DEVSECOPS COMMUNITY SURVEY 2017

Sonatype

PERFICIENT

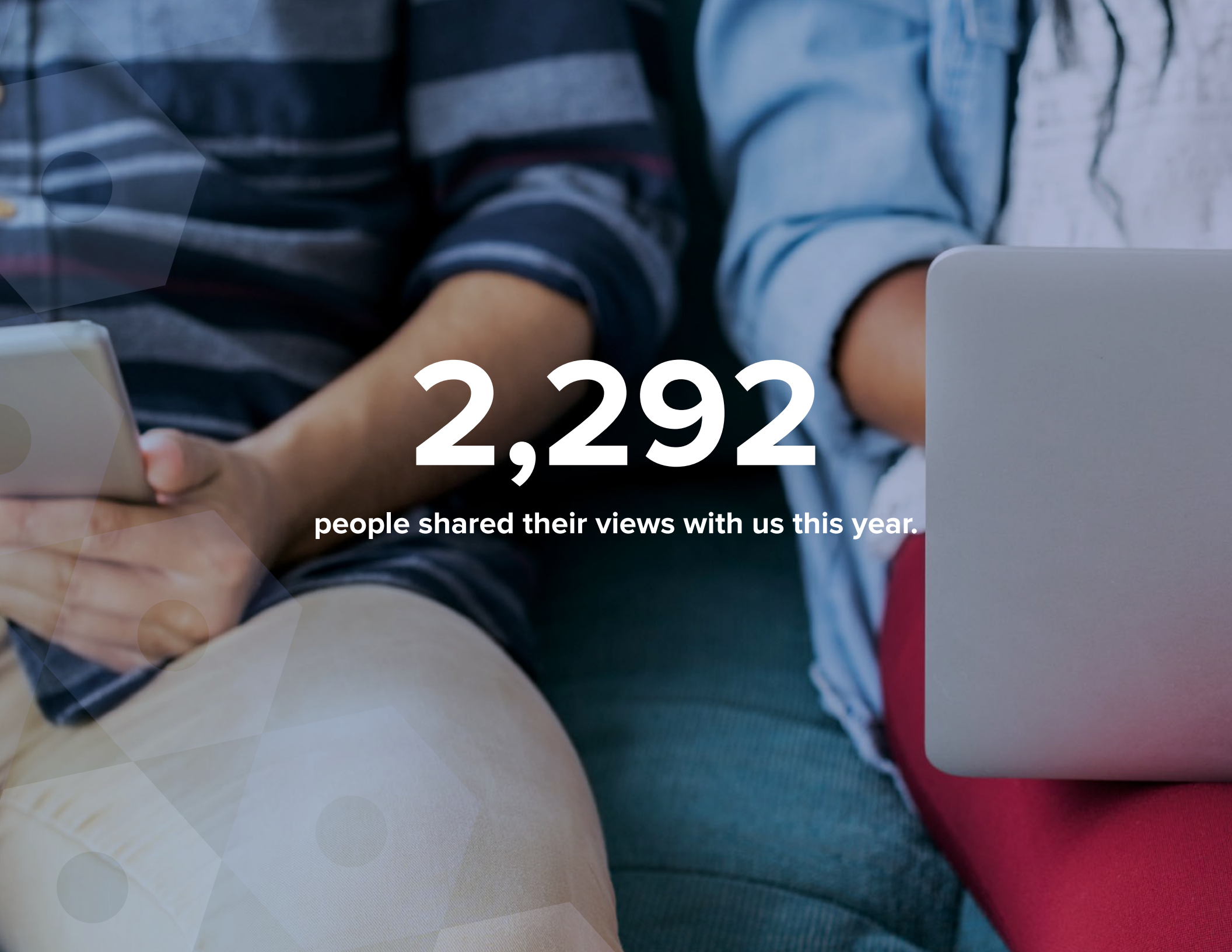
Signal Sciences

DZone

ranger4

emerasoft solutions to collaborate

CONTINO


2,292
people shared their views with us this year.

CEO **Message**

WAYNE JACKSON

Chief Executive Officer, Sonatype

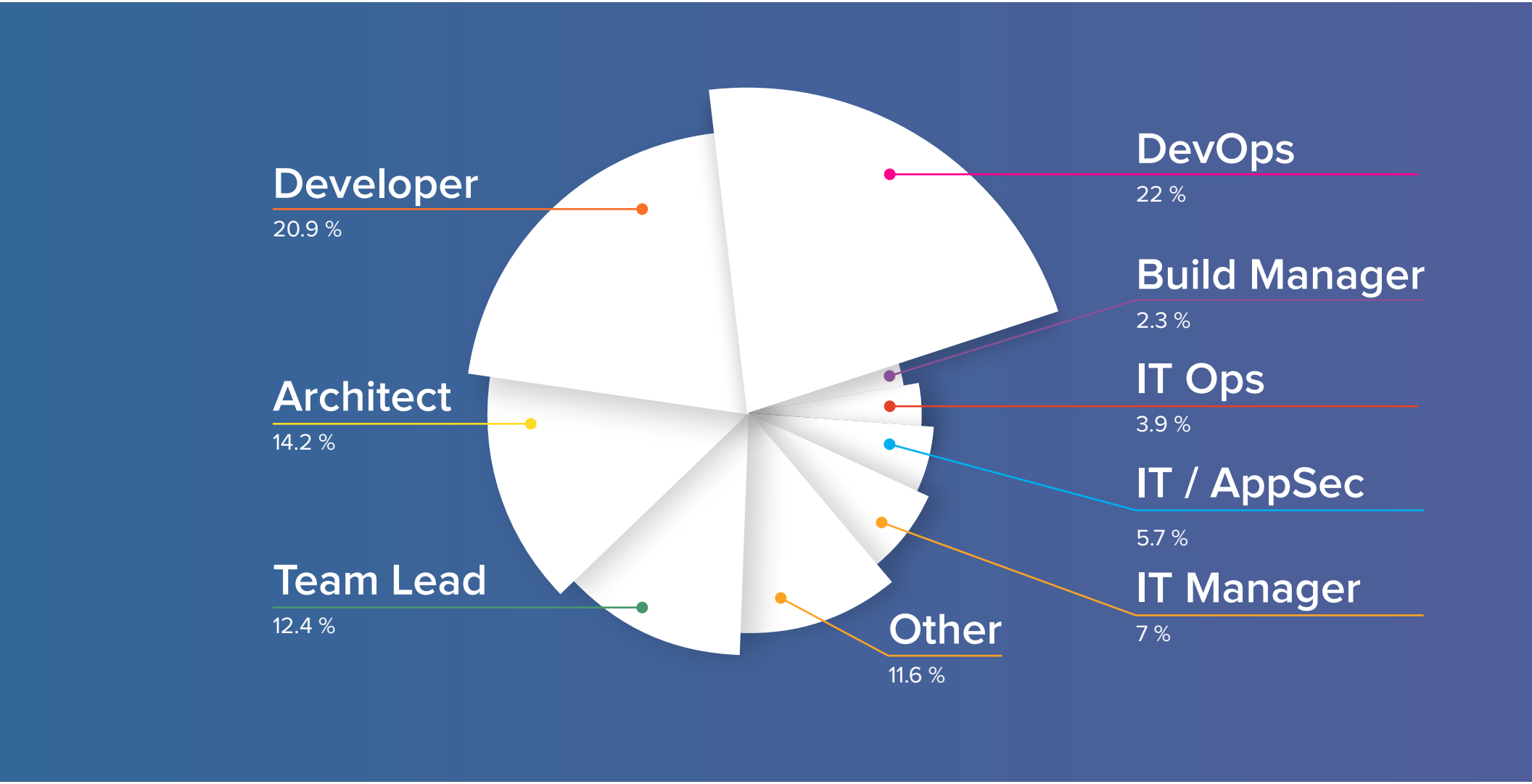
In the next few years, a growing number of enterprise DevOps initiatives will successfully incorporate automated security practices by moving away from waterfall-native tools, processes, and expectations. The DevSecOps community survey, representing the voice of 2,292 IT professionals demonstrates that DevOps practices are maturing rapidly, security is being automated earlier in the development lifecycle, and management of software supply chains is a critical differentiator.

While some results of our survey may surprise you, I hope they also encourage you to begin new conversations with your peers and across your industry. Sharing these results can help motivate all of us to further mature DevSecOps practices everywhere and to establish new benchmarks for speed, quality, and security.

Thank you to all of you who participated in the survey and to our community partners: Contino, DZone, Emerasoft, Ranger4, and Signal Sciences for helping us build this year's survey and promote its awareness.

WHO PARTICIPATED?

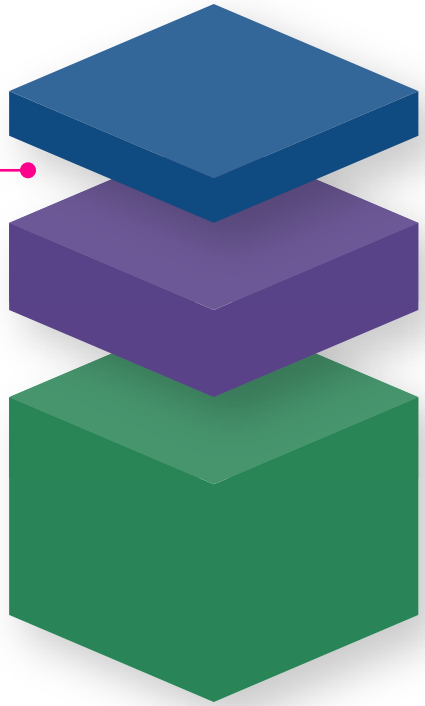
What is your role within the organization?



What is your level of seniority within the organization?

