
sonatype
DevSecOps
academy
2020
DEV
SEC
OPS
COMMUNITY
SURVEY
CloudBees
ADDO
ALL DAY DEVOPS
DevOps.com
DEV
SEC
OPS
DAYS
NowSecure
SECURITY
BOULEVARD
DevOps
INSTITUTE
ADVANCING THE HUMANS OF DEVOPS
VERICA
Carnegie
Mellon
University
Software
Engineering
Institute

Derek Weeks
Vice President,
Sonatype

DJ Schleen
DevSecOps Advocate,
Sonatype

2020 DEVSECOPS COMMUNITY SURVEY

Welcome to the 7th Annual DevSecOps Community Survey

As the longest and largest running survey of DevSecOps practices in the industry, our 2020 survey had 5,045 respondents from over 70 different countries.

Once again, we took a look at the differences between mature and immature DevOps practices, but added a new twist to explore how those maturity levels impacted developer delight. Those organizations with mature practices benefited the most from higher rates of job satisfaction, employee loyalty, and developer productivity.

We also discovered that happier developers work in organizations with more automated security tools and better training, while they also demonstrated greater adherence to security policies. The happiest developers built more security practices into their applications, and the pipelines that build them.

Our community survey also reviewed where DevSecOps investments were being made and to what extent that influenced developer interest in security. We also expanded our list of tool sets to get a pulse on what developers are both integrating and automating for their product development.

Finally, our research delves into developer awareness of breaches related to software development practices. While more investments have been made in DevSecOps, confirmations of breaches remain too high.

We hope you enjoy the DevSecOps Community Survey, use the findings to reflect upon your own practices, and begin new conversations about what your next priorities will be for 2020.

— DJ SCHLEEN & DEREK WEEKS

Who Participated?

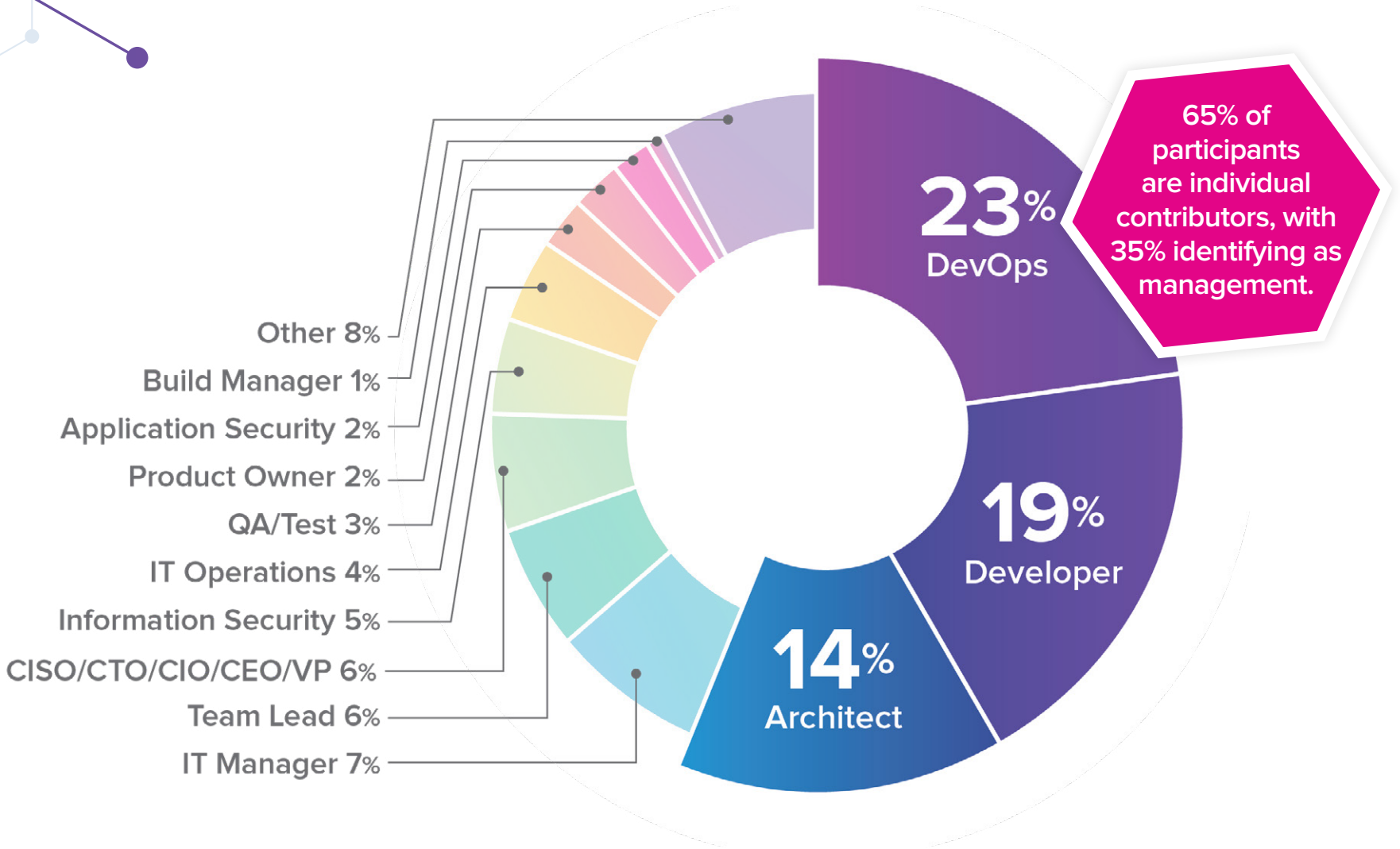
5,045

people shared their views for this survey.

