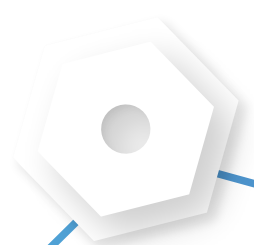




DEVSECOPS COMMUNITY SURVEY 2019





DEREK E. WEEKS

Vice President and DevOps Advocate, Sonatype

In the past few years, a growing number of enterprises have successfully adopted “build security in” practices within their maturing DevOps practices. Waterfall-native tools and security silos of expertise have given way to automated, integrated security approaches that focus on supporting developers in their native realm through better planning, tools, and training.

Our 6th annual DevSecOps community survey, represents the voice of 5,558 IT professionals and 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.

At the same time as DevSecOps practices are encouraging secure coding practices and improved cybersecurity hygiene, we continue to witness a growing volume of breaches that impact the trust of customers and reflect upon the advancements of our adversaries.

While some results of our survey may surprise you, we 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: CloudBees, Signal Sciences, Twistlock and Carnegie Mellon’s Software Engineering Institute for helping us build this year’s survey and promote its awareness.

WHO PARTICIPATED?



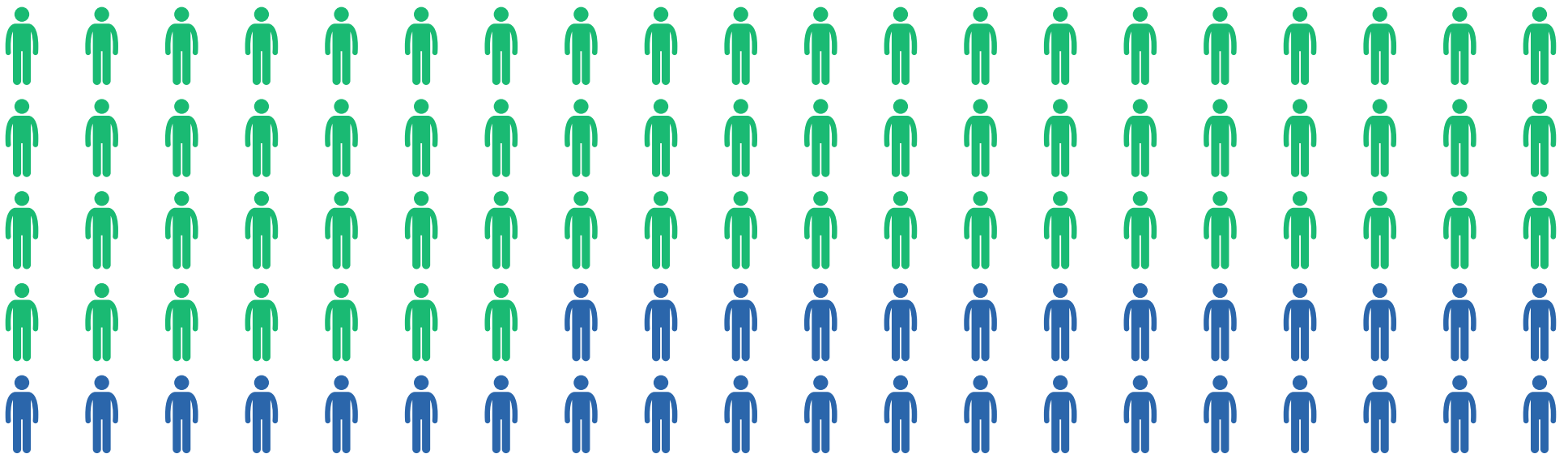
5,558

people shared their views with us
in the largest DevOps survey to date.



How many developers are in your organization?

67% HAVE MORE THAN 25 DEVELOPERS.



Which title best matches your role within the organization?

DevOps

22.74%

Developer

22.80%

Architect

14.70%

IT Manager

7.83%

QA / Test

2.09%

**Information/
Application
Security**

3.96%

IT Operations

4.03%

Team Lead

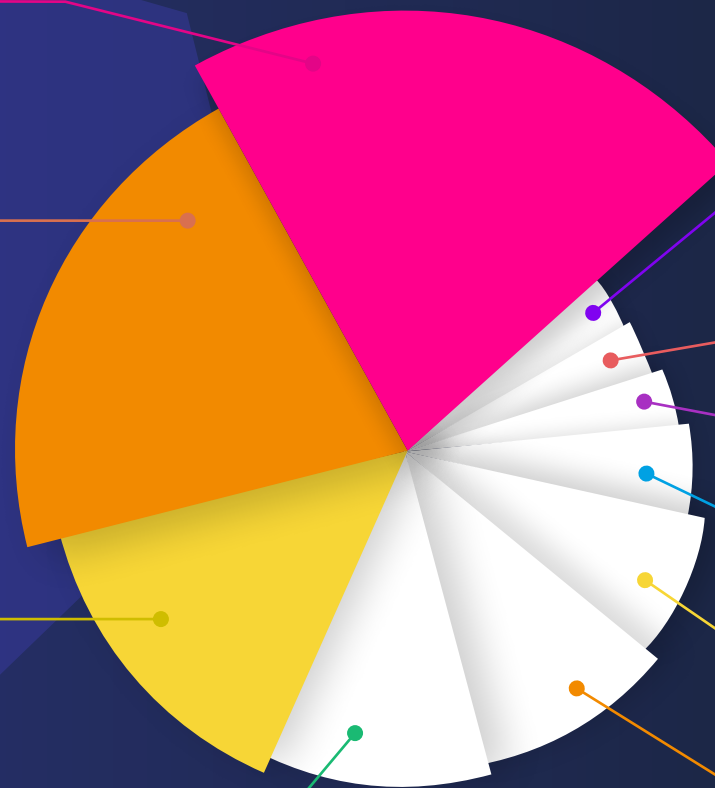
6.82%

Executive

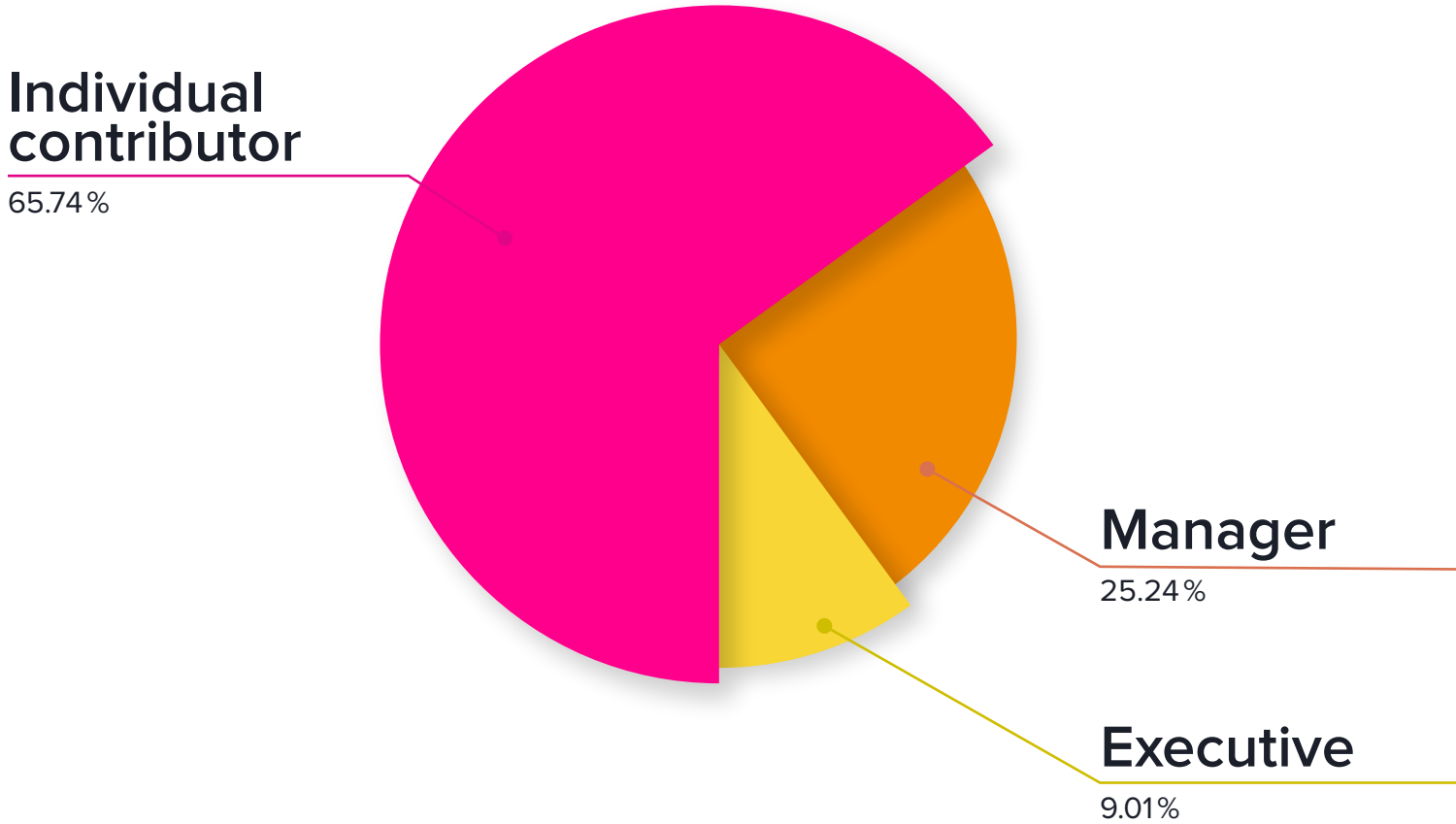
6.93%

Other

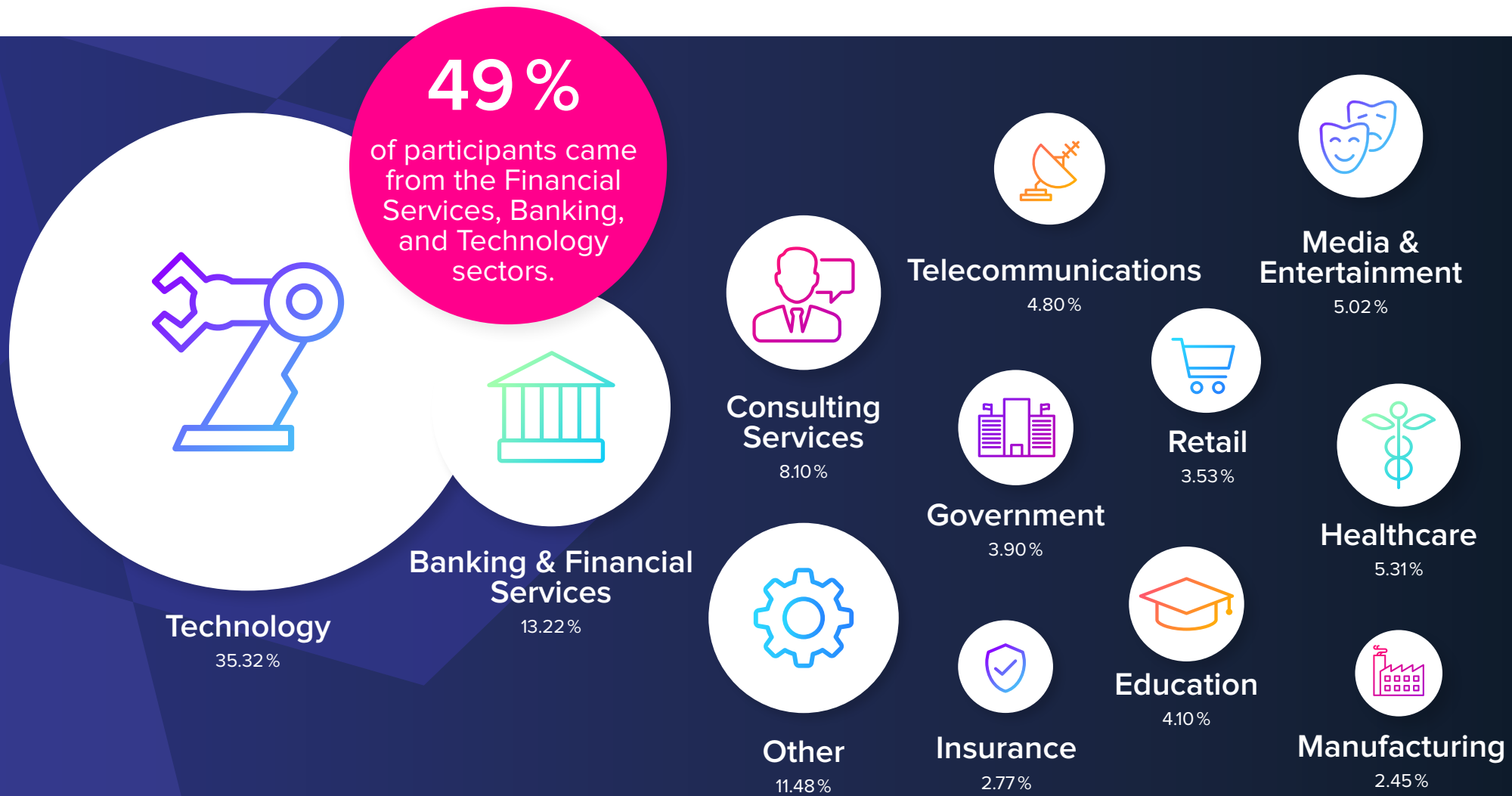
7.21%



What is your level of seniority within the organization?