29 %

of participants were **managers or executives.**



Executive

6.5 %

Manager

22.9 %

Individual contributor

70.6%

How mature is your adoption of DevOps practices?

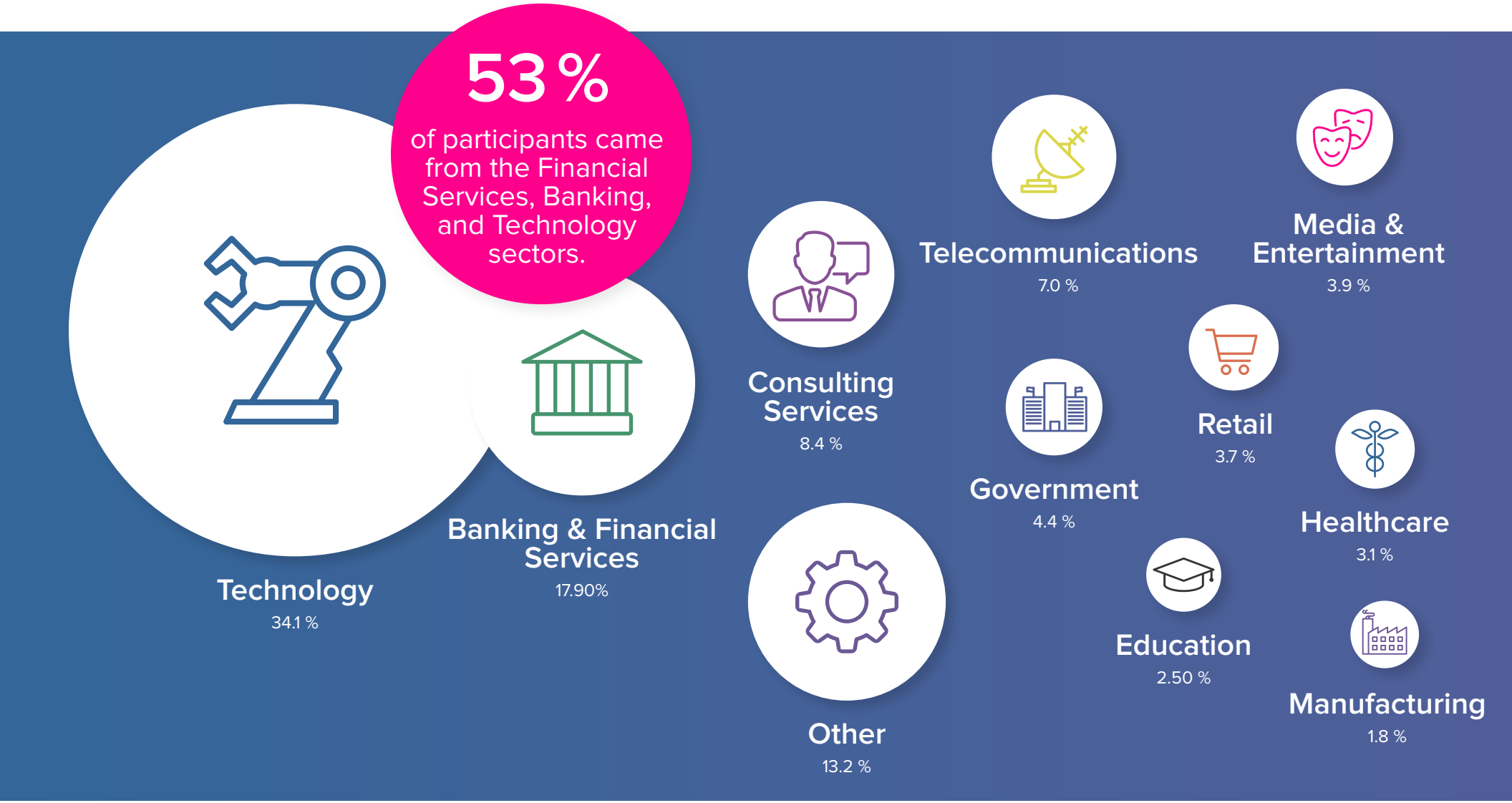
n = 2,115

HELEN BEAL

Ranger4

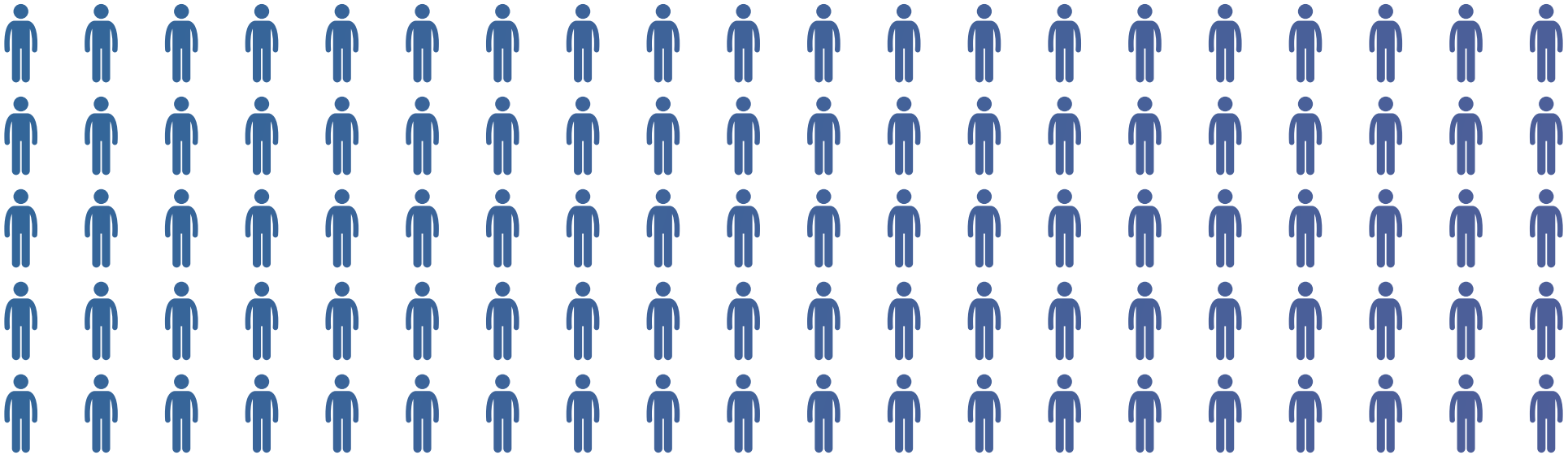
“DevOps is all about making better software faster. It also requires making software more safely while compressing the time between ideation to realization.”

In what industry is your company?



How many developers are in your organization?

48% HAVE MORE THAN **100** DEVELOPERS.



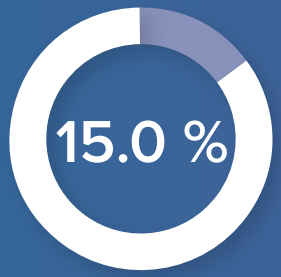
How many IT Operations professionals are in your organization?

Developers often outnumber IT Operations 10:1

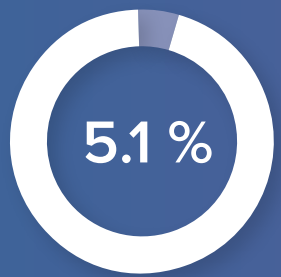
44 %
have less then 25 IT Operations professionals

