiple selections possible)



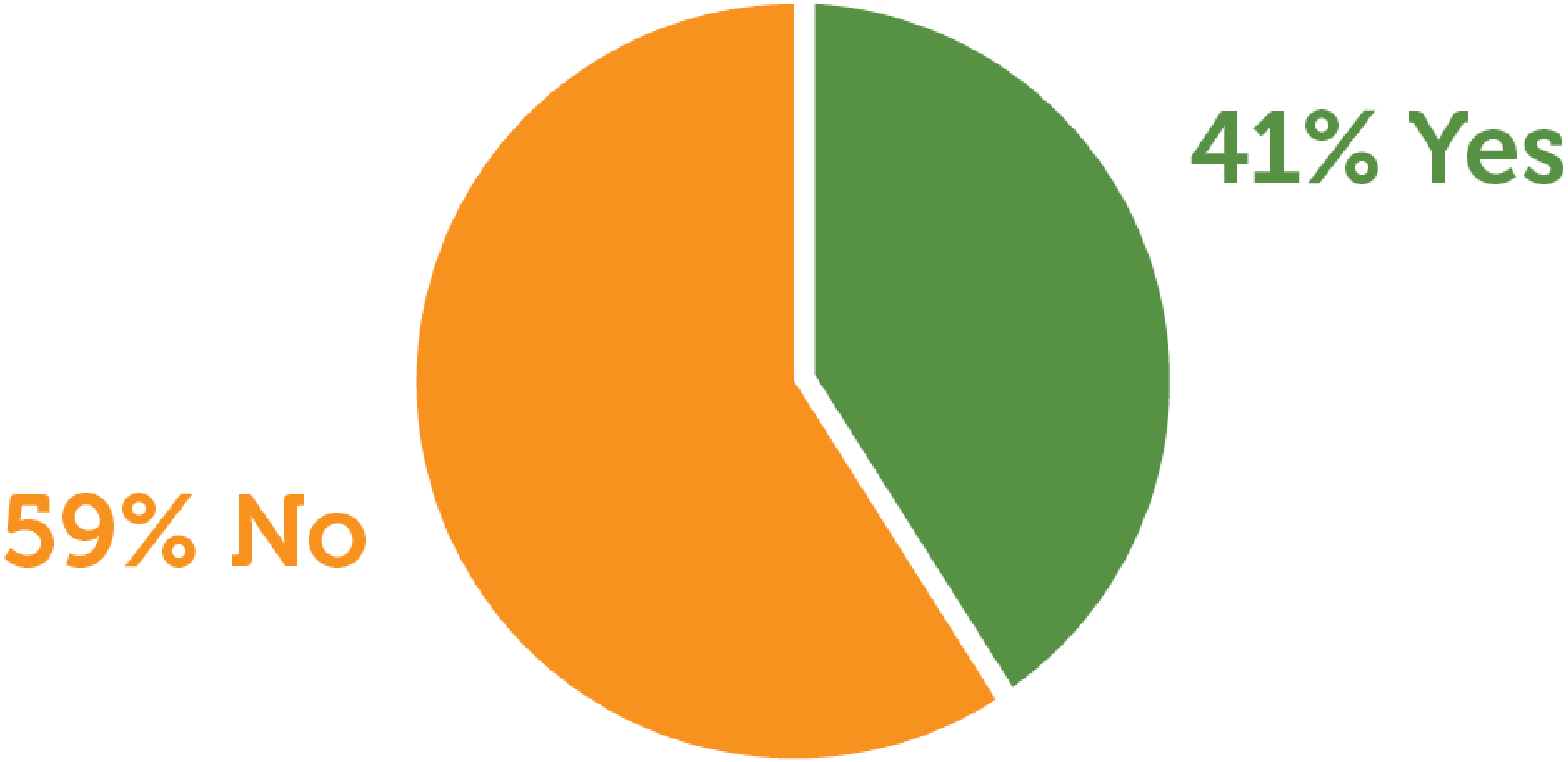
Source: 2014 Sonatype Open Source Development and Application Security Survey

WITH OPEN SOURCE COMES LICENSE CONSIDERATIONS

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.