The top 10 countries represented are:

- United States
- United Kingdom
- India
- Canada
- Australia
- Spain
- Netherlands
- Germany
- Singapore
- Israel

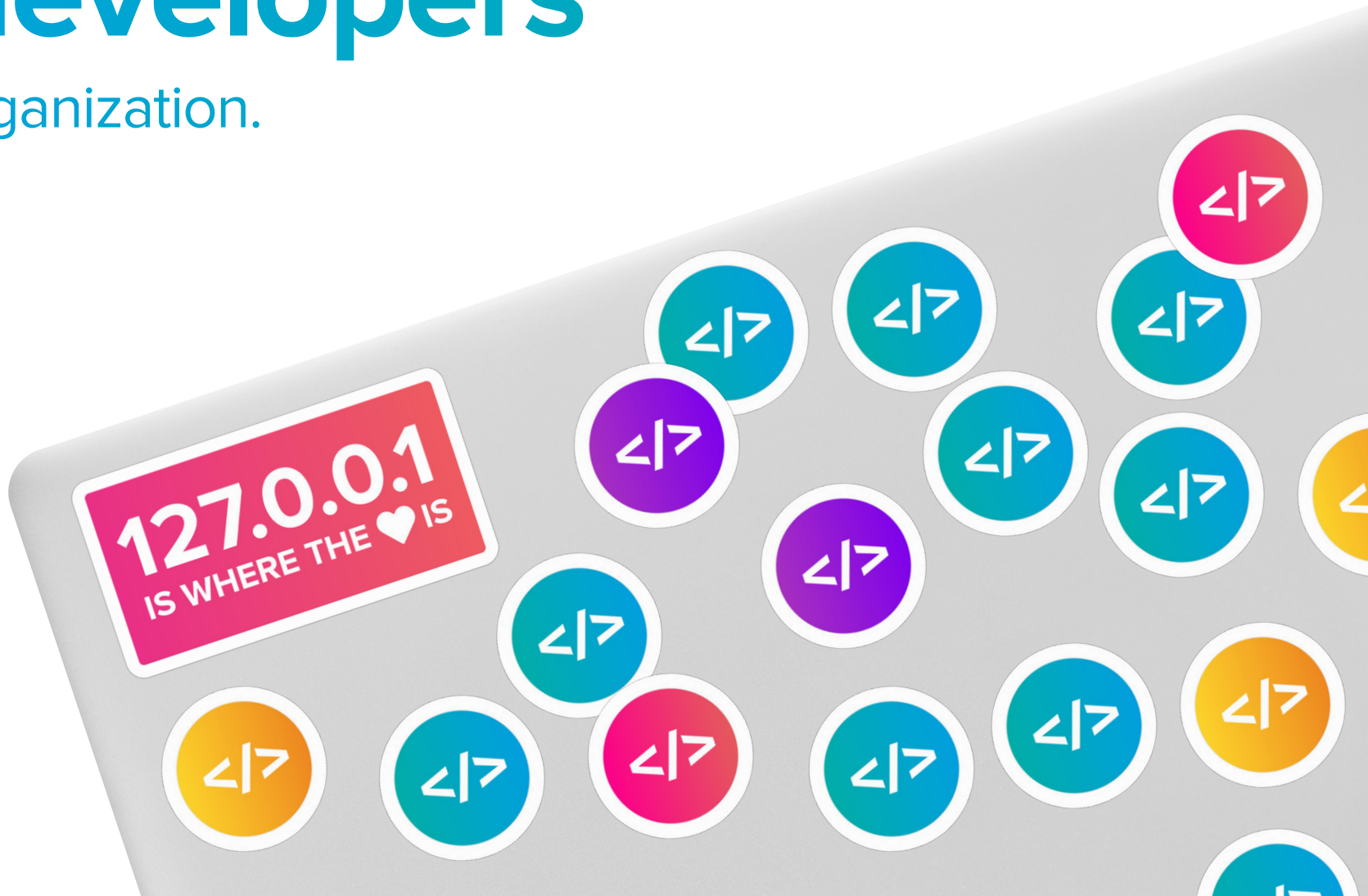
Which title best matches your role within the organization?