1 - 25

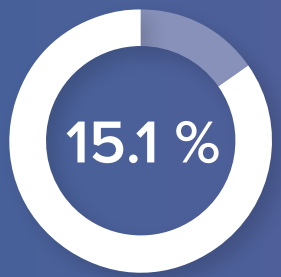
26 - 100



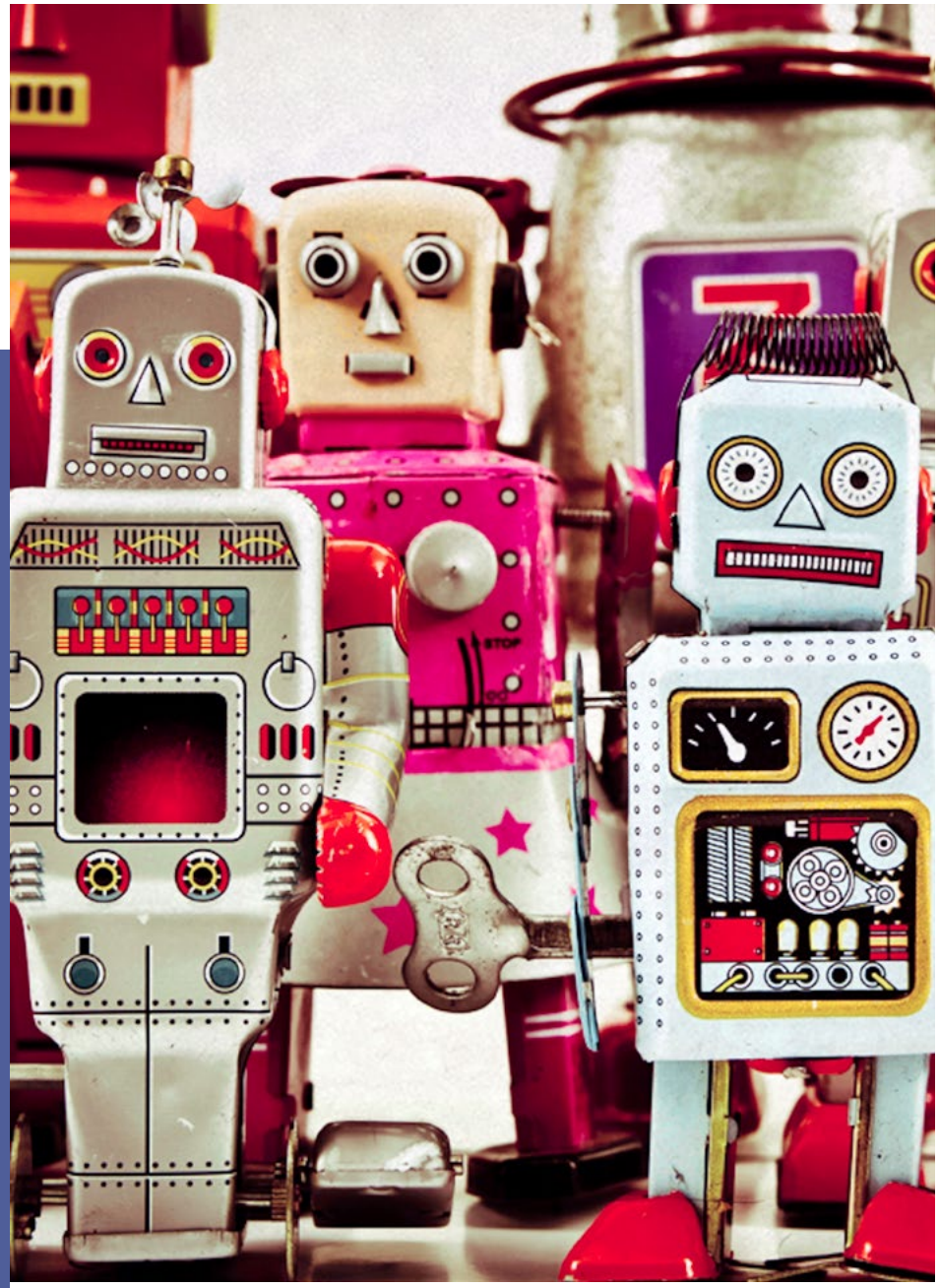
101 - 500

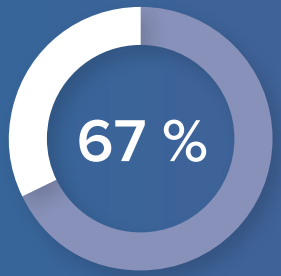


501 - 999

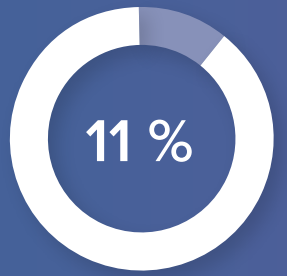


>1,000





10 or fewer



100 and more

How many Application Security professionals are in your organization?

Developers often outnumber AppSec professionals by 100:1.

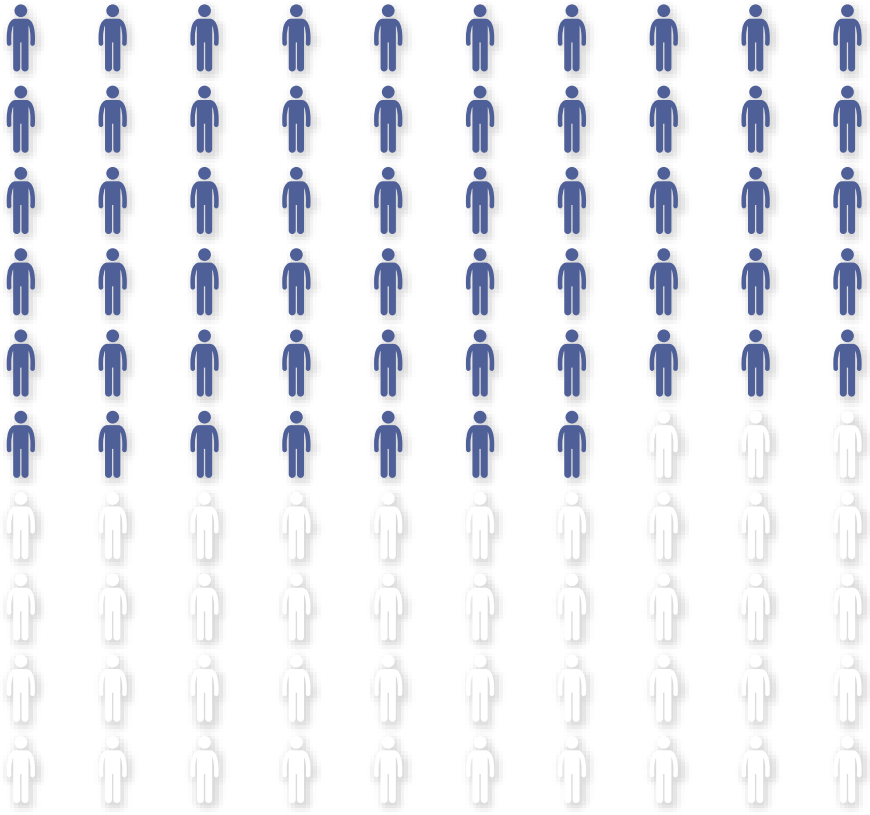
IN SEARCH OF AGILITY

58%

believe security is an inhibitor to DevOps agility.

Do you believe your information security policies/teams are slowing IT down?

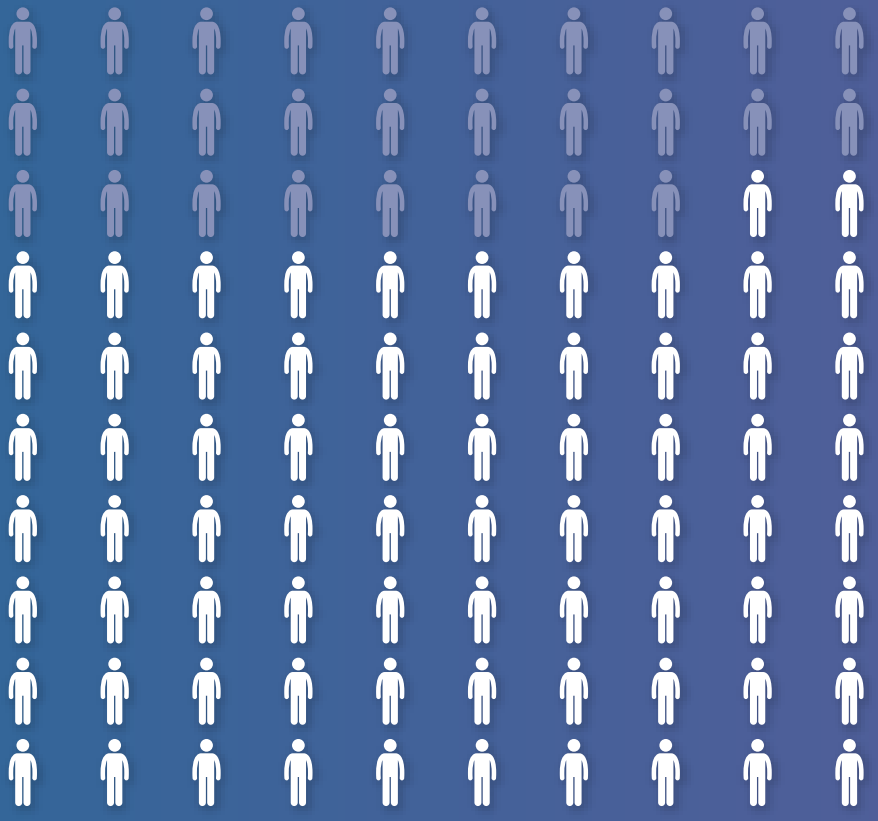
Mature DevOps practices have identified ways to integrate security at the speed of development.



47% YES

of Responses for Not Very Mature or No DevOps Practices.

n = 524



28% YES

of Highly Mature DevOps Practices

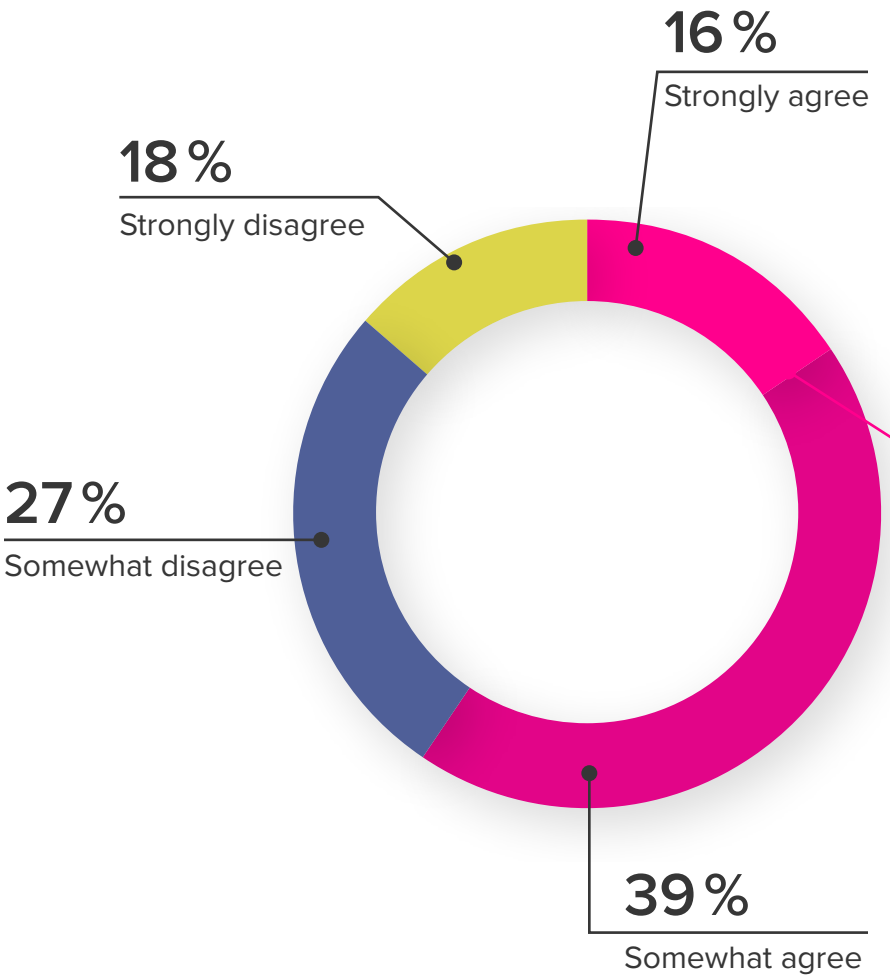
n = 459

50%

of developers know security is important but don't have enough time to spend on it.

n = 2,155

Our current approach to application security puts security pros in the role of nags who only point out vulnerabilities but who can't resolve them.