In which industry is your company?



We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“

Security is super important to us, yet if we take a traditional security approach (old school enterprise) our speed of development is severely slowed down. We need to be secure and move fast.”

- Kayla Altepeter
Merrillcorp

DEVOPS MATURITY



CHARACTERIZING THE DEVSECOPS ELITE

One of the key questions we ask each year is about an organization's DevOps maturity level. The survey asked participants to self-identify their DevOps maturity level from a variety of choices. We once again compared results of those in mature DevOps practices with those that had immature to no DevOps practices in place. In many cases, survey responses were dramatic and telling.

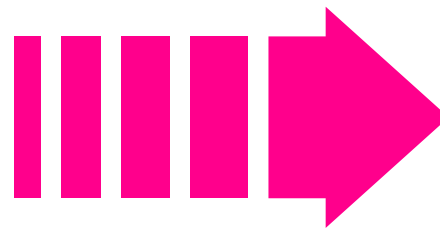
The responses to our 2019 survey revealed where DevOps teams have integrated and automated security, where practices have “shifted left”, and where collaboration efforts between Dev, Ops, and Sec teams are paying dividends. We also explored what industries are making the most progress in transitioning from agile and waterfall development methods to DevOps practices.

One thing is abundantly clear, DevSecOps investments are paying off in terms of cultural change management, automated tooling, training, and cybersecurity hygiene. Advances made by the most mature organizations since last year's survey helped us better characterize traits of the DevSecOps Elite.

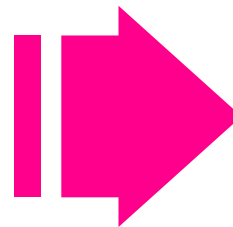
How mature is your adoption of DevOps practices?



27%
have **mature**
DevOps practices

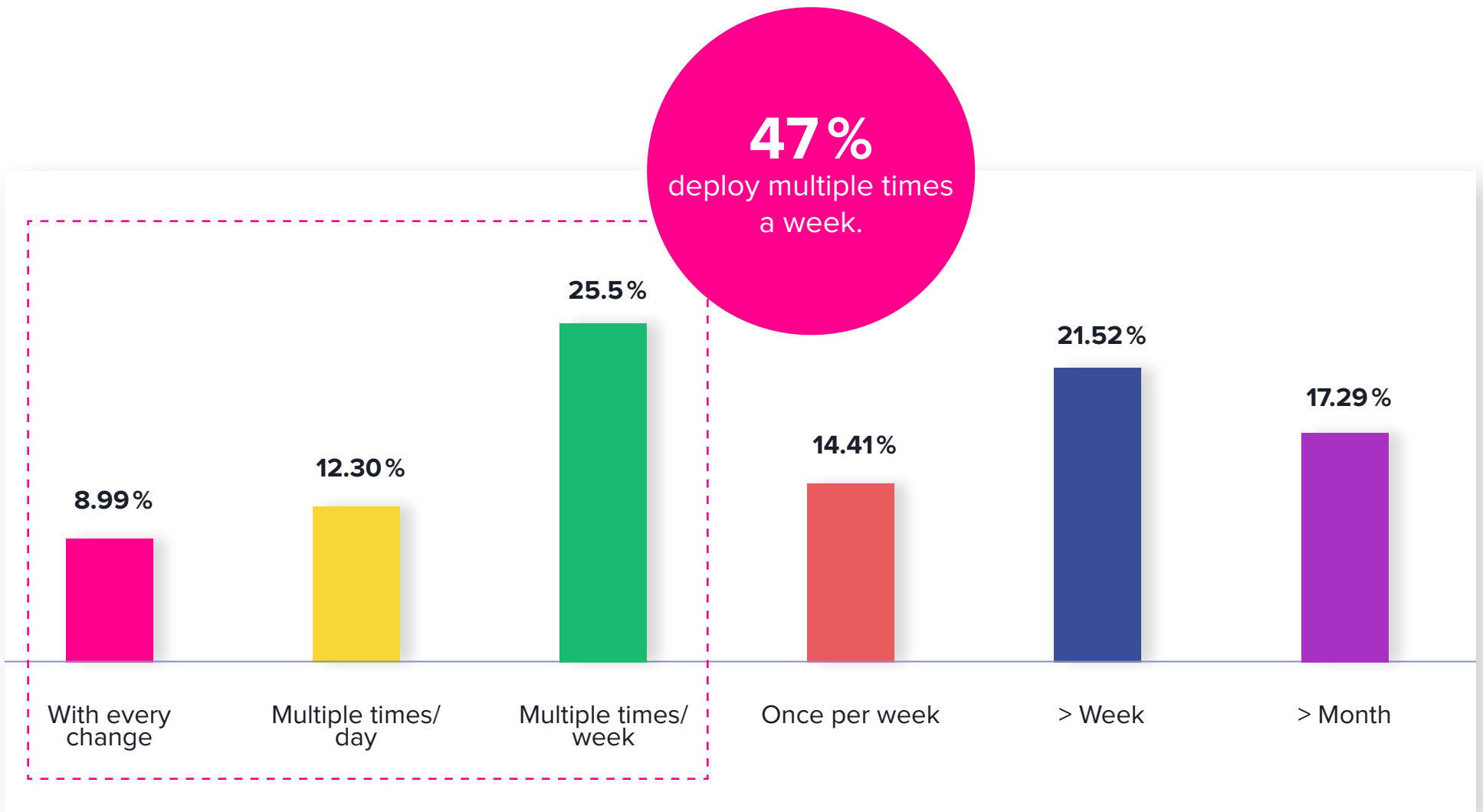


48%
are **improving**
their maturity.



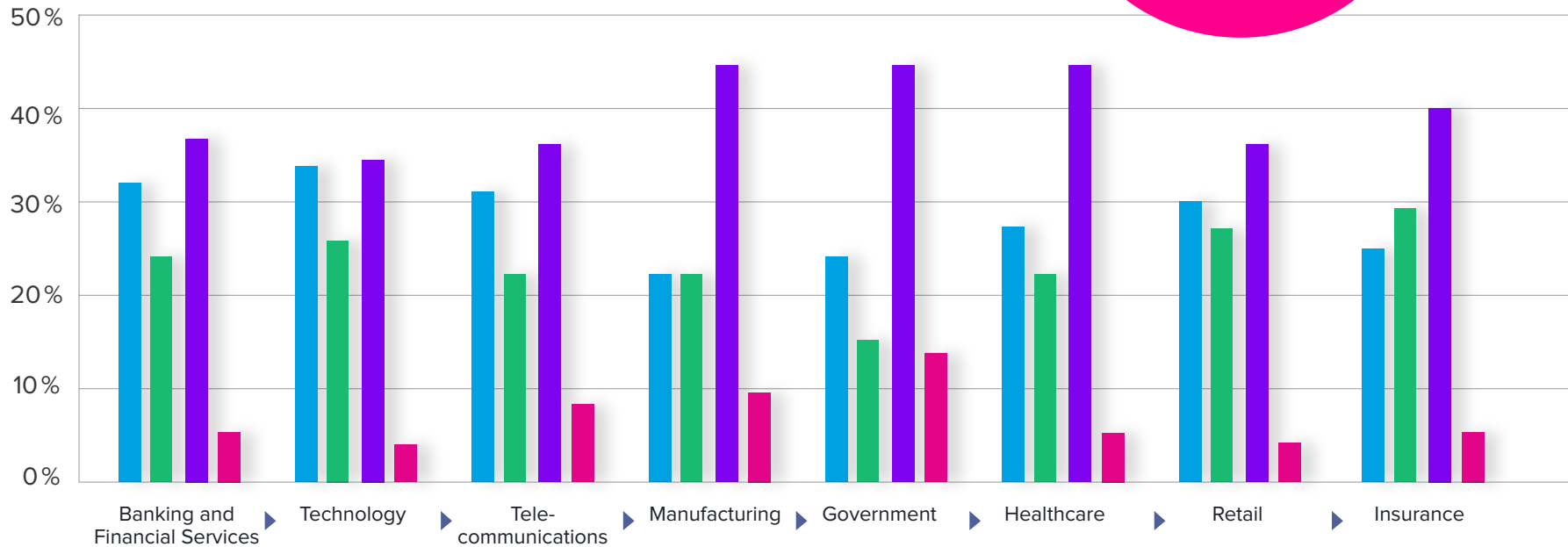
25%
immature
practices

How frequently do you deploy to production?



What type of development/deployment practices are used in your company?

DevOps shows strength in Banking, Communications and Retail.



■ DevOps ■ CI/CD ■ Agile ■ Waterfall

We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“DevSecOps practices helps us stay competitive and helps us develop and deploy securely from day one. This proactive approach helps mitigate security issues and keeps things in order—instead of firefighting.”

- Sreenivas V
A&E Corporation

MOTIVATIONS AND INTEREST



PRIORITIZING DEVSECOPS

Developers know security is important, but don't have enough time to spend on it. Interestingly, this same theme has repeated itself year over year in our survey. Half of the respondents each year admitted to not having enough time to spend on security, while at the same time, security practices are developing among the DevOps Elite.

We see that when security shifts left and becomes integrated with development tooling; adoption and adherence to security practices improves. While DevOps professionals and developers have no more time to spend on security, across the DevOps Elite, cybersecurity hygiene was significantly elevated

Investments of the DevOps Elite were apparent, not only from their tooling and processes, but in the training opportunities they made available.

One of the more telling set of responses in this year's survey was where motivations were centered on implementing security across the SDLC. In some cases, organizations were motivated by customer trust and requirements, where others viewed security as a quality differentiator, and still others saw it as simply security for security's sake.