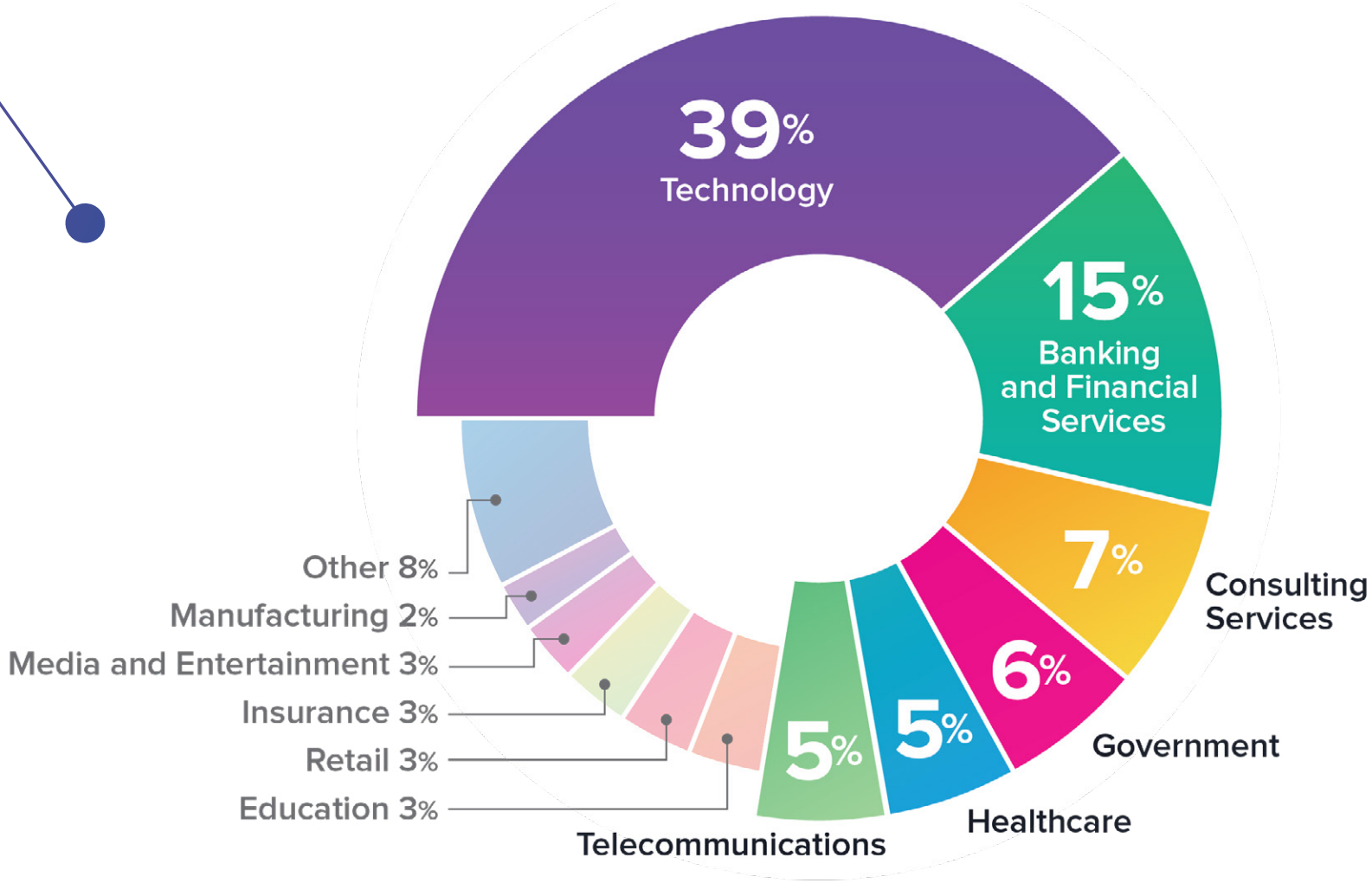
Of respondents to the survey,

68% have more than 25 developers

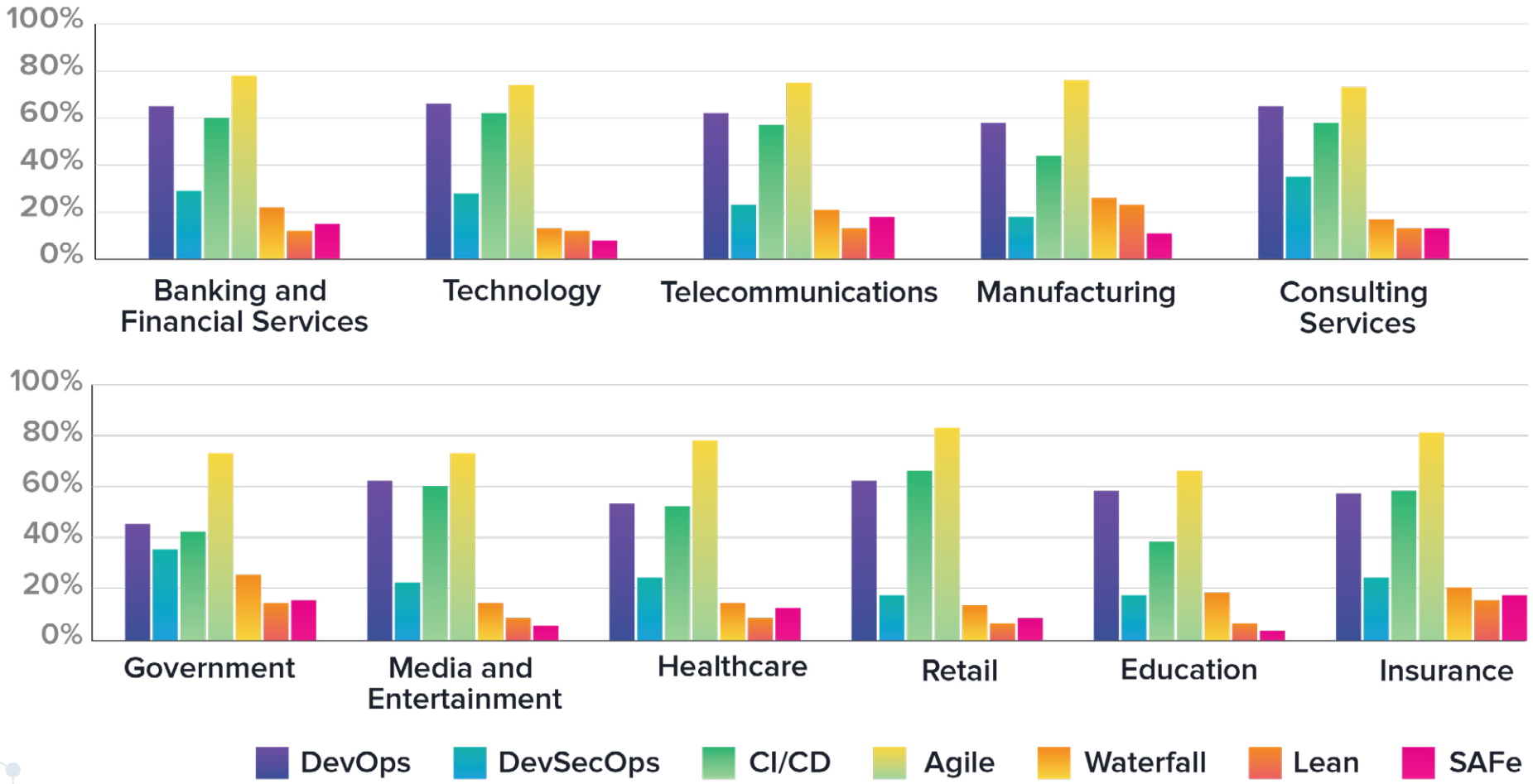
in their organization.