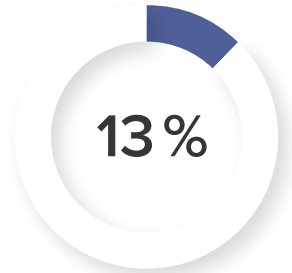


n = 1,775

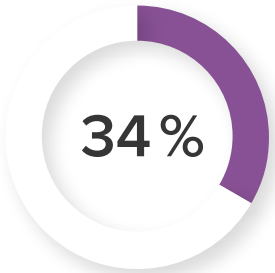
AUTOMATING SECURITY

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

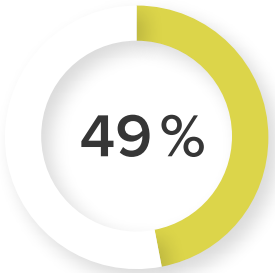
ALL RESPONSES
for automated security



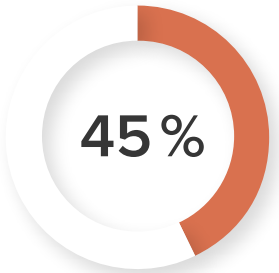
Design / Architecture



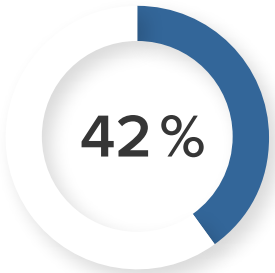
Development



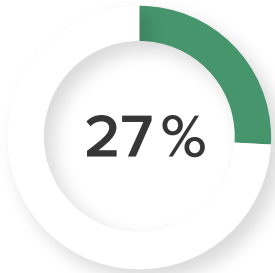
During QA/Test



Prior to release into production



In Production

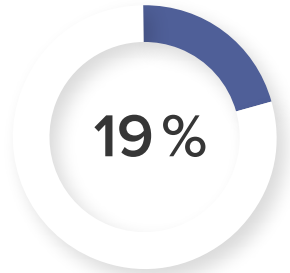


All of the above

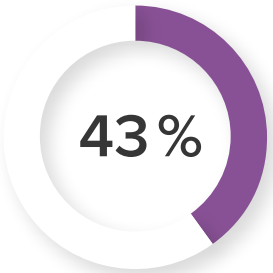
n = 1,791

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

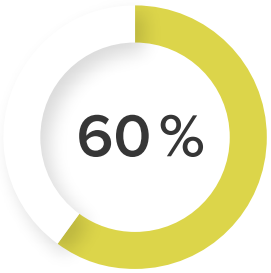
HIGHLY MATURE DEVOPS
for automated security



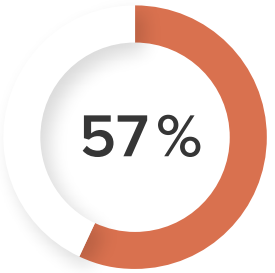
Design / Architecture



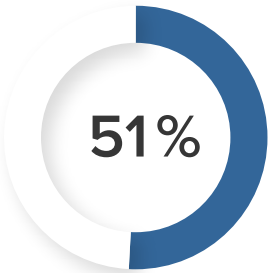
Development



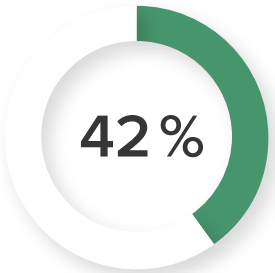
During QA/Test



Prior to release into production



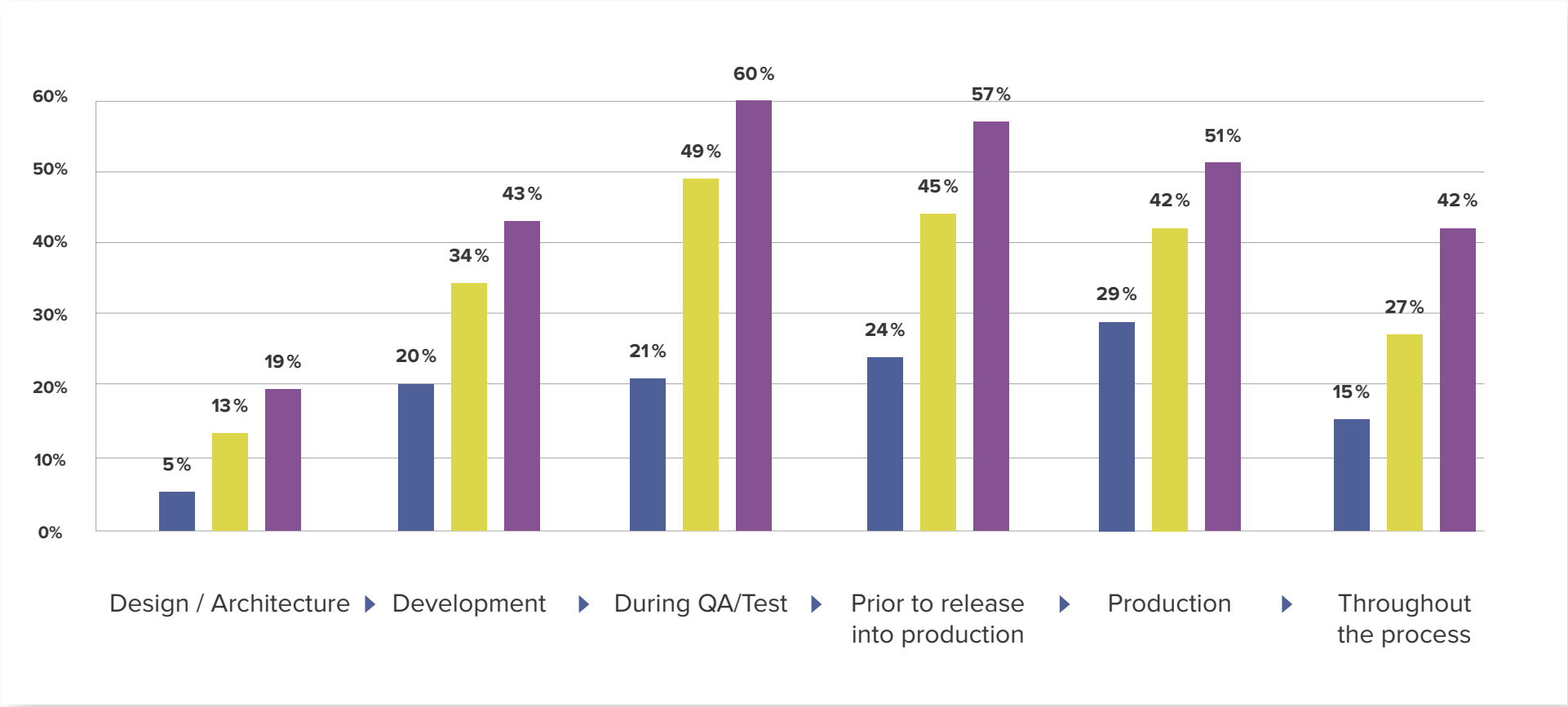
In Production



All of the above

n = 461

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



Does your organization perform automated application security testing within your CI/CD practices?

Highly mature DevOps practices are implementing more automated security.