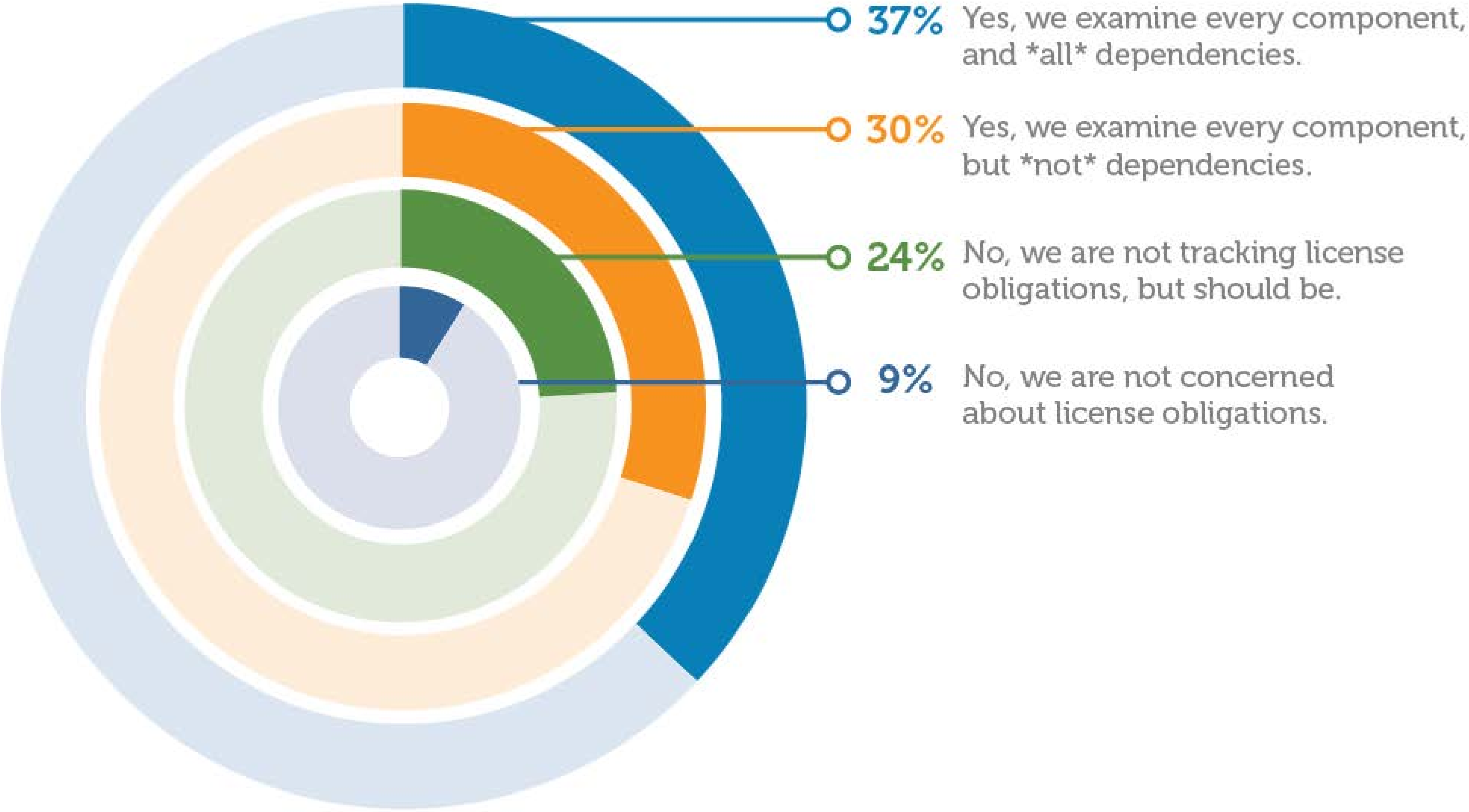
Q: Are open source licensing risks or liabilities a top concern in your position?



Source: 2014 Sonatype Open Source Development and Application Security Survey

63% have an incomplete view of license risk. 33% don’t manage it at all.