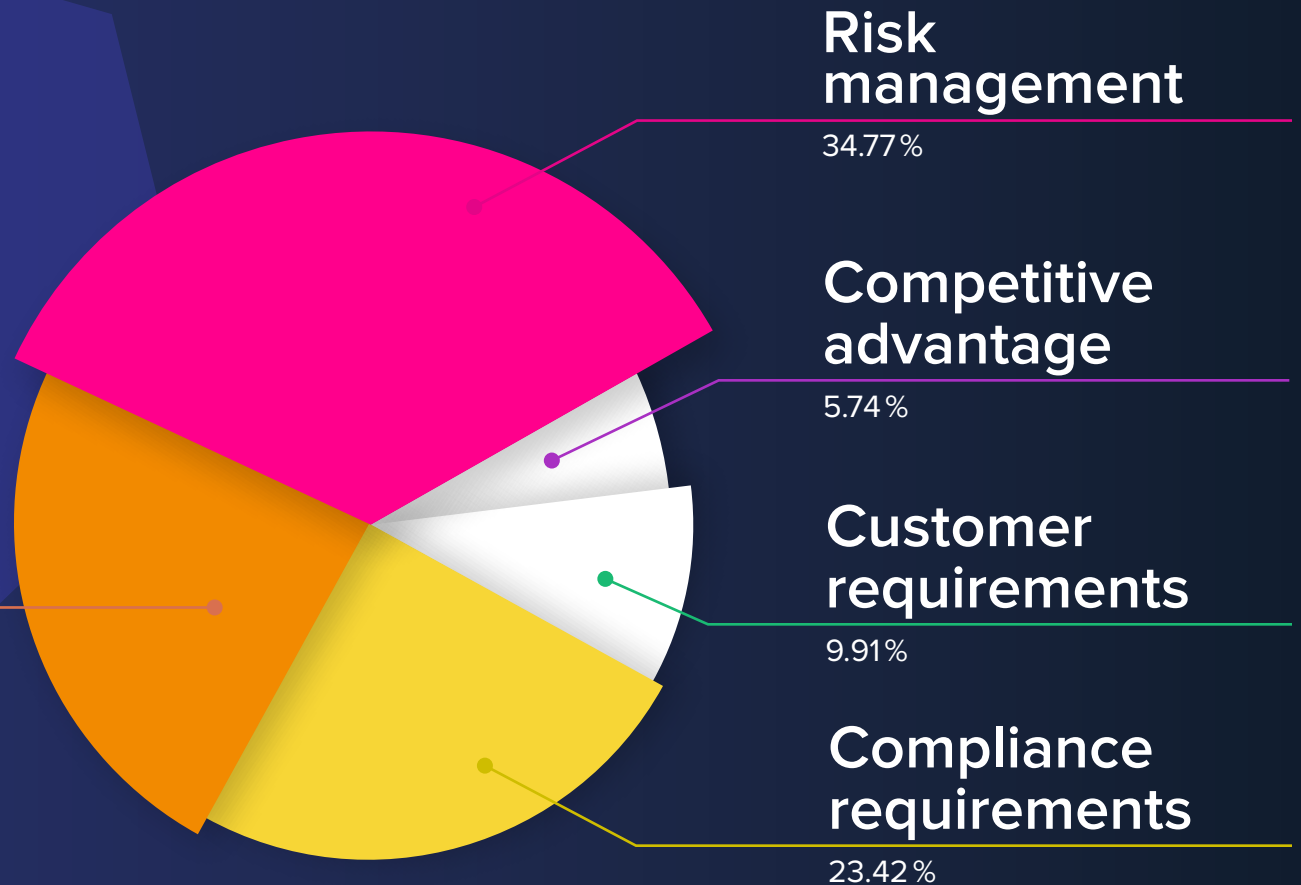
What is your main motivation to implement security across the development lifecycle?

1 in 4

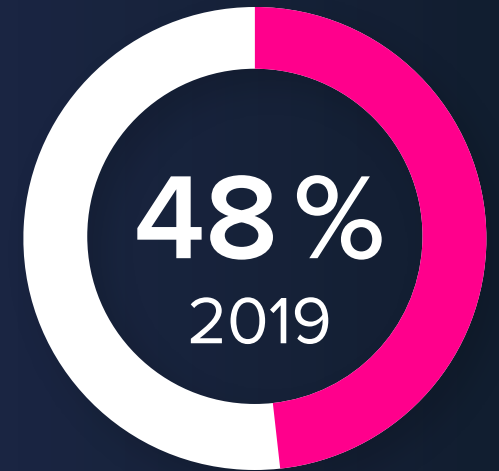
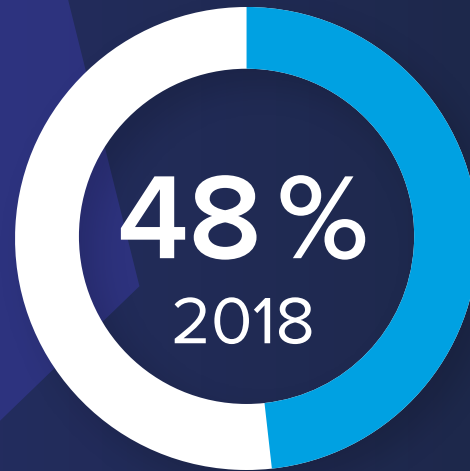
believe “security” is synonymous with delivering “quality”.

Improve quality of the code / application

24.75%



Developers continue to believe security is important
but **don't have enough time to spend on it.**



E-learning dominates security education for developers. What application security training is available to you?

ANSWERS FROM Mature DevOps organizations

29%
within Agile and
Waterfall practices
received no security
training.



None

11%

Instructor led

11%

**Secure coding/
programming**

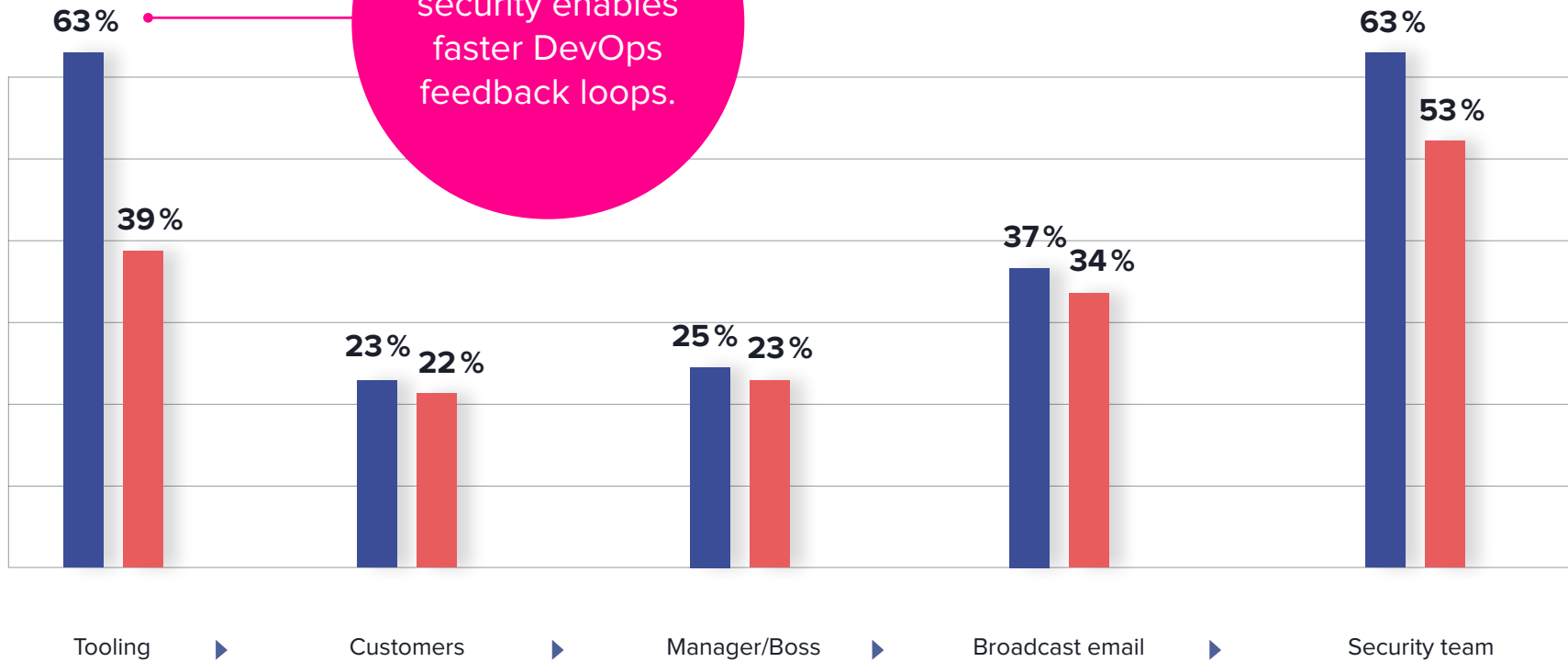
19%

E-learning

59%

How are you informed of InfoSec and AppSec issues?

Automating security enables faster DevOps feedback loops.



■ 2019 DevOps Elite Practices

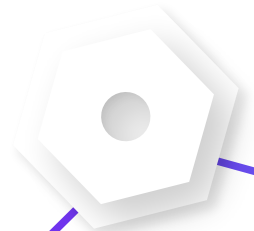
■ 2019 No DevOps Practice

We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“Not recognizing the importance of security in a DevOps strategy is a recipe for disaster. No matter how fast the velocity of a DevOps organization, if what they produce is not supportive of confidentiality, integrity & availability then they have failed. Including security in everything that is done is part of enabling the business to meet its strategic goals. DevOps needs security.”

- Lu Cortez
Canva

SDLC AND TOOLS



THE WHERE AND THE WHAT OF DEVSECOPS

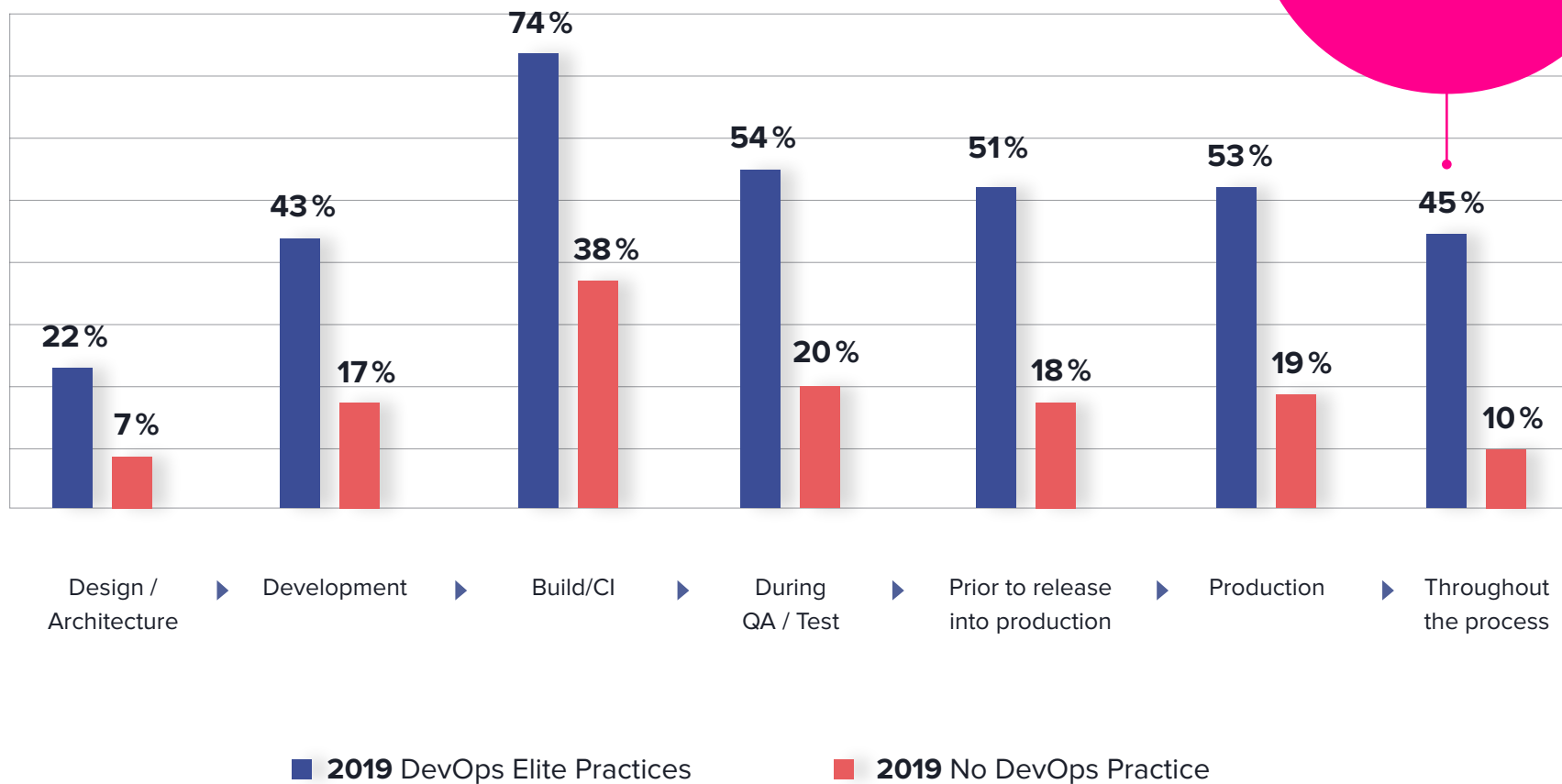
It's not just where you do something, but how you do it. Each year in our survey we have asked where automated security is being introduced into the SDLC to better understand how much practices are shifting left for the DevSecOps Elite. But while security introduced early in the development lifecycle reduces dreaded rework and accelerates DevOps feedback loops, it is clear that more organizations have placed value in distributing security throughout the SDLC.