only **39%**

of all participants have automated security testing **within CI/CD.**

n = 2,015

yet **58%**

have automated security testing **in highly mature DevOps practices.**

n = 461

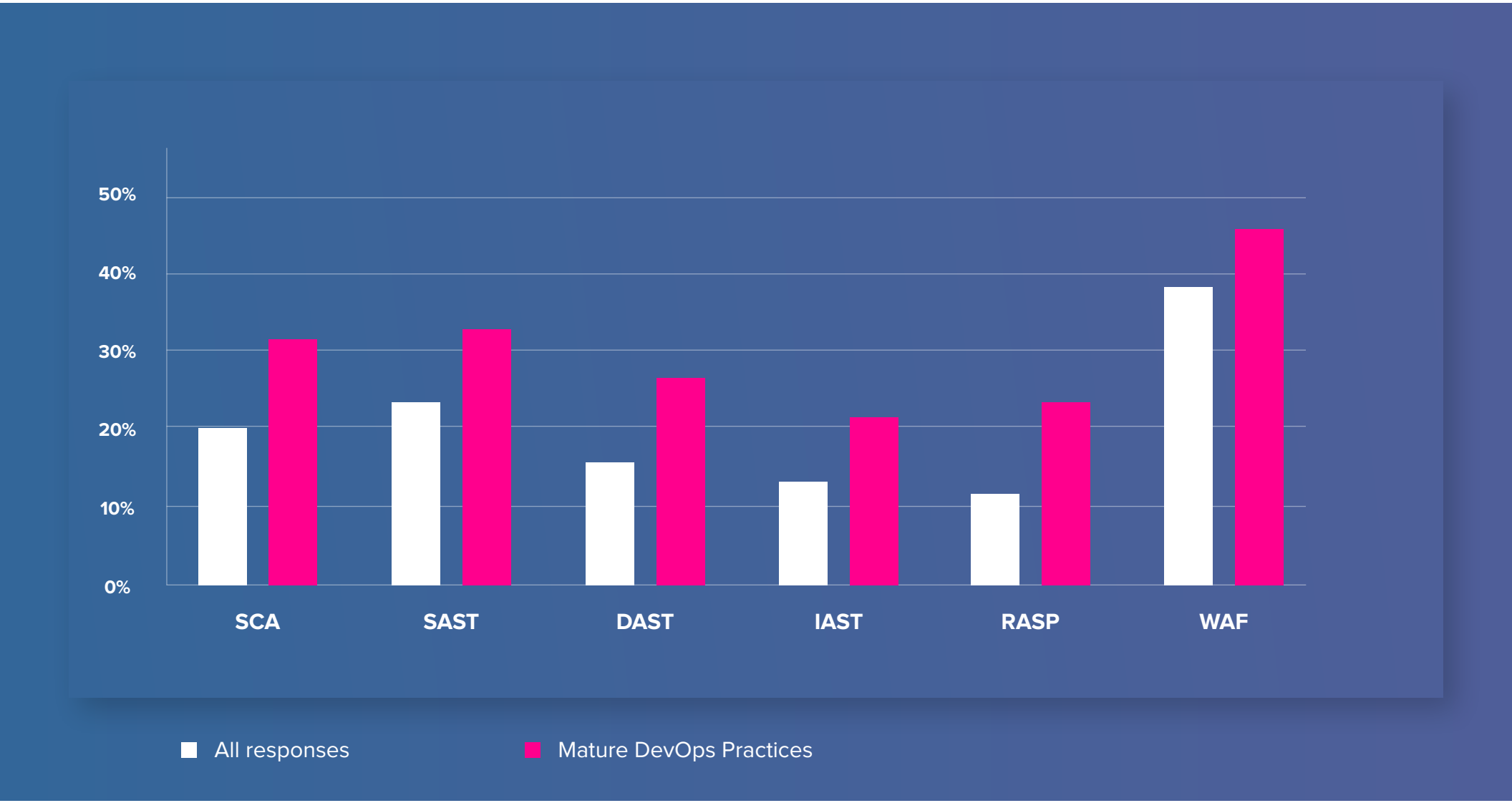
DJ SCHLEEN

DevSecOps Evangelist

“Business needs require software to be developed and shipped in a timely fashion. Developers want to code the software in the most optimal way possible. The Operations team wants the application to be highly available and stable. And the Security team wants it to have no vulnerabilities and low risk to the organization.

This isn’t a situation where having one team succeeding means another has to falter – rather it’s a perfect ecosystem for collaboration. Security is the responsibility of every individual in an organization and should never supersede the object being delivered. It should be an attribute.”

For your organization, please rate the following application security tools in use.



IMPLEMENTING CONTROLS

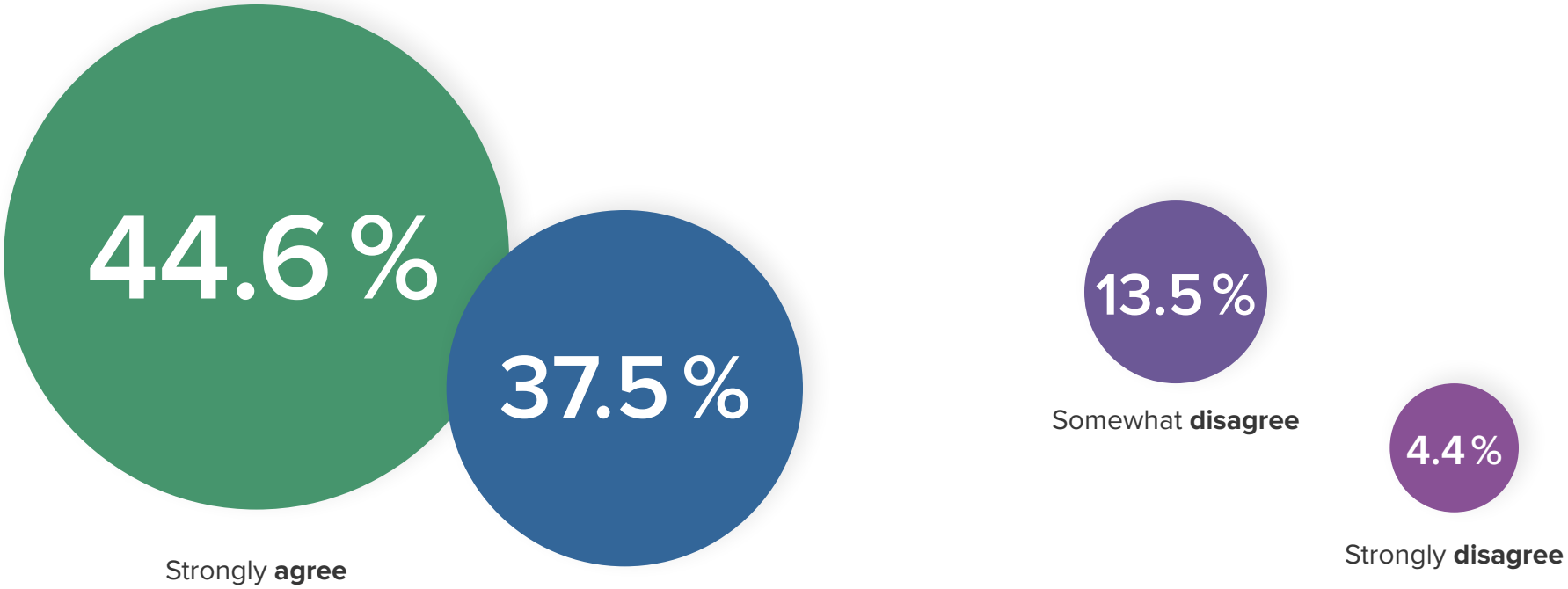
OLEG GRYB

Chief Security Architect

“For those of us who have been involved on the front lines of traditional AppSec activities such as penetration testing, dynamic or static code analysis, it may be obvious that the traditional tools and techniques we use were built more for waterfall-native rather than DevOps-native environments.

Yet for executives who came to security from infrastructure, networking or development domains and have never run a security scan, the challenges of bringing traditional tool sets and practices into the new velocity expectations of DevSecOps may not be so obvious.”

We've implemented good version control practices and tools to maintain clear accountability and traceability for all the applications deployed into production.

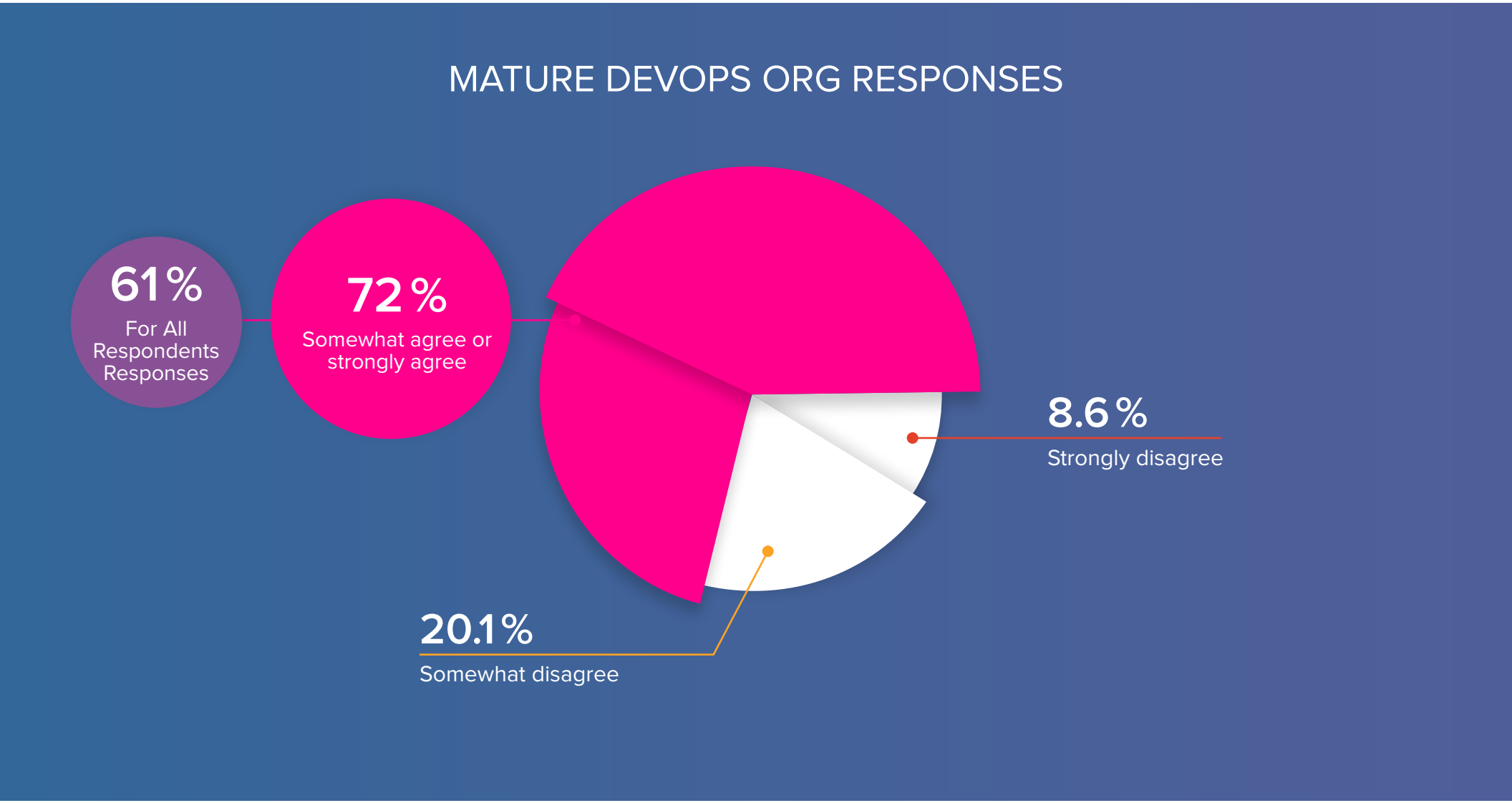


82%

have implemented good version control practices.