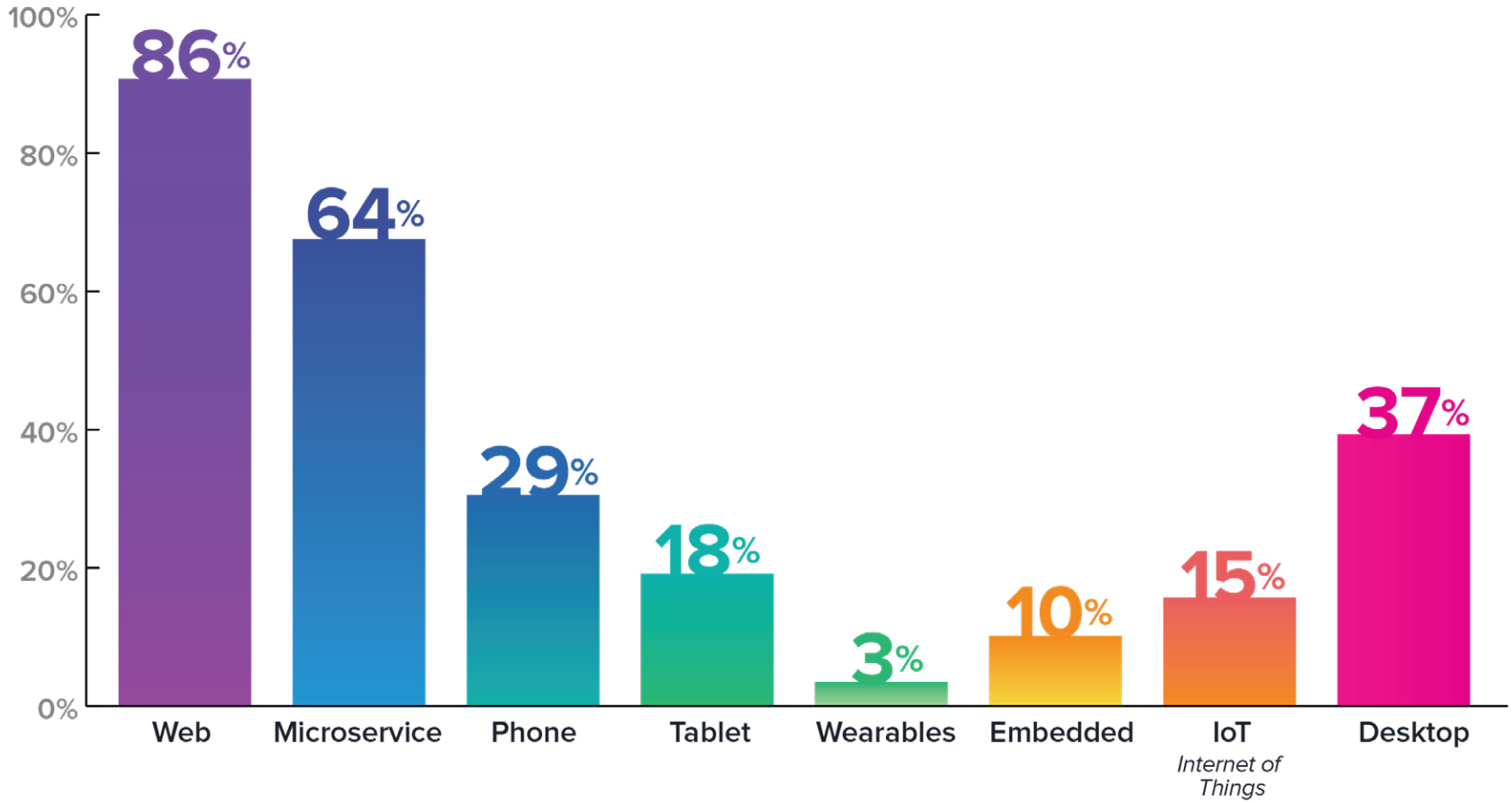
In what industry is your organization?



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



What types of applications do you build?