As with all DevOps practices, security tooling choices are plentiful. This year's survey revealed the top five tooling investments being employed by the DevSecOps elite and compared those choices to their less mature counterparts.

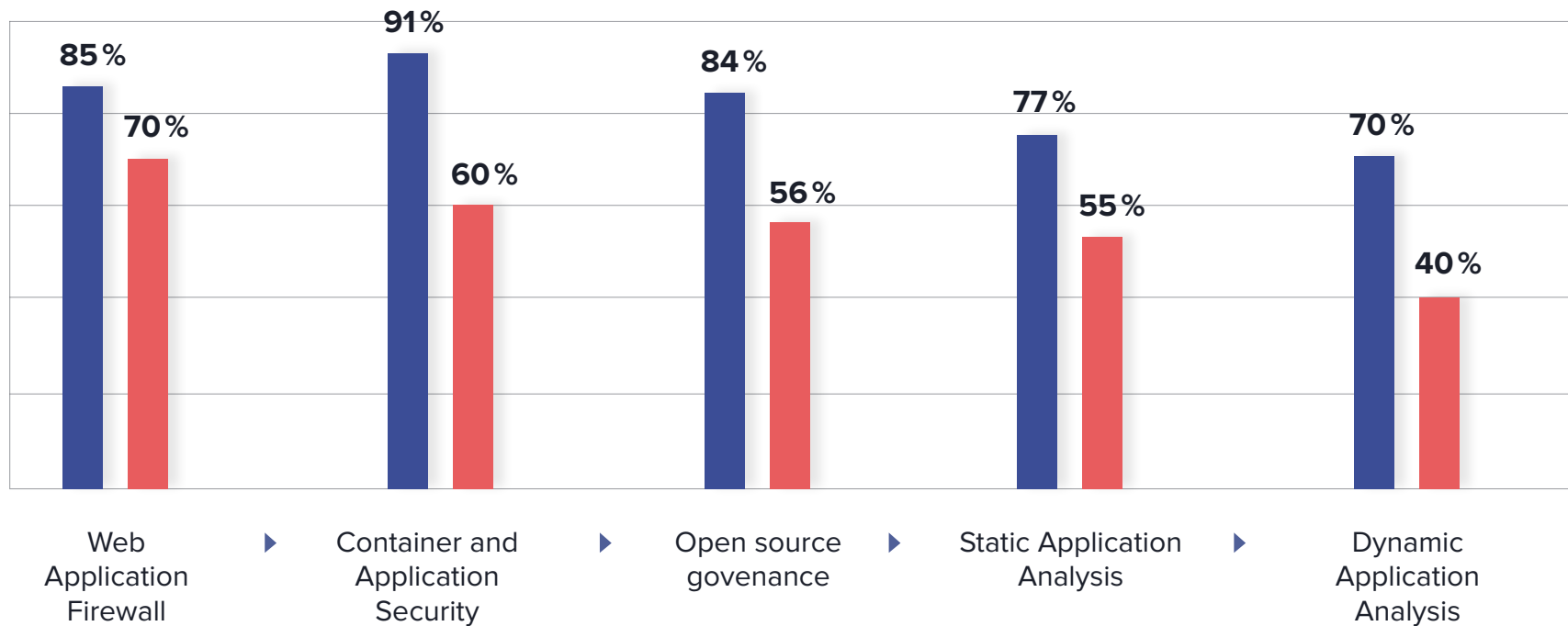
Automated doesn't mean the same thing to everyone. Therefore, this year's survey explored how automated practices are understood and defined. While the nirvana of fully automated and integrated security is pursued by many, only 1 in 4 organizations in the DevSecOps Elite attained that maturity attribute. It was also clear that those with no DevOps practices were still dealing with security, operating as a silo with practices bolted on later in the development lifecycle.

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

Mature DevOps practices are 350% more likely to integrate automated security.



Which application security tools are used?

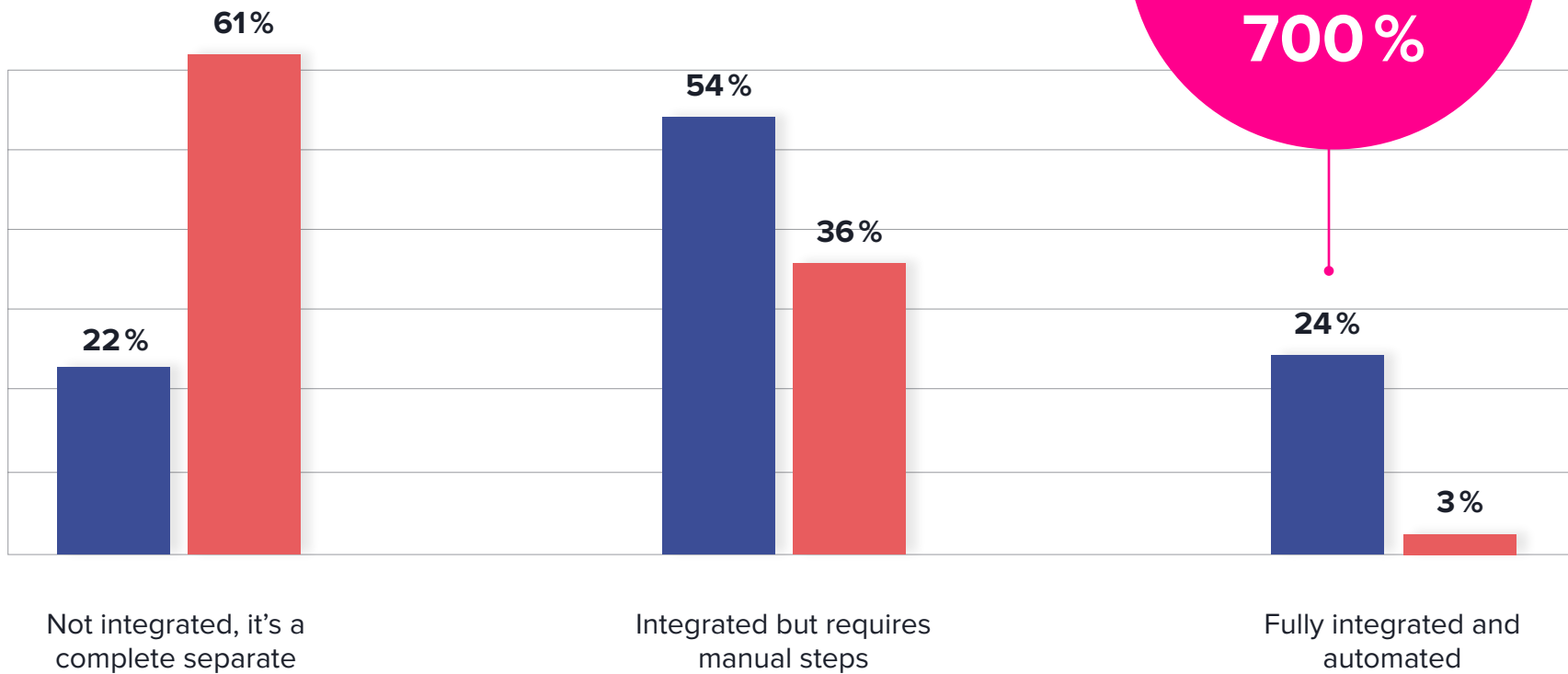


■ 2019 DevOps Elite Practices

■ 2019 No DevOps Practice

In general, which description best fits the integration of your security tools within your DevOps pipeline?

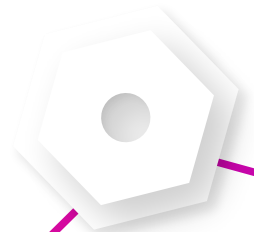
Elite DevOps practices favor automation over manual processes by **700%**