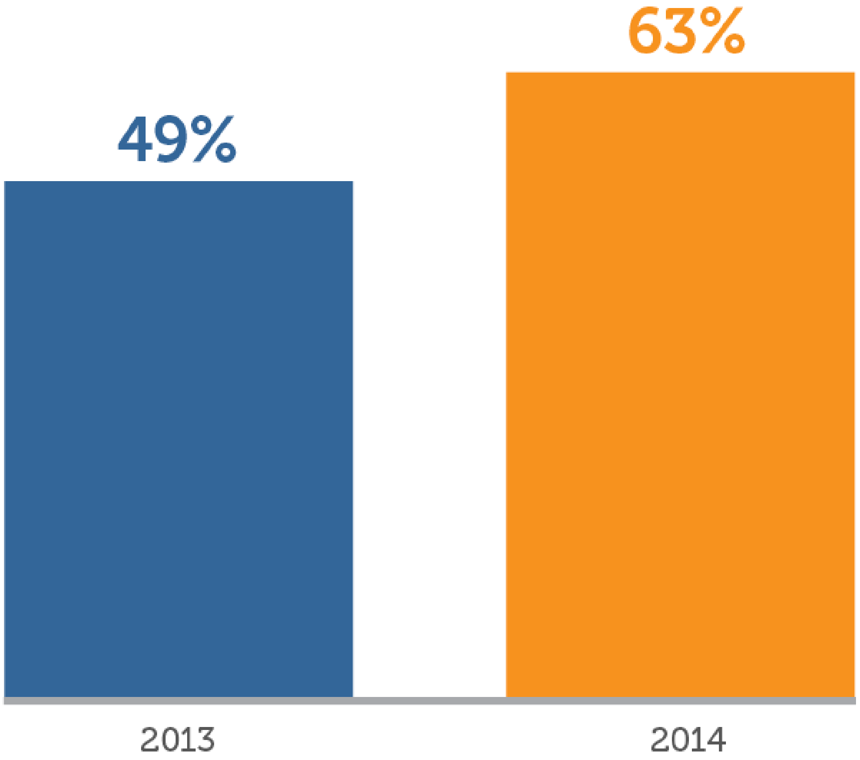
Q: Does your organization/policy manage the use of components by license types? (e.g., GPL, copyleft)?



Source: 2014 Sonatype Open Source Development and Application Security Survey

License risk on the rise

Q: Does your organization/policy manage the use of components by license types? (e.g., GPL, copyleft)?



Have no effective licensing policy.

If it doesn't have a license, you have no right to use it

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

Executive Summary

2014 Sonatype Open Source and Application Security Survey

BACKGROUND

- 90% of a typical application is assembled with open source components
- Open source component requests have grown to 13 billion annually
- Applications are the #1 attack vector leading to breaches
- Applications receive the lowest percentage of security investments