Practices

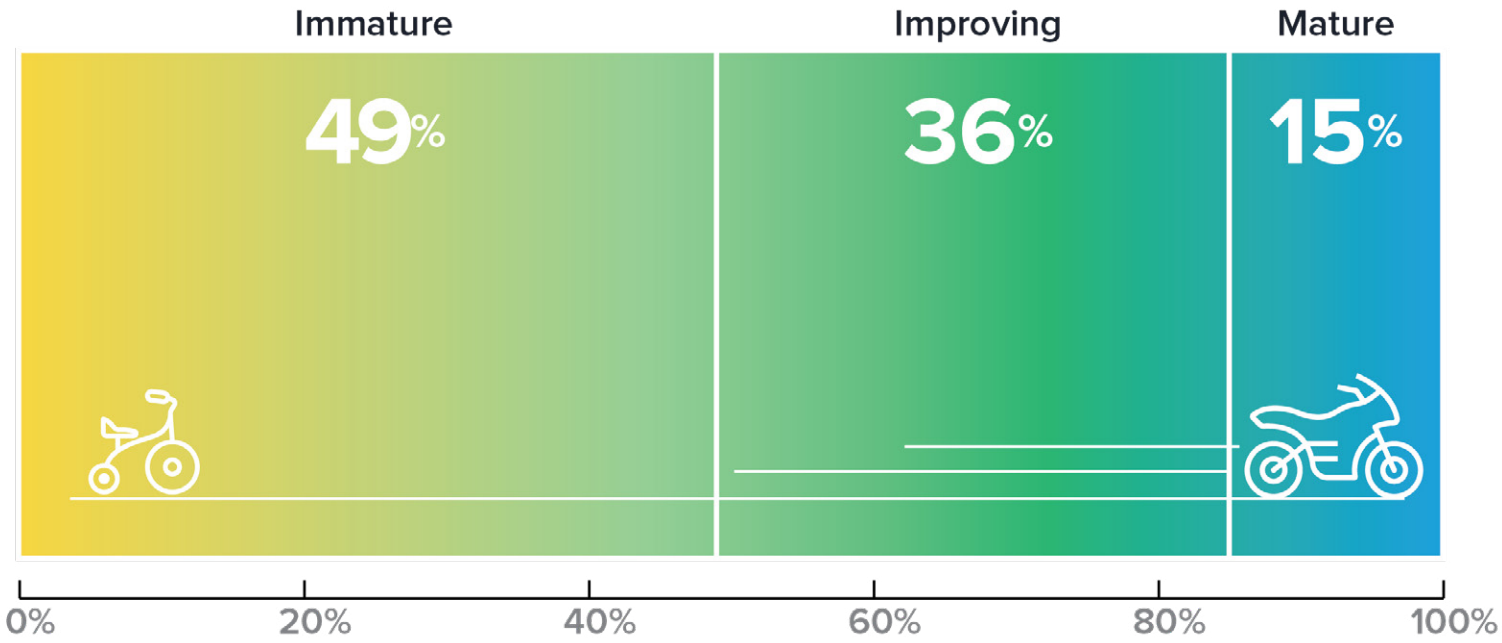
It's not what we do once in a while that shapes our practices, it is what we do consistently.

Buckminster Fuller once said, "You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete." This is where technique in DevSecOps resonates and culture lives, as more organizations implement tool automation. They are in essence creating a new model and changing the way applications are built.

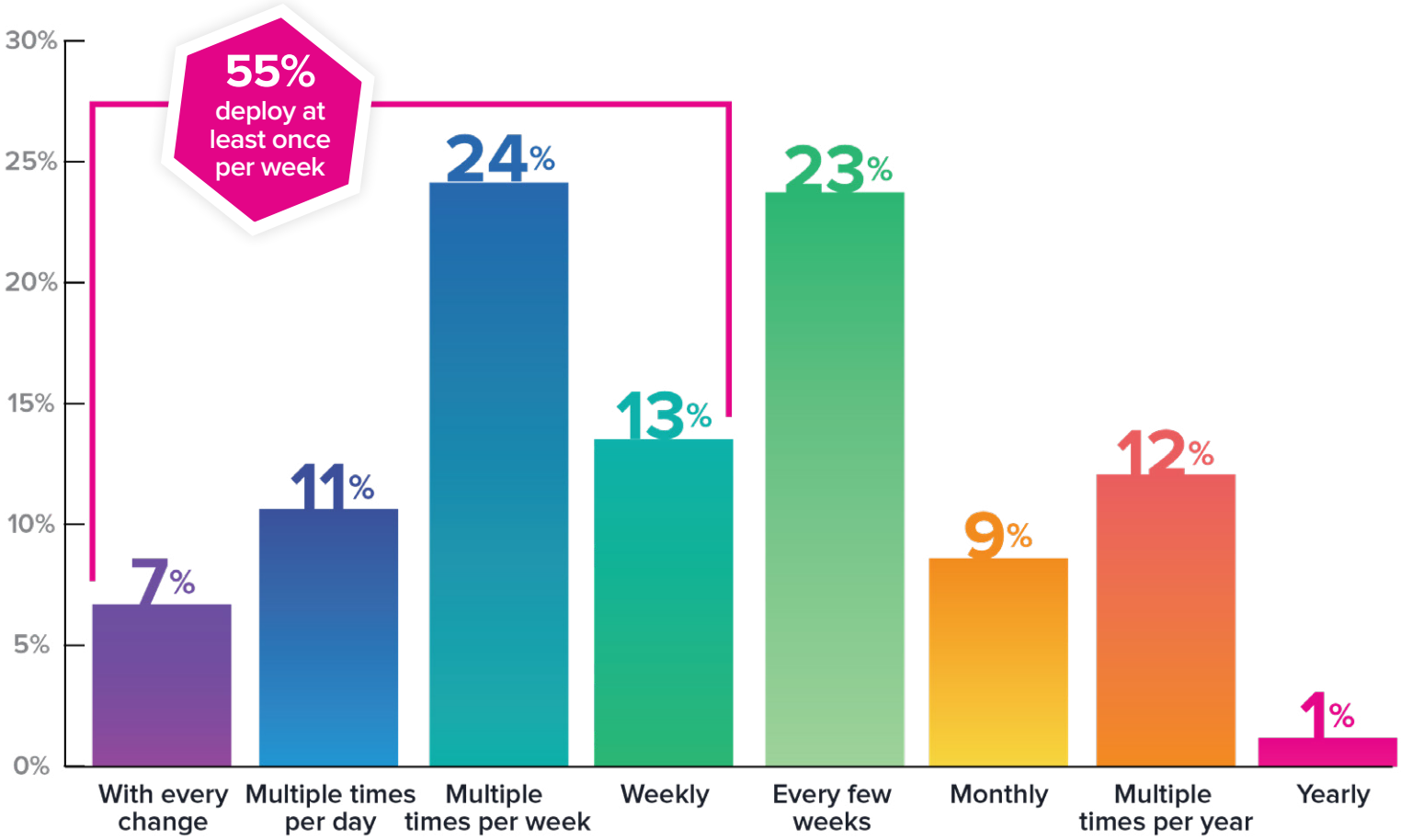
The integration of security controls into automated pipelines continues to be stronger in mature practices, although immature and evolving DevOps practices continue to integrate more and more of these security controls. In all organizations, we see that Web Application Firewalls, Intrusion Detection Systems, and Open Source Governance make up the top three security controls implemented.