■ 2019 DevOps Elite Practices

■ 2019 No DevOps Practice

CONTAINERS AND CLOUD



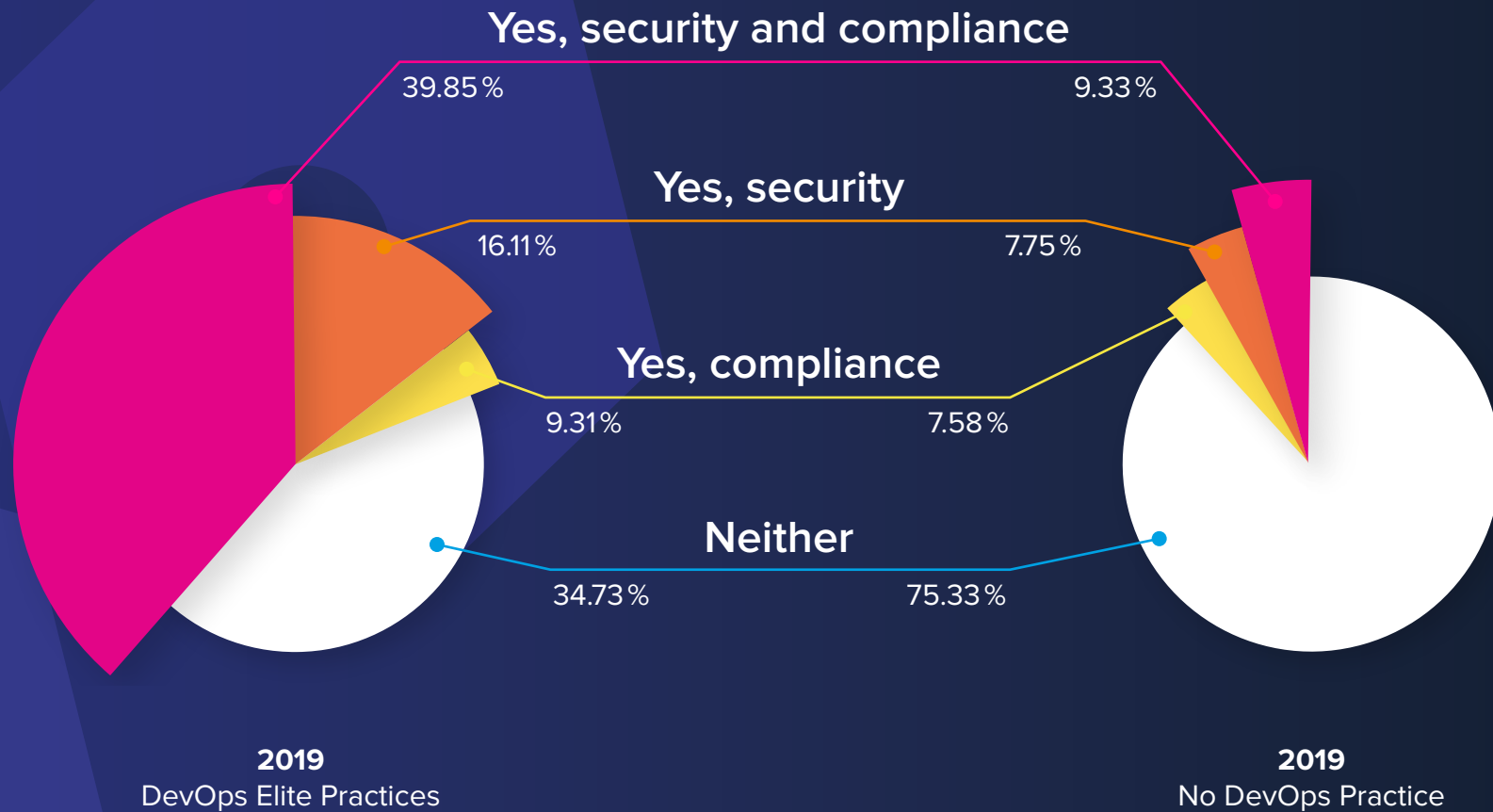


WHERE THERE IS DEVOPS, THERE ARE CLOUDS AND CONTAINERS

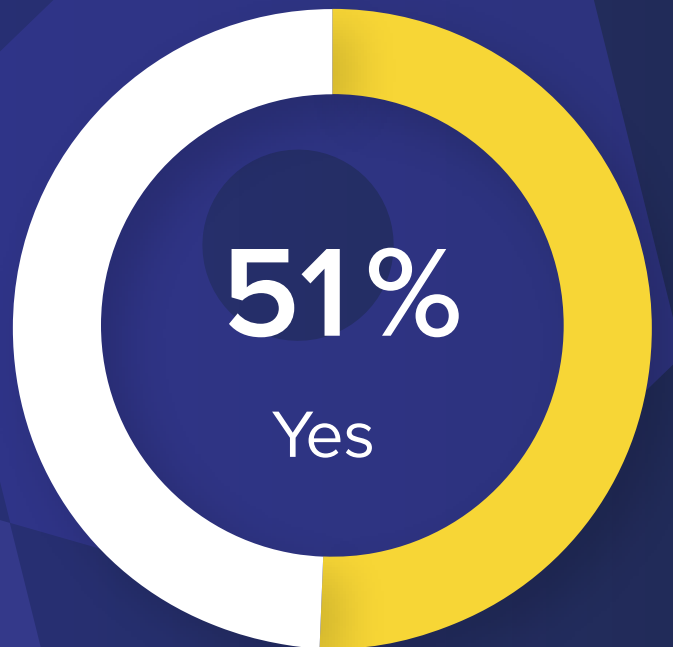
For those pursuing higher levels of DevOps maturity, container and cloud technologies come with the territory. The efficiencies gained through these technologies have accelerated the integration of Dev and Ops practices. As multiple studies have revealed over the years, containers and clouds come with their own security requirements and exposures. Therefore, we were not surprised to see large investments in security tools within this realm.

One of the more telling questions that was new to the survey this year focused on security in the cloud - asking where the burden of security lay as operations and development transitioned from on-premises to the cloud. As practices mature in this area, it will be interesting to continue watching what the trend is for the security burden: shifted, shared, or owned.

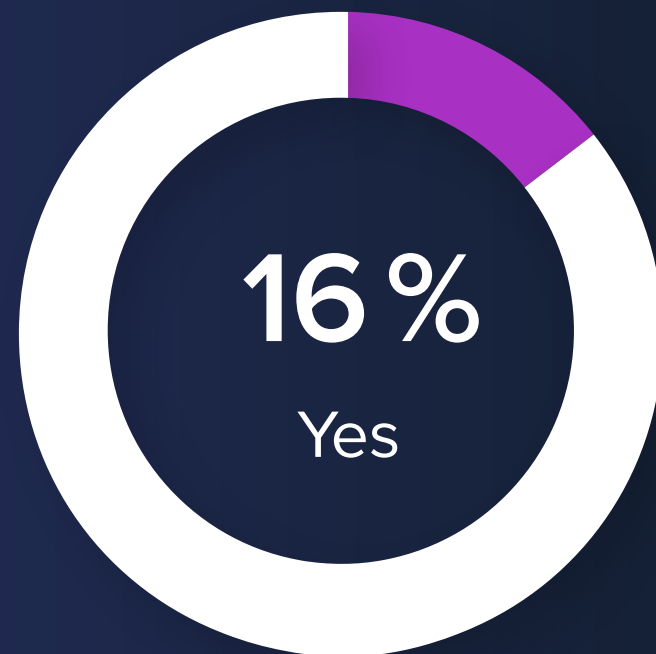
Do you have automated security and compliance checks in place for your cluster organization tool?



Do you have a Docker / Container specific security solution in place?



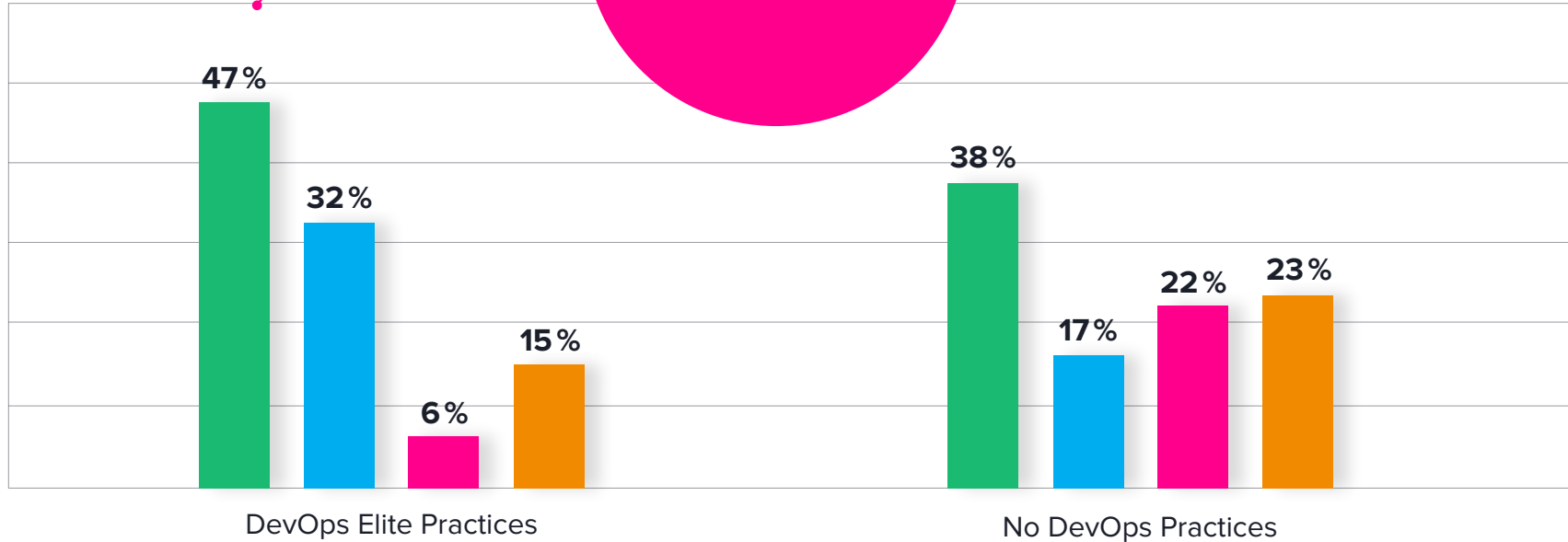
2019
DevOps Elite Practices



2019
No DevOps Practice

What cloud security protection do you utilize?

When infrastructure heads to the cloud, security for it follows.



■ Rely on cloud vendor

■ Utilize 3rd party tools

■ Don't use cloud technologies

■ Not sure

We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“Many people believe they can build software and that passing a hacking audit is all that’s needed to guarantee security. The reality is that audits only detect a small portion of problems within in a static snapshot of the application—which inevitably changes. The only way to really ensure security is to put automated controls in the pipelines so that every time a developer builds a new piece of code, it is checked (not only the code, but also its dependencies, dockerfiles, secrets, etc.)”

- Juanjo Torres
BBVA

CONTROLLING OPEN SOURCE



AUTOMATING OPEN SOURCE SECURITY

The race toward greater velocity in DevOps has also lifted the open source software tide. Today, over 85% of a modern application is built from open source components as developers choose to download in a second what might take days or weeks to write from scratch.

While software developers have exponentially grown their reliance on open source software components, we've learned that not all components are created equal. From OpenSSL's Heartbleed, to Poodle, to Bash, to Struts2, open source related breaches are on the rise.

When it comes to DevSecOps practices, we saw more organizations investing in controls that start with keeping an inventory of all components used. This was also where survey respondents revealed that automation of security practices tied to open source governance were hard to ignore.

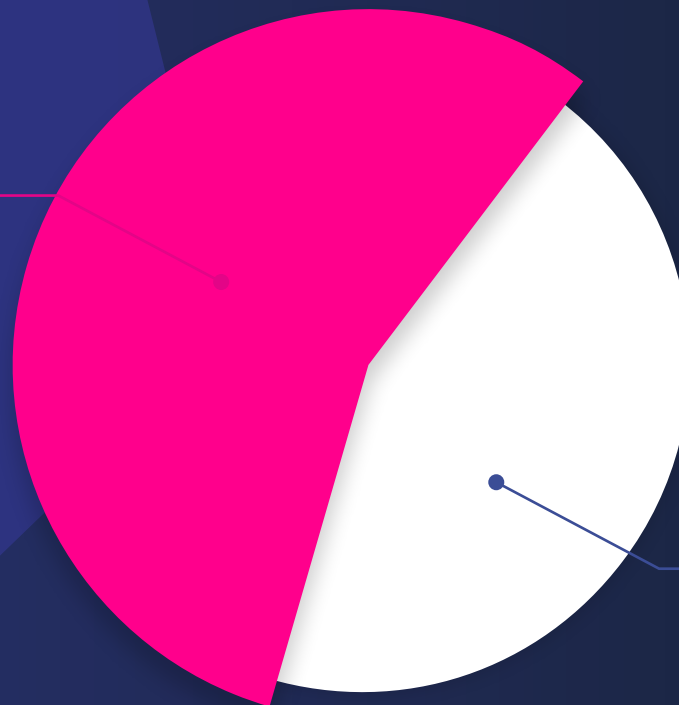
Automating security is paying off for the DevOps Elite, but that may not be directly apparent from the numbers. When comparing open source related breaches within the DevSecOps Elite group to those with immature DevOps practices, the more mature practices noted a higher percentage of breaches. With less visibility and fewer controls surrounding open source in less mature organizations, we suspected the lower breaches in the immature group were more an indication of lack of breach awareness.

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

53%

of mature DevOps practices keep a complete software bill of materials.

Compare that to those with no DevOps practice where only 21% keep a complete software bill of materials.