Yet

SURVEY RESULTS

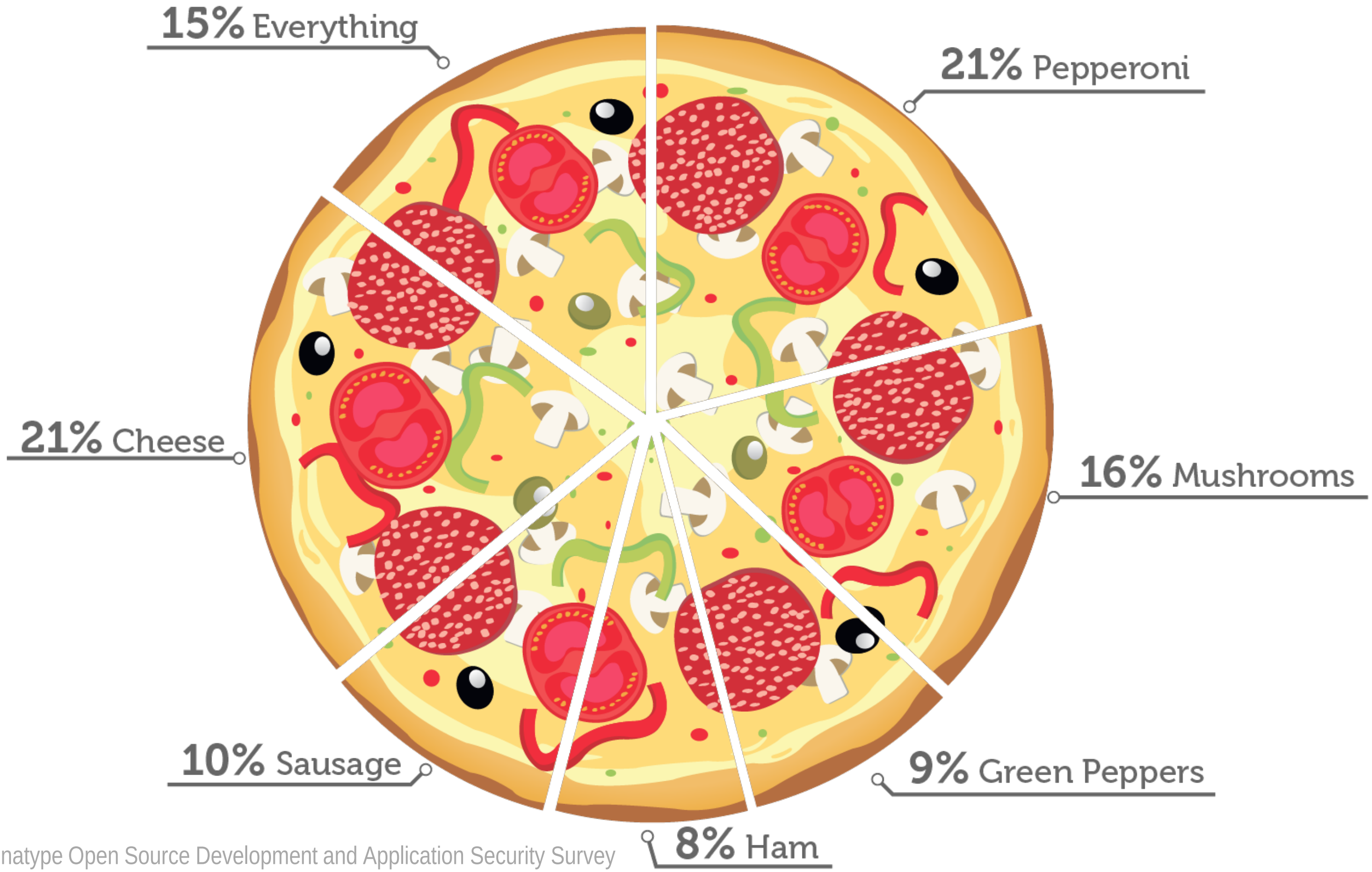
- *75% don't enforce or don’t have an OSS policy*
- *58% are not concerned about license risk*
- *63% don't actively monitor for changes in vulnerability data*
- *77% have never banned an open source component*
- *The majority of organizations rely on manual application security analysis*
- *31% had or suspect a breach due to an open source (OSS) component*

ON THE LIGHTER SIDE…

We know open source developers care about more than open source. They also eat pizza and now we've got the data to prove it ...

(Many were upset that bacon was not an option)