Integrated tooling provides detailed information further left in the application development lifecycle and therefore allows developers to quickly identify and remediate issues and zero-day vulnerabilities earlier in the process.

How mature is your adoption of DevOps practices?

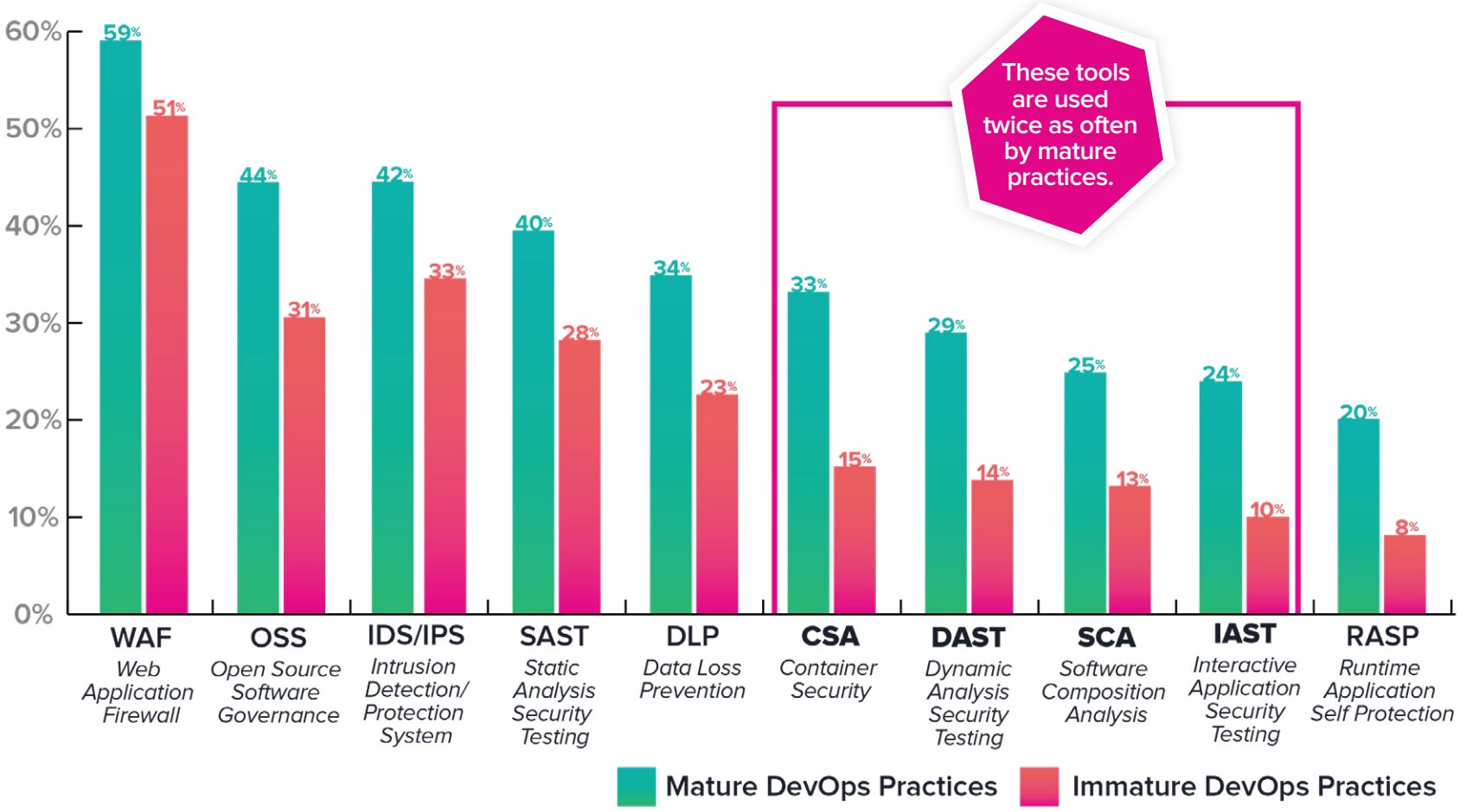


How frequently do you deploy to production?