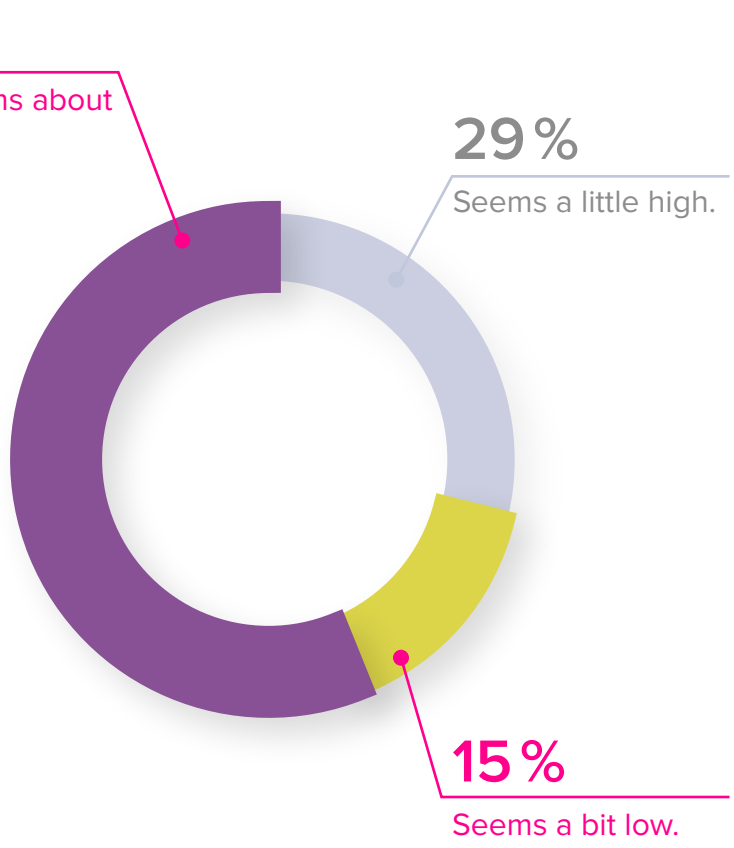
n = 1,786

We have adopted an immutable infrastructure mindset where production systems are locked down.

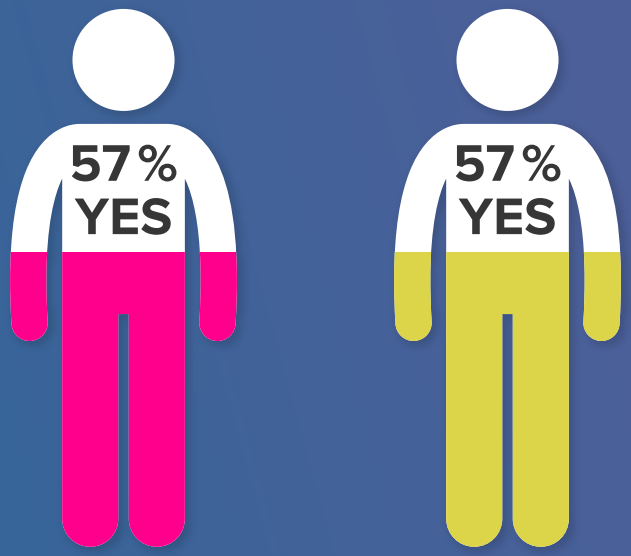


n = 460

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



Does your organization have an open source governance policy? (i.e., rules about using good, not bad, components)

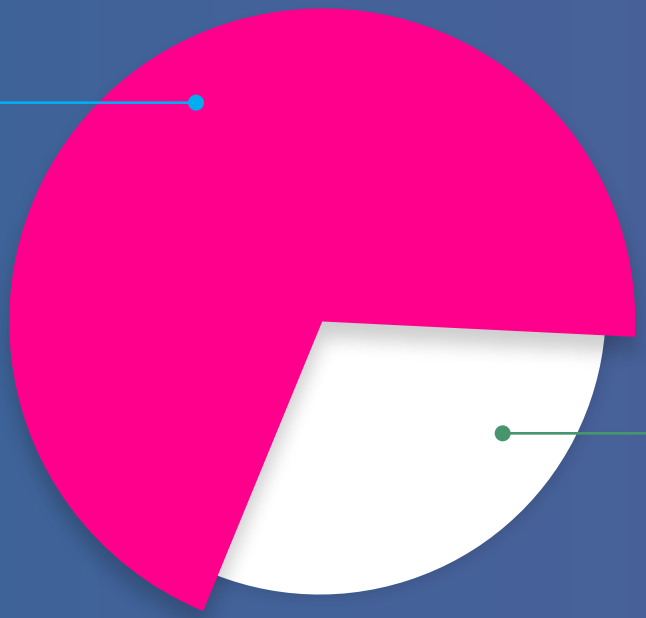


n = 2,520

How well does your organization control which open source and third-party components are used in development?

65 %

of organizations **do not have meaningful controls** over what components are in their applications.



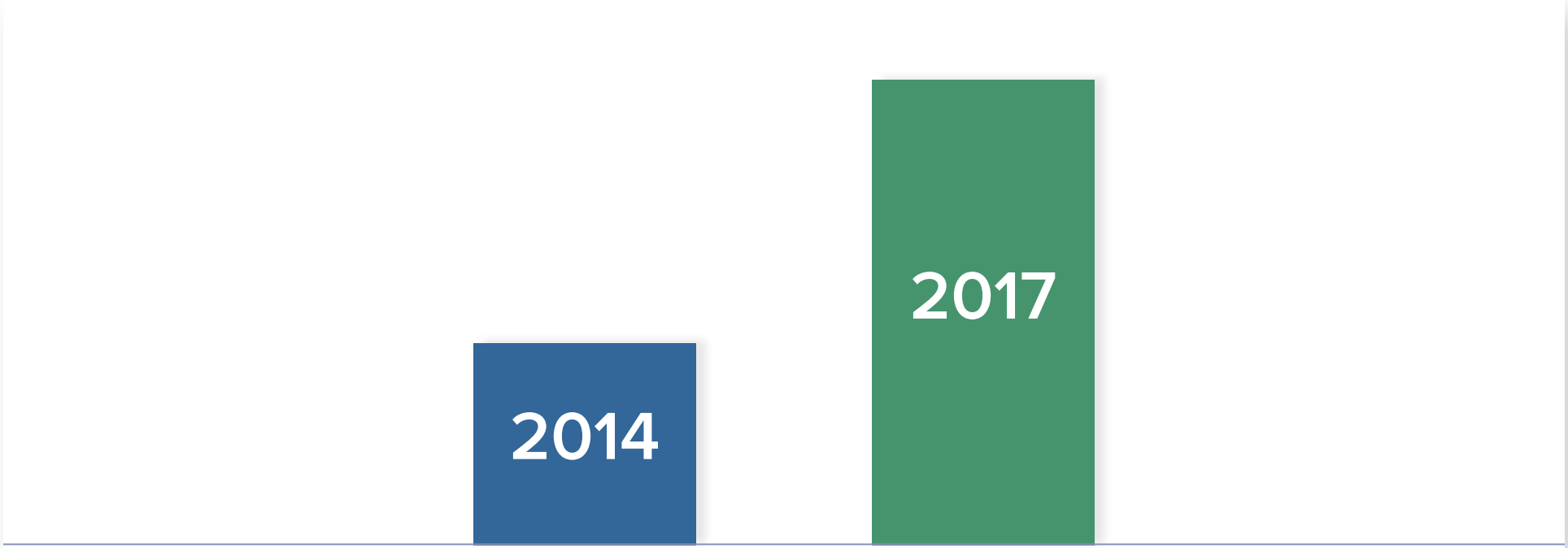
35 %

have a **complete software bill of materials** for each application.

n = 1,701

BREACHES HAPPEN

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?