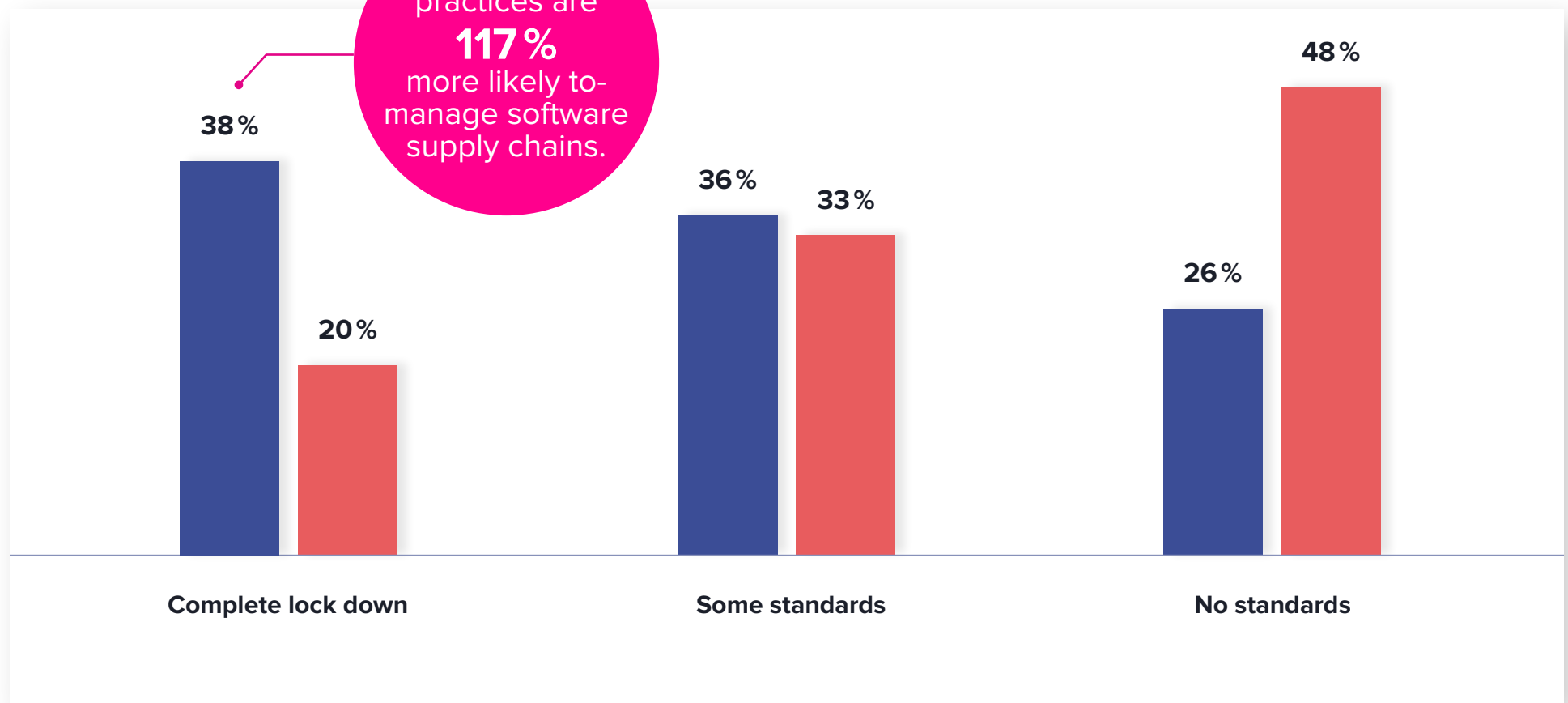


47%

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

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

Elite DevOps practices are **117%** more likely to manage software supply chains.

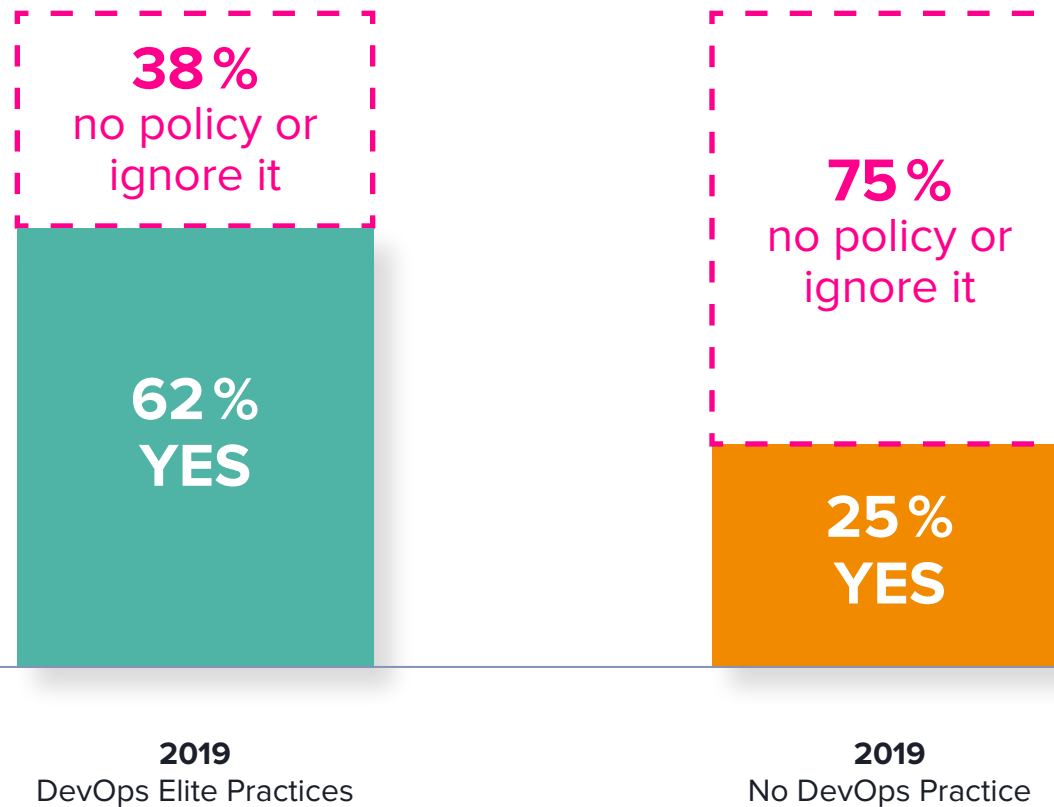


■ 2019 DevOps Elite Practices

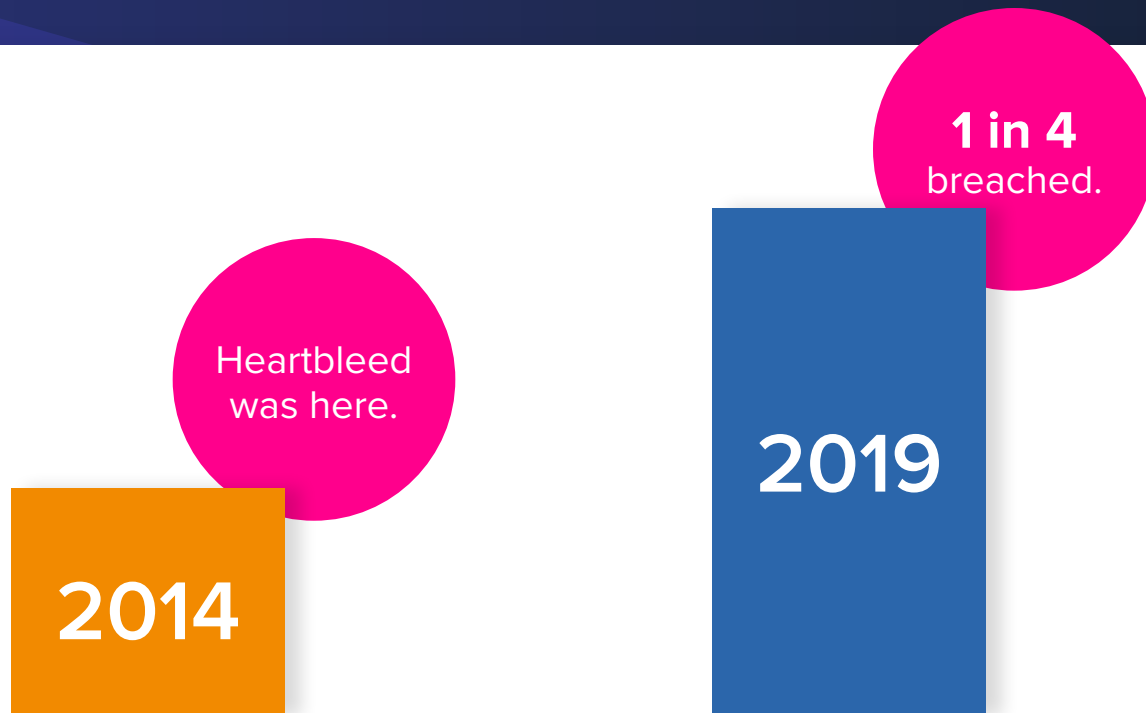
■ 2019 No DevOps Practice

Automation continues to be difficult to ignore.

Question: Does your organization have an open source governance policy? If yes, do you follow it?



Breaches tied to open source software components increased 71% over a five year period.

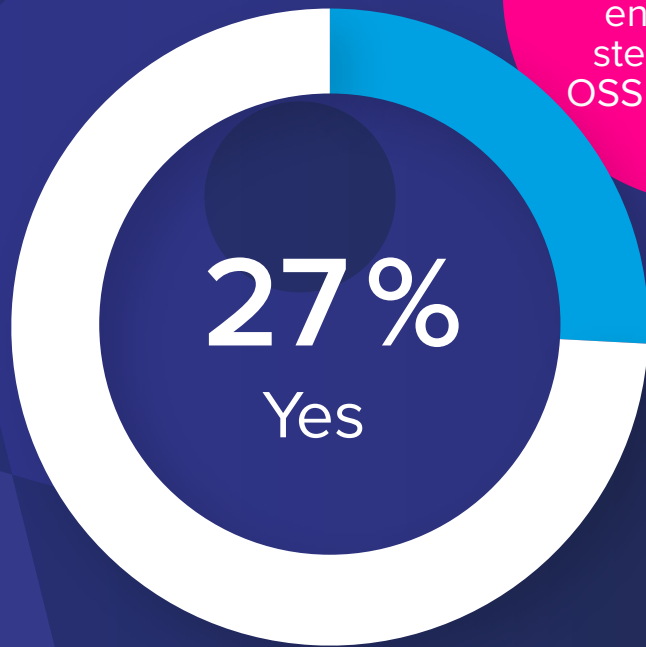


14%
suspect or have verified a breach related to open source components in the **2014 survey**.

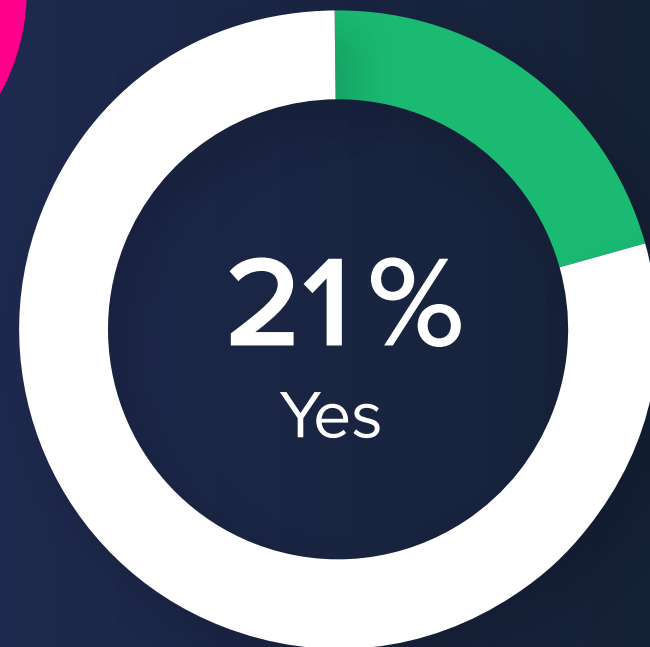
24%
suspect or have verified a breach related to open source components in the **2019 survey**.

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?

Elite practices are more aware of breaches in their environments stemming from OSS components.



2019
DevOps Elite Practices



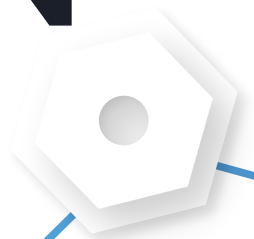
2019
No DevOps Practice

We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“DevOps practices enable us to deliver quality products, flexibility and time to market required today. The incorporation of security as part of the product development cycle is key. To really embrace DevOps, security needs to be seamlessly integrated to the software development lifecycle.”