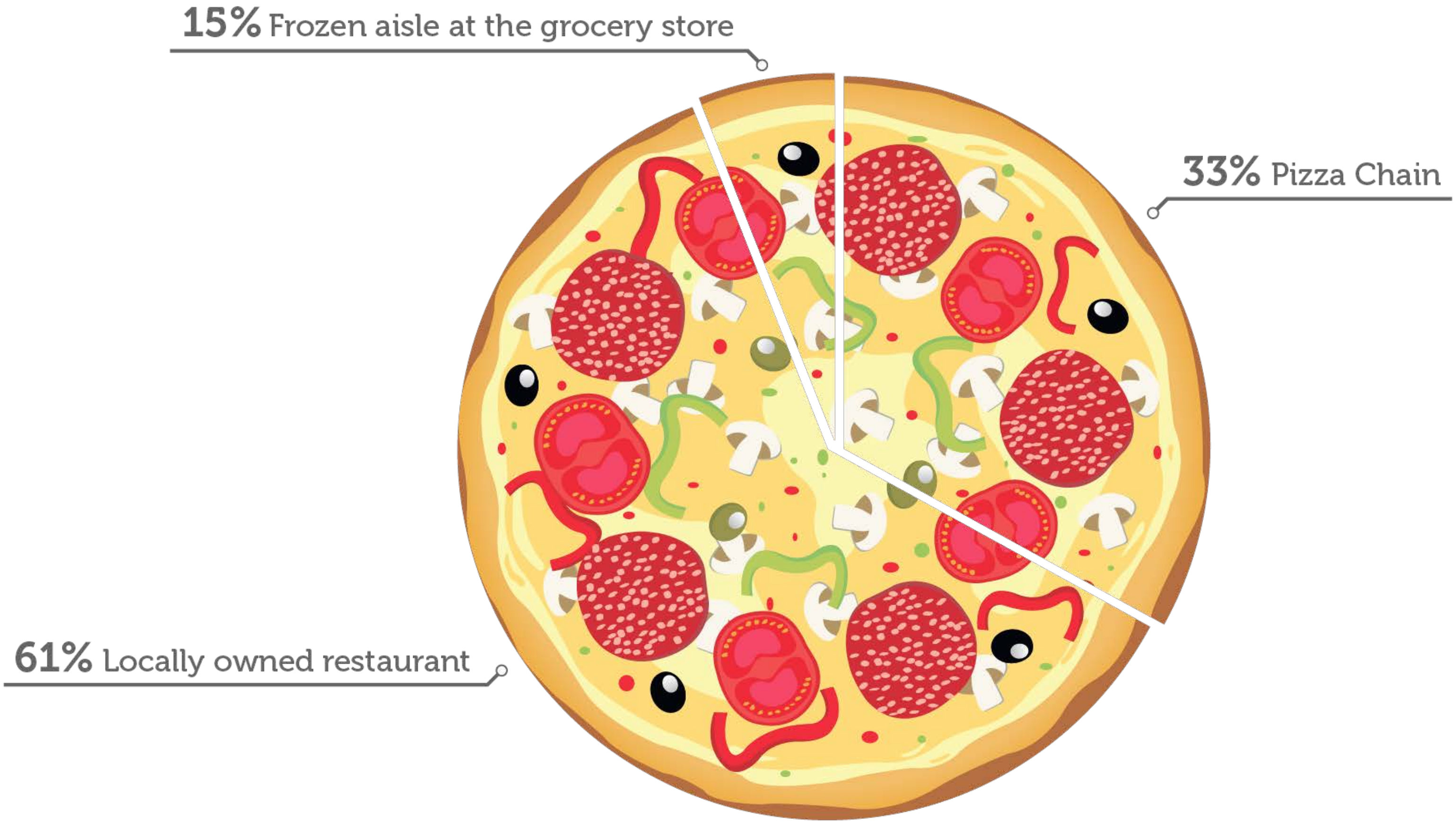
Q: What is your favorite pizza topping?



Source: 2014 Sonatype Open Source Development and Application Security Survey

They also prefer local pizza places …

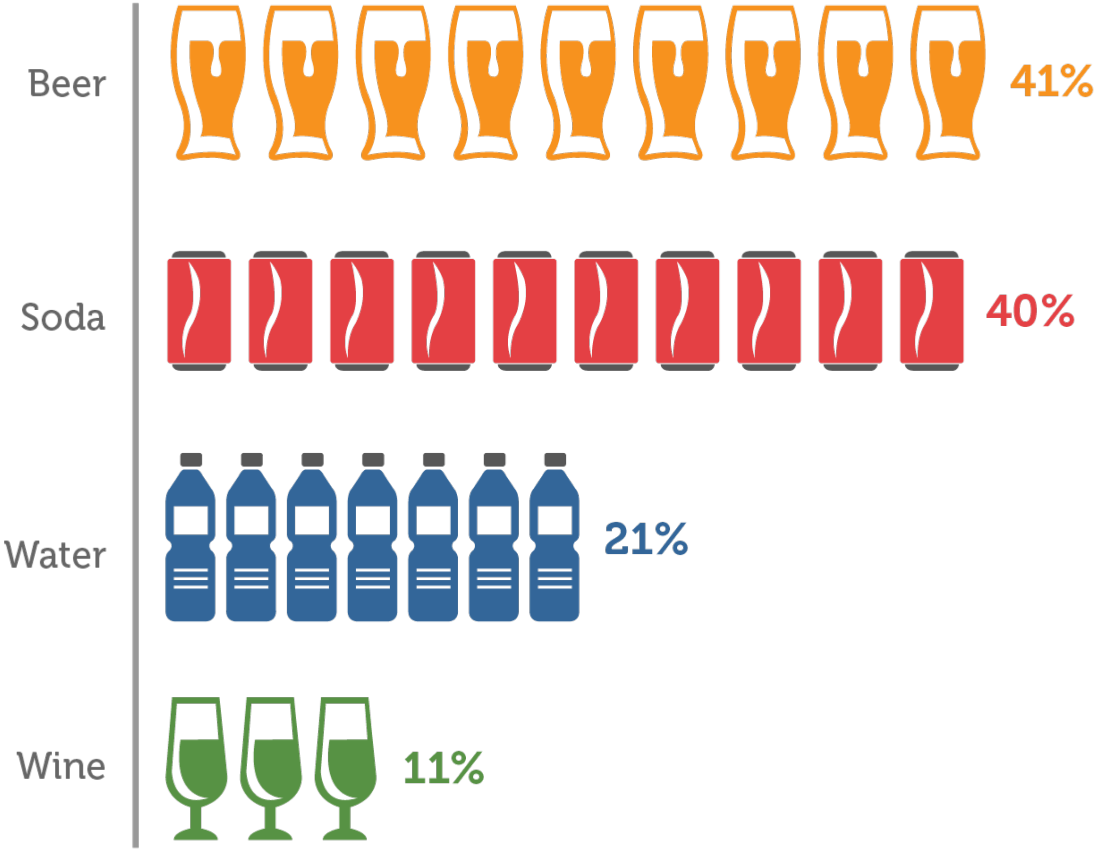
Q: Where do you get your pizza?