14%

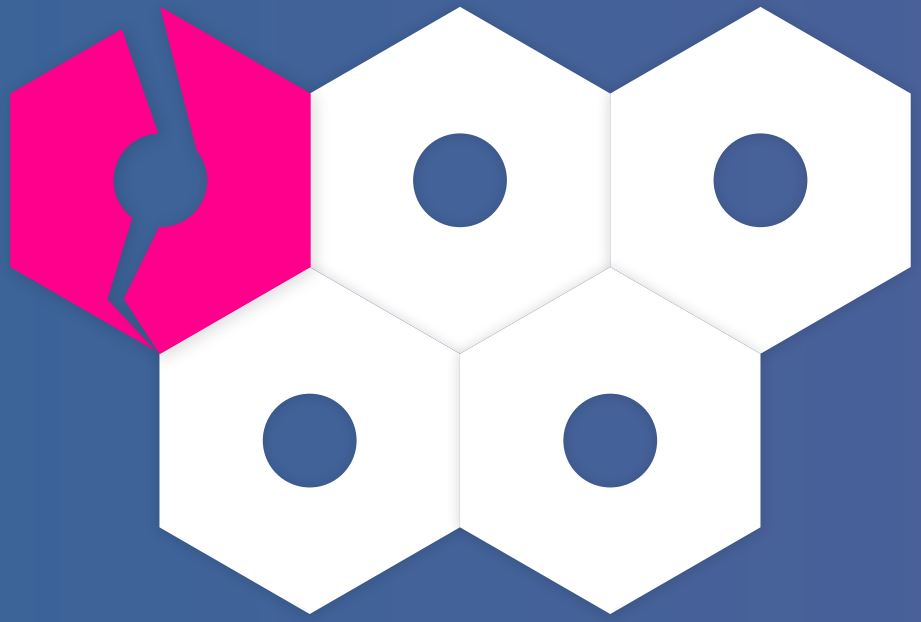
suspect or have verified a breach related to open source components in the **2014 survey.**

n = 2,727

20%

suspect or have verified a breach related to open source components **in the last 12 months.**

n = 1,827



1-in-5 had or suspected a
web application vulnerabilities
in the last 12 months.

n = 1,327

DEREK WEEKS
Sonatype

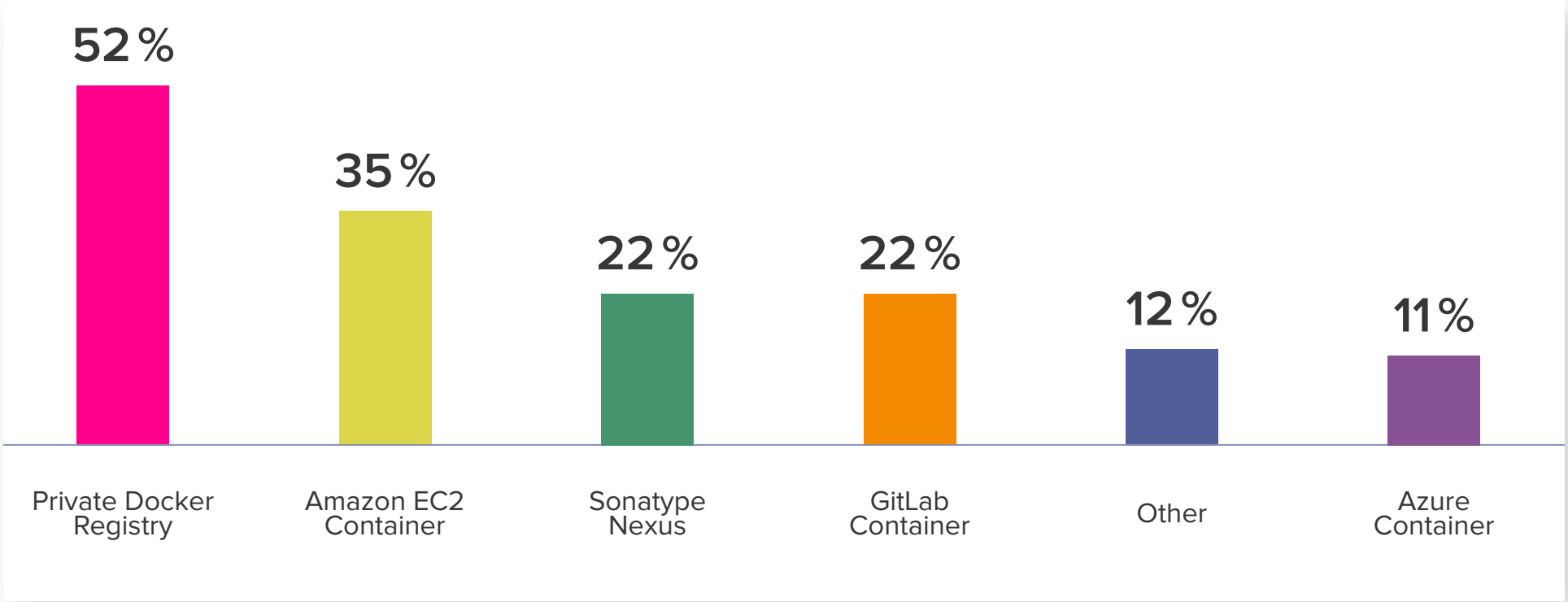
“Confirmed or suspected breaches related to vulnerable open source components increased nearly 50% from 2014 to 2017..

Yet, during the same period, the percentage of organizations governing the use of secure components remained the same.”

CONTAINER SECURITY

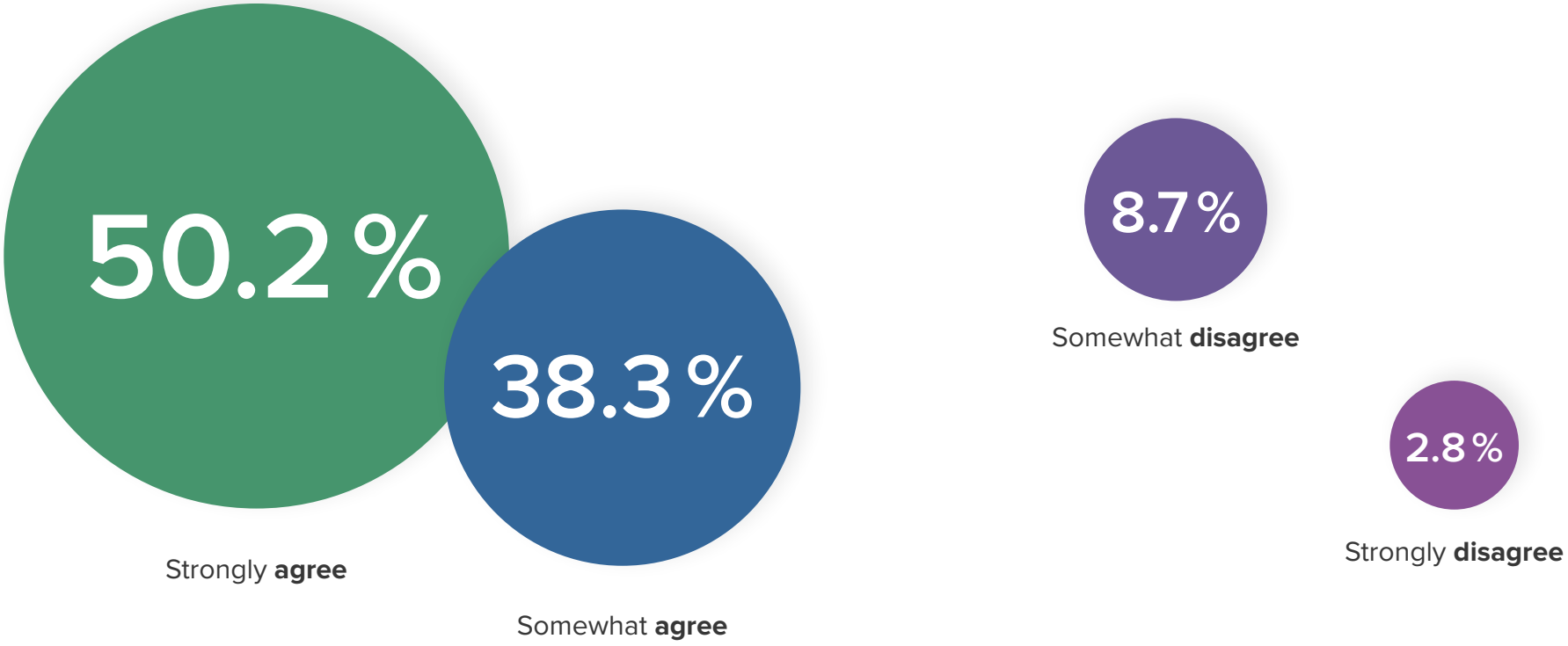
Which private container registries does your organization use?

While Docker private container registries are the most popular, **no dominant vendor has emerged**



n = 1,608

Security is a top concern for us when deploying containers.