- Ariel Kirshbom
Ernst & Young

ARTIFACTS AND AUDIT TRAILS, ENCRYPTION





COMPLIANCE AS CODE

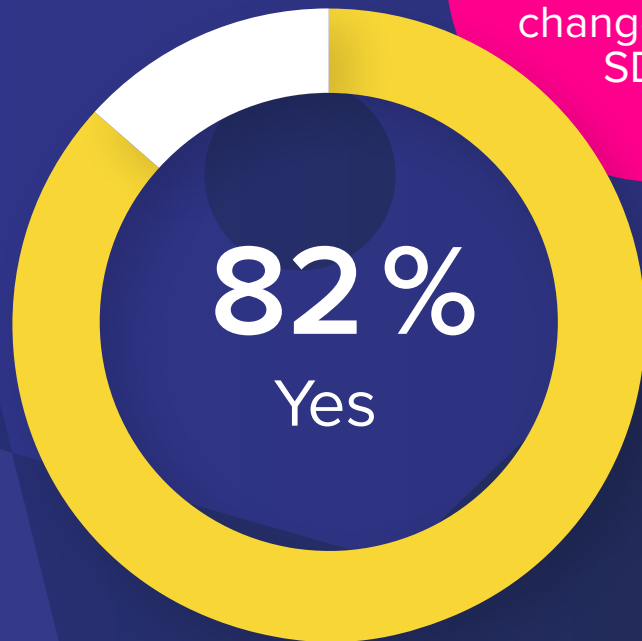
Many DevOps practices strive to achieve “compliance as code”. Building codified compliance policies and audit trails into development and operations enables these important guardrails to become an integral part of how DevOps teams work on a day-to-day basis.

Compliance policies and controlled workflows defined upfront by all stakeholders, help improve pipeline velocity while encouraging faster feedback loops when actions do not comply with policies. Within elite DevSecOps practices, changes to the policies or workflows can be formally approved and documented before being instrumented in code.

SECURING CREDENTIALS

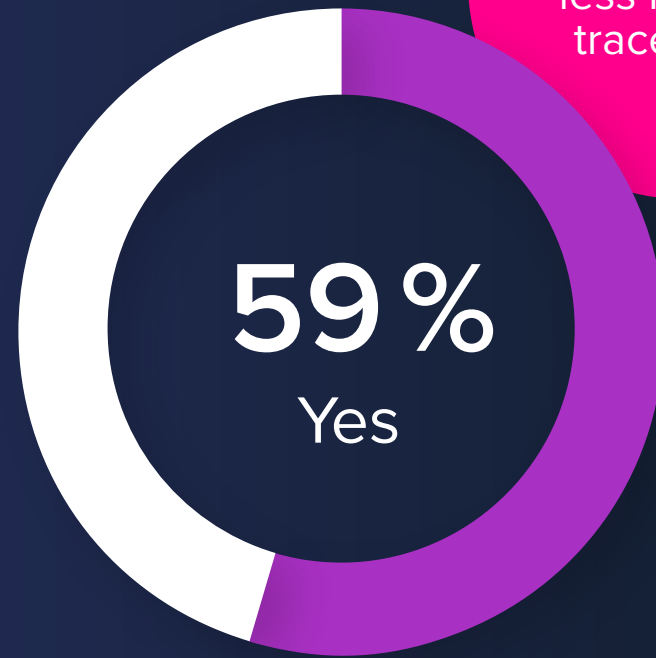
Committing passwords or keys to code within any repo is a poor practice. Yet for years, developers have electively published unprotected credentials to business critical databases, accounts, and applications to their internal repos, or worse yet, public repos like GitHub. Such practices can lead to data breaches or account takeovers with catastrophic effects. Automating encryption practices and improved training opportunities within elite DevSecOps organizations demonstrated that credentials are protected 63% more often when compared to those organizations with no DevOps practices.

Do you keep an audit trail of who changes what and when?



2019
DevOps Elite Practices

Developers have tools to monitor and audit all environmental changes in the SDLC.



2019
No DevOps Practice

Manual practices have less inherent traceability.

Do you have a retention policy of artifacts deployed to Staging and Production?

Staging Only

5.10%

Production Only

19.78%

No

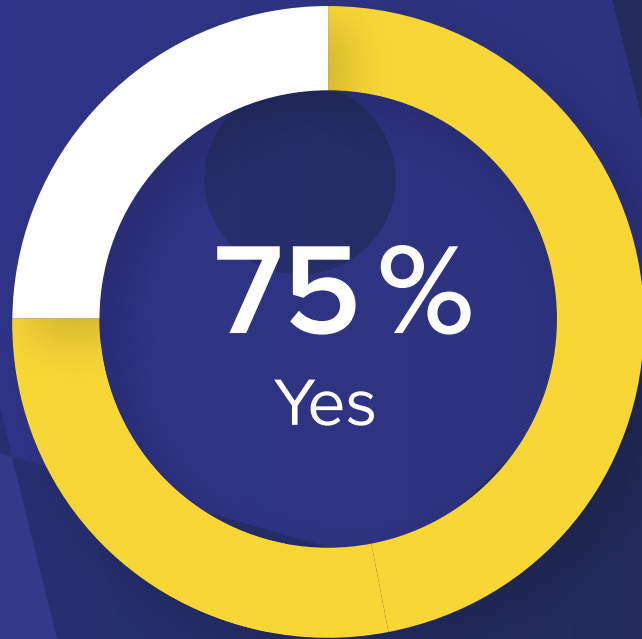
28.82%

Both Staging and Production

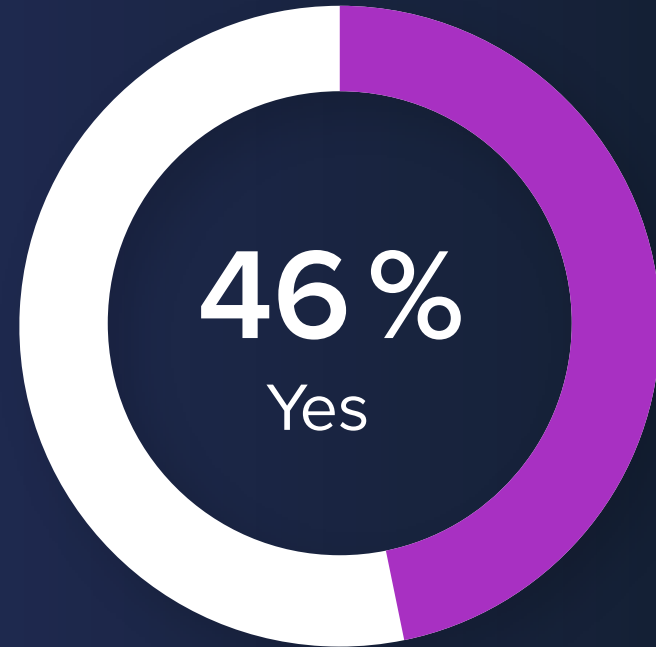
46.30%



Do you have all of your application-level credentials encrypted?



2019
DevOps Elite Practices



2019
No DevOps Practice

We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“**Successful DevSecOps projects are able to bring security into the DevOps processes without slowing them down. All in all, DevSecOps delivers reduced cost, reduced development churn, and reduced application attack surface, which delivers higher security and higher confidence to the organization.**”

- Jonas Manalansan
Northrup Grumman

TOP CHALLENGES





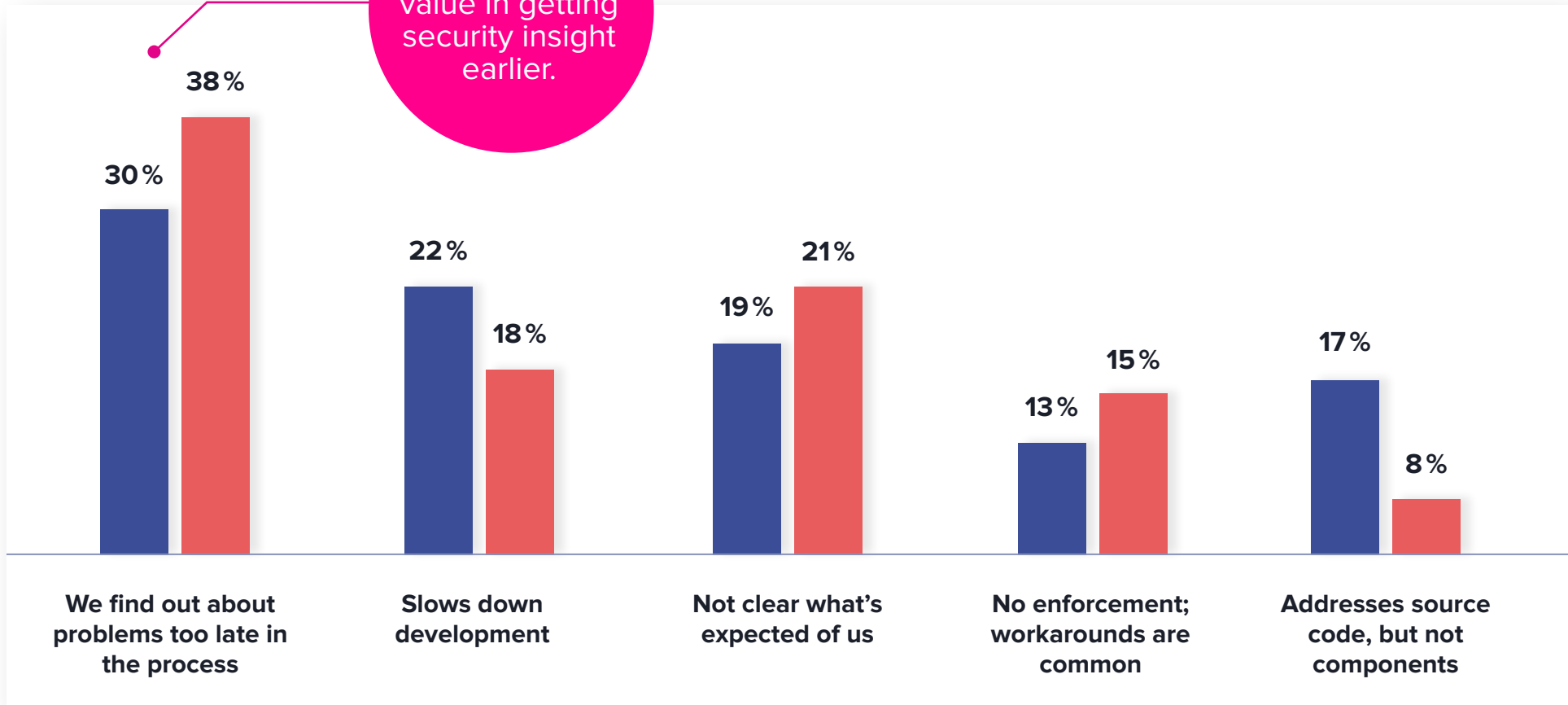
TO MOVE FAST, BE INFORMED

When applications and operational security practices are codified within a DevOps pipeline, compliance to those practices becomes easier. As noted earlier in this report, elite DevSecOps practices are building automated security practices into their SDLC processes not only more often, but much earlier.

While application developers continue to remark that security is important, this year's survey continues to reveal challenges developers face when security information is delivered to them late in the process, introducing dreaded rework and slowing their desired velocity.

Rank the top challenges with your application security processes.

Everyone sees value in getting security insight earlier.