Source: 2014 Sonatype Open Source and Application Security Survey

…and prefer beer 4-to-1 over wine.

Q: What do you like to drink with your pizza?



Source: 2014 Sonatype Open Source Development and Application Security Survey

About our sponsors

Sonatype

Every day, developers rely on millions of third party and open source building blocks – known as components – to build the software that runs our world. Sonatype ensures that only the best components are used throughout the software development lifecycle so that organizations don't have to make the tradeoff between going fast and being secure. Policy automation, ongoing monitoring and proactive alerts makes it easy to have full visibility and control of components throughout the software supply chain so that applications start secure and remain that way over time. Sonatype is privately held with investments from New Enterprise Associates (NEA), Accel Partners, Bay Partners, Hummer Winblad Venture Partners and Morgenthaler Ventures. Visit: www.sonatype.com

CONTRAST SECURITY

Contrast automatically identifies vulnerabilities and offers a continuous, real time, application security dashboard for every application. The advanced instrumentation-based vulnerability engine is not an external scanner, but an internal monitor which requires no scheduling, onboarding, or security expertise. The Contrast leadership team members are founding members of the Open Web Application Security Project (OWASP), and have made vast industry contributions including the OWASP Top Ten, Enterprise Security API (ESAPI), Application Security Verification Standard (ASVS), AntiSamy, and WebGoat. For more information, please visit www.contrastsecurity.com or follow @contrastsec.

NEA®

New Enterprise Associates, Inc. (NEA) is a leading venture capital firm focused on helping entrepreneurs build transformational businesses across multiple stages, sectors and geographies. With approximately $13 billion in committed capital, NEA invests in information technology, healthcare and energy technology companies at all stages in a company's lifecycle, from seed stage through IPO. The firm's long track record of successful investing includes more than 175 portfolio company IPOs and more than 300 acquisitions. In the U.S., NEA has offices in Menlo Park, CA; Boston, MA; New York, NY; Chicago, IL; and the Washington, D.C. metropolitan area. In addition, New Enterprise Associates (India) Pvt. Ltd. has offices in Bangalore and Mumbai, India and New Enterprise Associates (Beijing), Ltd. has offices in Beijing and Shanghai, China. For additional information, visit www.nea.com.

APPLICATION SECURITY TSWA TRUSTED SOFTWARE ALLIANCE

The Trusted Software Alliance was founded in May of 2013 to raise public and professional awareness of application security as a major risk in application development. We capture the thoughts, ideas and trends as seen by the most important voices in the appsec industry. This includes a series of "50 in 50 Interviews",working with OWASP on a best practices series for managing open source component risks, and promoting major industry surveys and reports.

RUGGED

We believe that the key to producing secure code is to change your software development culture. We have to get beyond looking at the technology and look at the software development organization that created it. We believe this evolution has to start with the people, process, technology, and culture of that organization. Rugged is not a process model – it doesn't require any particular practices or activities. Instead, Rugged is about outcomes – you decide the who, how, and when. We believe this evolution is a natural outcome of attempts to simplify and strengthen security stories. Learn more at https://www.ruggedsoftware.org

Please visit:

www.sonatype.com/2014survey

for the complete analysis, blogs, and the infographic detailing the 2014 Sonatype Open Source Development and Application Security Survey