88%

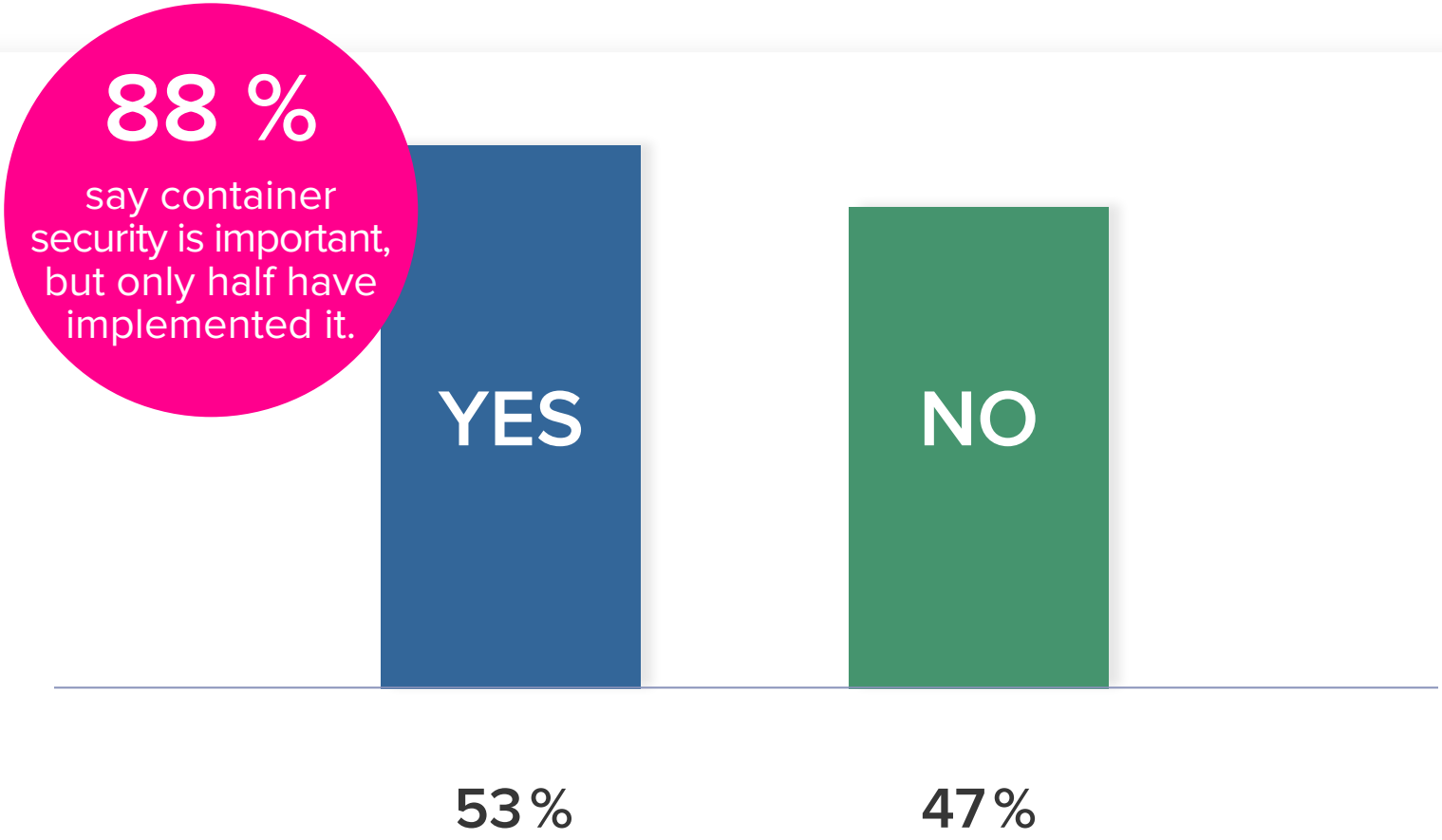
agree security is a concern when deploying containers.

n = 1,931

BENJAMIN WOOTTON
Contino

“On the positive side, containers also add additional process isolation features to limit how processes can behave when executing. The various platforms also enable other features for container provenance, traceability and signing. These can all contribute to form a much more secure software delivery pipeline than could be achieved using non containerized stacks.”

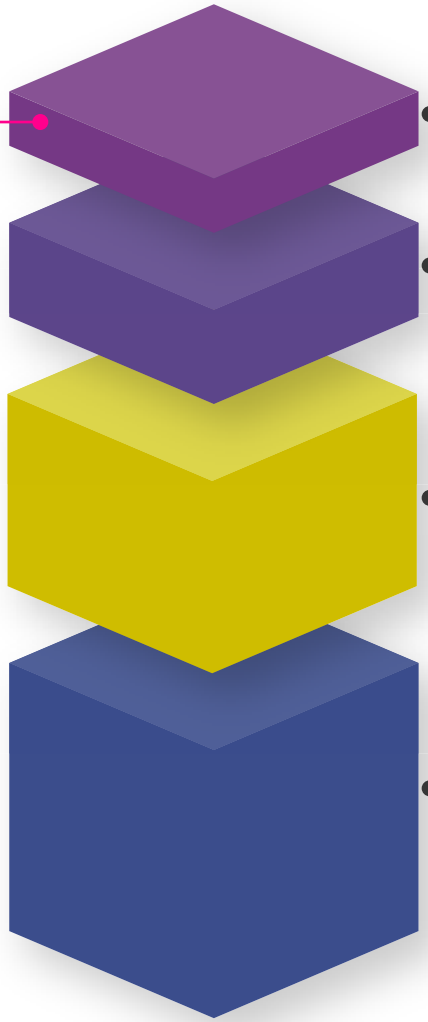
We leverage security products to identify vulnerable applications/OS/configurations in containers.



What application security training is available to you?

ANSWERS FROM
Highly mature DevOps organizations

30 %
of those with immature DevOps practices **received no training.**



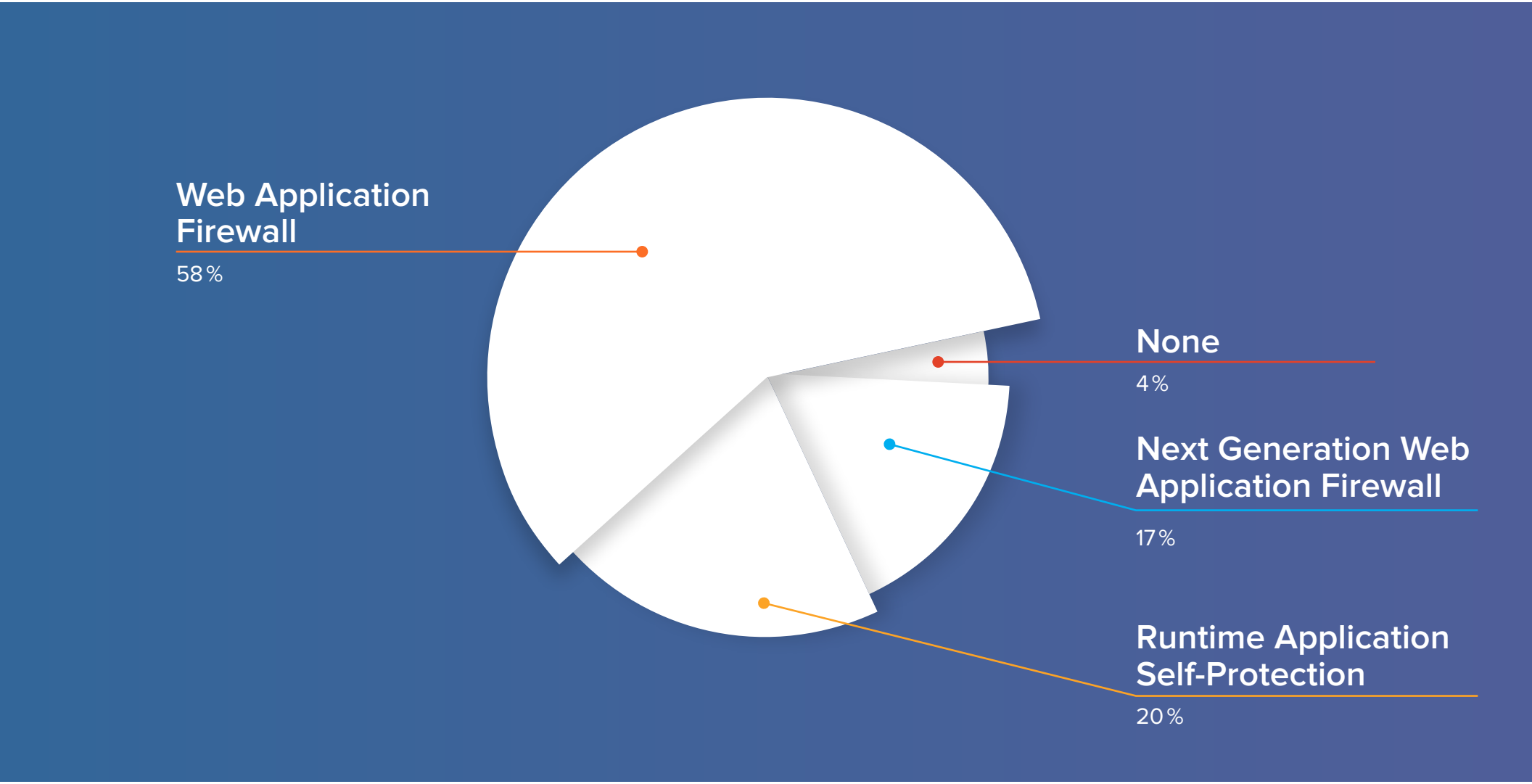
None
15 %

Instructor led
26 %

Secure coding/ programming
53 %

E-learning
74 %

What type of protection does your organization use for running applications?



DEVSECOPS COMMUNITY SURVEY 2017

ABOUT
The Survey

Just as the DevOps community has rapidly grown over the past several years, we have witnessed very strong interest in security practices that run within higher velocity, more collaborative, and highly integrated environments across this popular. Traditional waterfall-native security practices often don't fit in the DevOps native world and we wanted to use this survey to get a better sense of how organizations are adapting, what challenges they've overcome, and what approaches they are prioritizing.

The results reported here came in response to 37 questions asked by the Sonatype and our DevOps community partners, including Contino, DZone, Emerasoft, Ranger4, and Signal Sciences. The online survey was conducted between February 1, 2017 and February 28, 2017.

This is the fourth such survey conducted by Sonatype since 2011 focused on application development and security practices that have recently evolved into what we now call DevSecOps. The data collected in the DevSecOps Community Survey the provides statistically representative results on the adoption, practices, and challenges of managing DevOps practices with regard to security requirements.

For this project, 2,292 IT professionals responded to the survey with 1,759 (77%) completing it in its entirety. We have reported the tally of survey responses for each question within the report. In a few cases where we were seeking definitive knowledge by the participants, we chose to not include "I don't know" responses in the final results.

To establish historical trends, some of the questions in our 2014 and 2017 surveys were identical. Although we invited past participants to our 2017 survey, not all participants between the two surveys were the same.

For people who self-identified, we saw that 788 (45%) live in North America, 428 (24%) live in Europe, 158 (9%) live in China or India, and the remainder of the people participated from other regions of the world.

The survey's margin of error is ±2.02 percentage points for 2,292 IT professionals at the 95% confidence level.