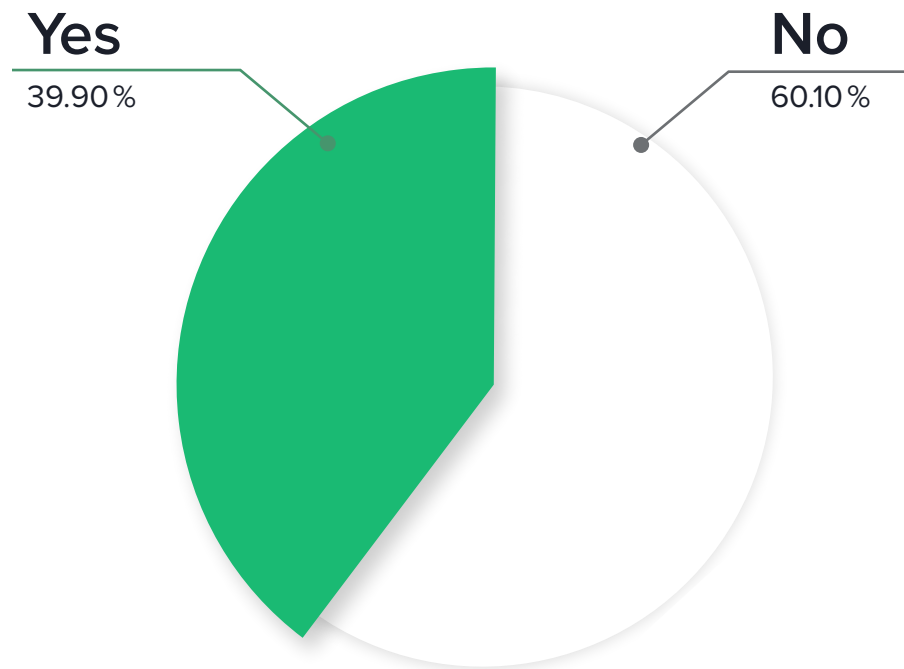


■ 2019 DevOps Elite Practices

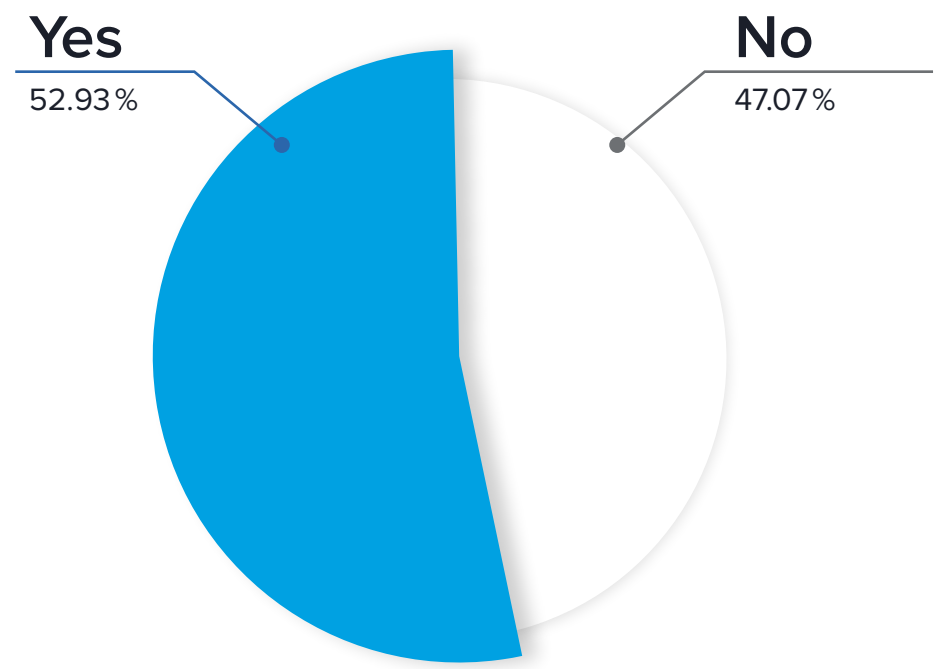
■ 2019 No DevOps Practice

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

Larger organizations generally have more personnel and processes in place that slow development.



Less than **100** developers



More than **5000** developers

We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“**DevSecOps and the automation that is usually paired with it is the only way a tiny appsec team can even remotely hope to get a handle of the huge number of development teams and applications in the organization.”**

- Michael Imamuraz
Turner Broadcasting System

BREACH AND RESPONSE



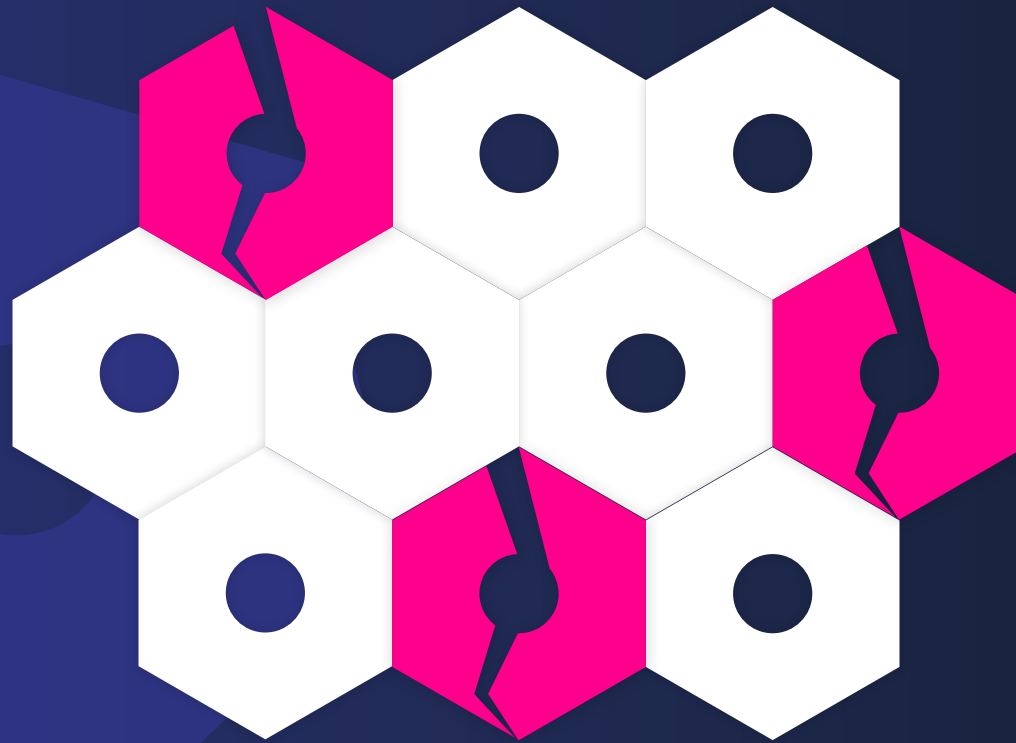


BE PREPARED

DevOps practices continued to reveal that the pace of software development is increasing. This year's survey revealed that 47% of organizations are deploying changes to production multiple times per week. This practice enables organizations to release value to customers faster and stay ahead of their competition.

While continuously challenged to stay ahead of peers in the marketplace, business also needed to stay head of the increasing threats from adversaries. Applications are now recognized as the most successful breach vector for adversaries, and this year's survey revealed how systemic the problem is. In the past 12 months, 24% of organizations surveyed revealed a breach within one of their web applications. Elite DevSecOps practices have come to realize that breaches are an inevitable part of business and as a result are ensuring plans exist to help accelerate operations returning to normal following an incident.





**1 in 4 companies confirmed or suspected a
web application breach
in the last 12 months.**

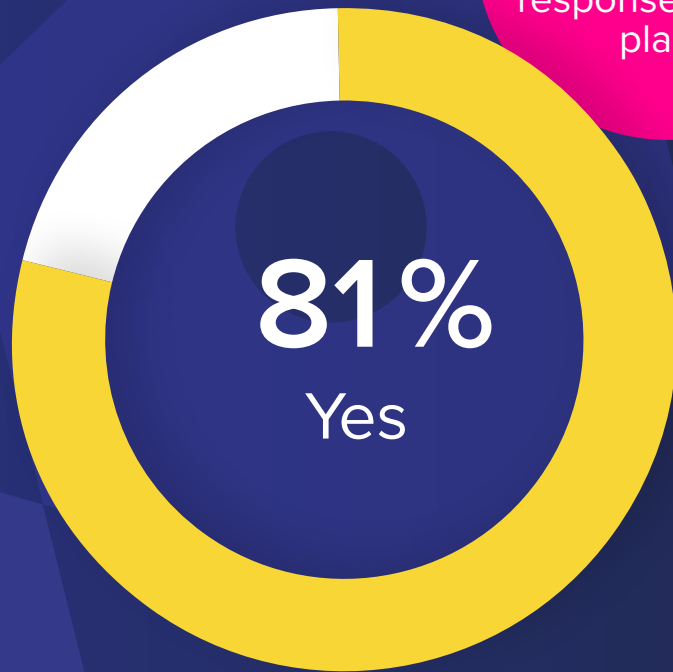
We asked each survey participant to tell us why DevSecOps practices are important to them. This is what they had to say:

“Key DevOps principles including: continuous learning via collaboration, automation (CI/CD), infrastructure as code, and monitoring, help ensure effective and timely responses to any breach. We must all recognize security is a living thing and organizations should be prepared to prevent and respond to breaches at any moment within their application lifecycle. It is difficult to imagine proper cybersecurity hygiene and sufficient preparations for a breach without DevSecOps in place.”

- Hasan Yasar

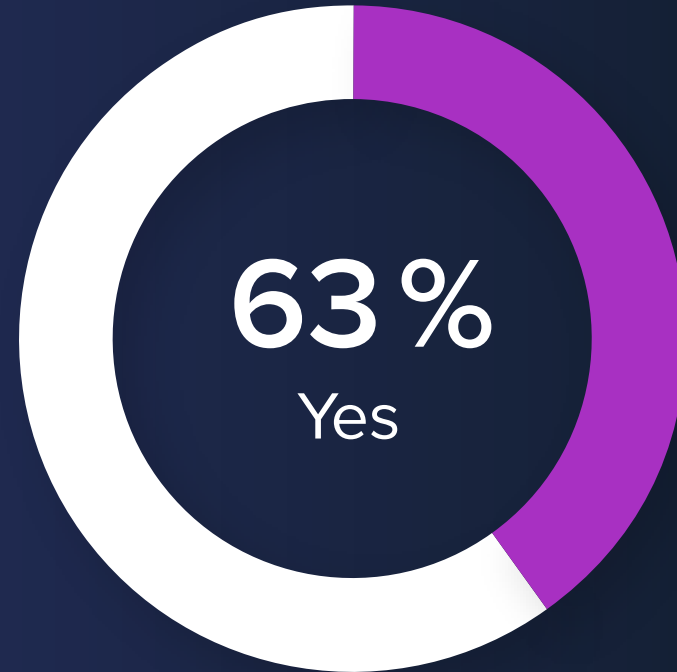
Software Engineering Institute | Carnegie Mellon University

Do you have a cybersecurity incident response plan in place?



2019
DevOps Elite Practices

Elite DevSecOps practices are 29% more likely to have response plans in place.



2019
No DevOps Practice




ABOUT THIS SURVEY

The DevOps community has rapidly grown over the past several years while pursuing security practices that run within high velocity, collaborative, and integrated environments. Waterfall-native security practices needed to evolve in order to prosper in a DevOps native world. 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 41 questions asked by Sonatype and our DevOps community advocates including CloudBees, Signal Sciences, Twistlock and Carnegie Mellon's Software Engineering Institute. The online survey was conducted between January 14, 2019 and February 4, 2019. This is the sixth 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 provides statistically representative results on the adoption, practices, and challenges of managing DevOps practices with regard to security requirements. For this project, 5,558 IT professionals responded to the survey with 3,779 (68%) completing it in its entirety.



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 2019 survey were identical to prior years. Although we invited past participants to our 2019 survey, not all participants between the two surveys were the same. For people who self-identified, we saw that 58% live in North America, 18% live in Europe, 9% live in Asia, and the remainder of the people participated from other regions of the world. Overall, we saw IT professionals from over 150 countries participate.

The survey’s margin of error is ± 1.226 percentage points for 5,558 IT professionals at the 95% confidence level.