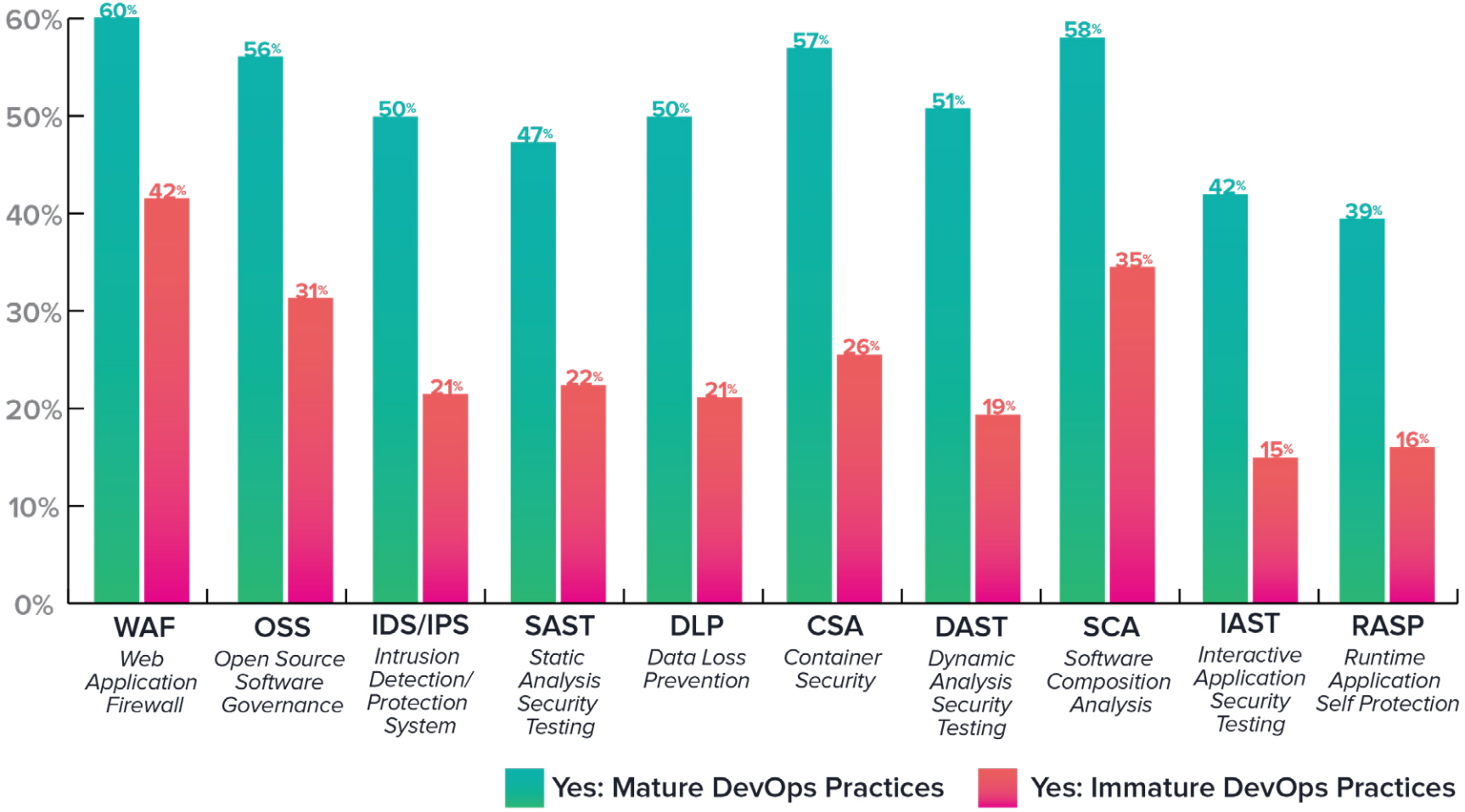


What security tools do you or your team use?

Mature DevOps practices prioritize WAF, OSS Governance, and IDS/IPS.



Are security tools properly integrated within your team's development pipeline?

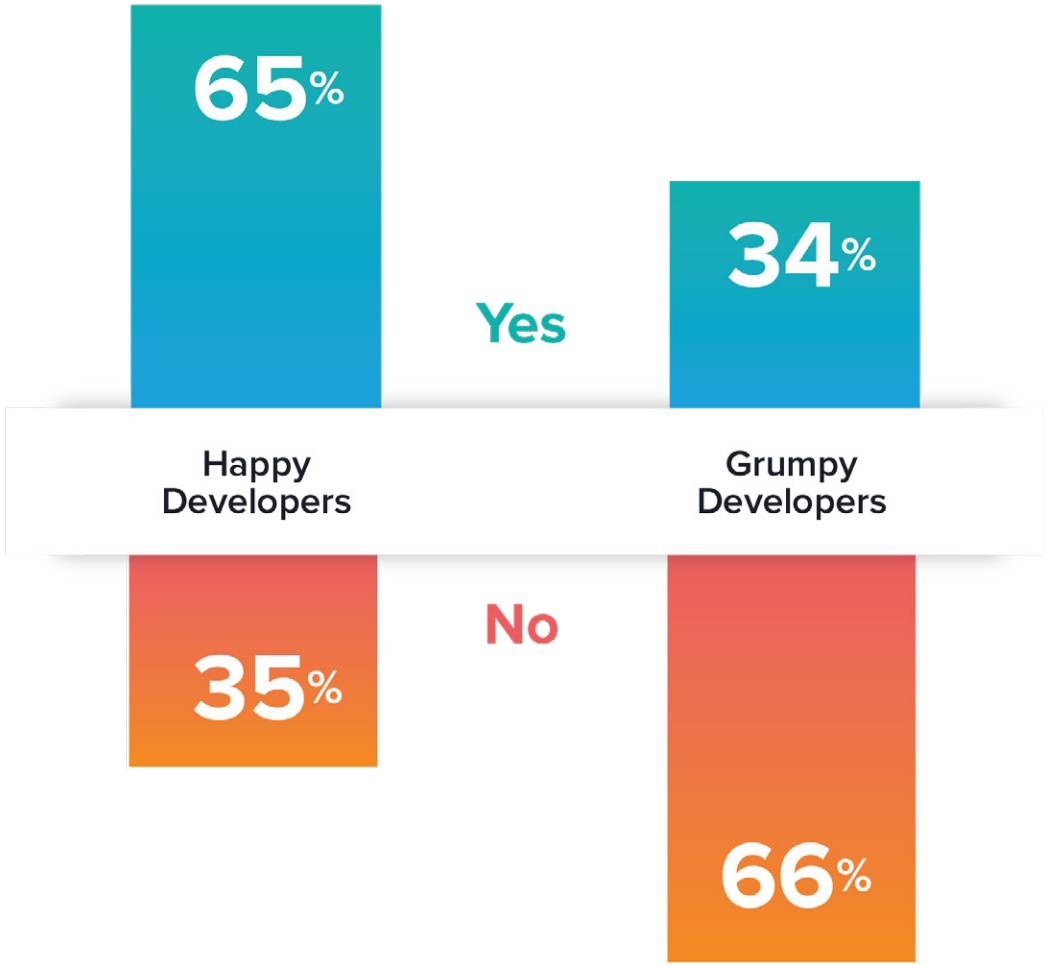


Mature DevOps teams properly integrate automated security tools

almost two times more often

than immature development practices.

Does your team perform security analysis of its code?



“

Security falls short when things get shipped under pressure. This is not the case as often when security is part of the process.

”

DENNIS ORNER, *Software Engineer, TWT Digital Health, Germany*

Culture

Happiness Matters in DevSecOps

Culture cannot be forced. It has to be nurtured. Strong development culture is based on candid communication between team members, respect people have for one another, and the celebration of technical artistry. Together, culture flourishes.

Our 2020 DevSecOps Community Survey reveals that the more evolved DevOps practices are in an organization, the happier we found their developers. Here, we'll share evidence that happy developers spend more time thinking about security than grumpy developers in less mature organizations.

So who are the happiest developers? We combined several attributes of survey respondents, including those who were satisfied, or extremely satisfied, with their job. The happy crew also recommended their employer to friends seeking a new job. They also had the tools they need to complete their job, were more likely to receive training, and were mostly part of mature DevOps teams.

Grumpy leaned in the opposite direction. These developers demonstrated low job satisfaction rates, wouldn't recommend their employer, and had less access to training. They also had access to fewer automated security tools compared with their happier peers.

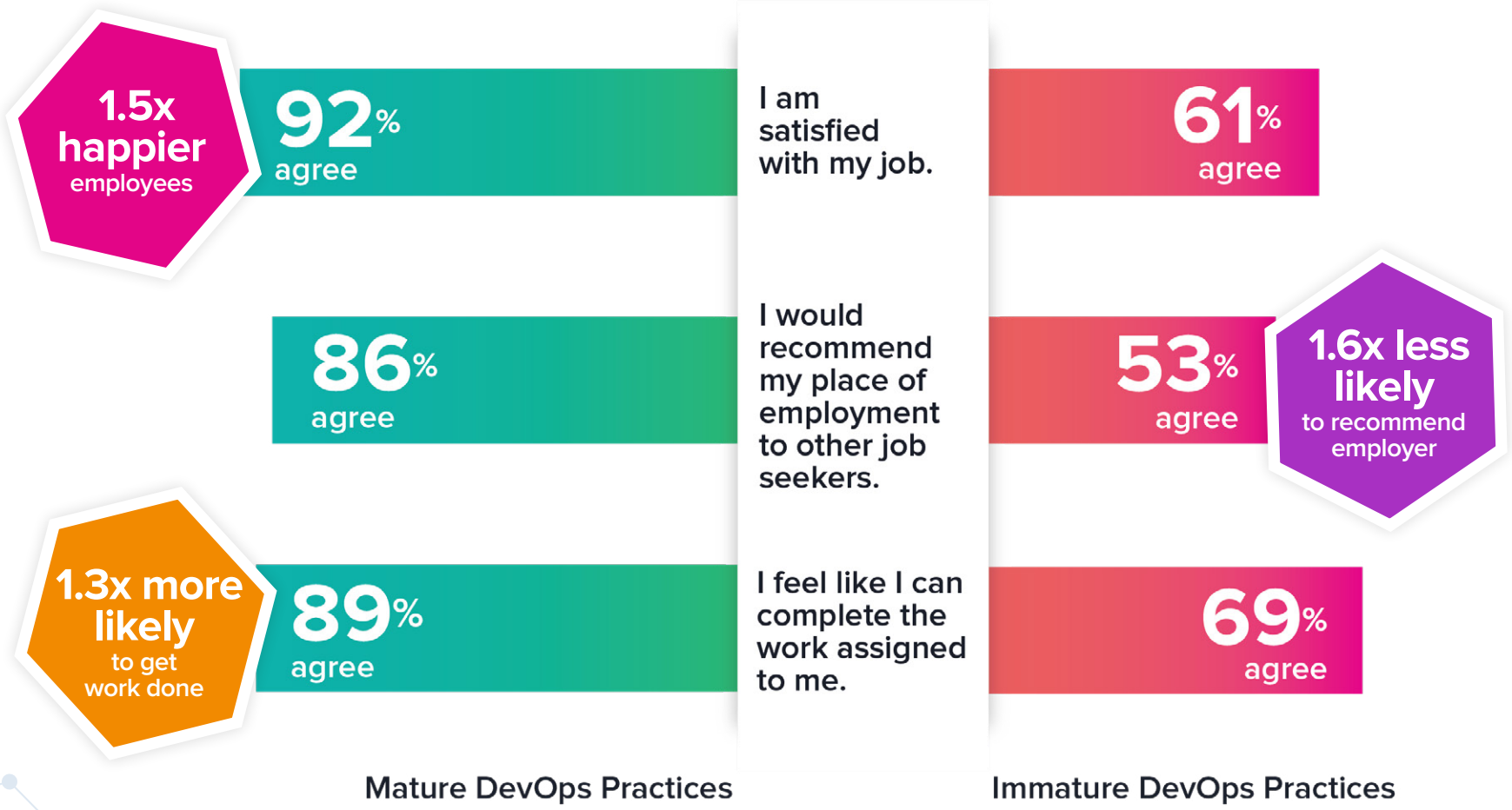
One question that we had originally intended to be a humorous was "Who causes the most friction in your organization?" As it turned out, the question was very relevant to culture. In mature DevOps practices, developers overwhelmingly said that there was no friction on their teams, while in immature practices management was identified as the key source of friction.

Happy developers are

3.6x more likely

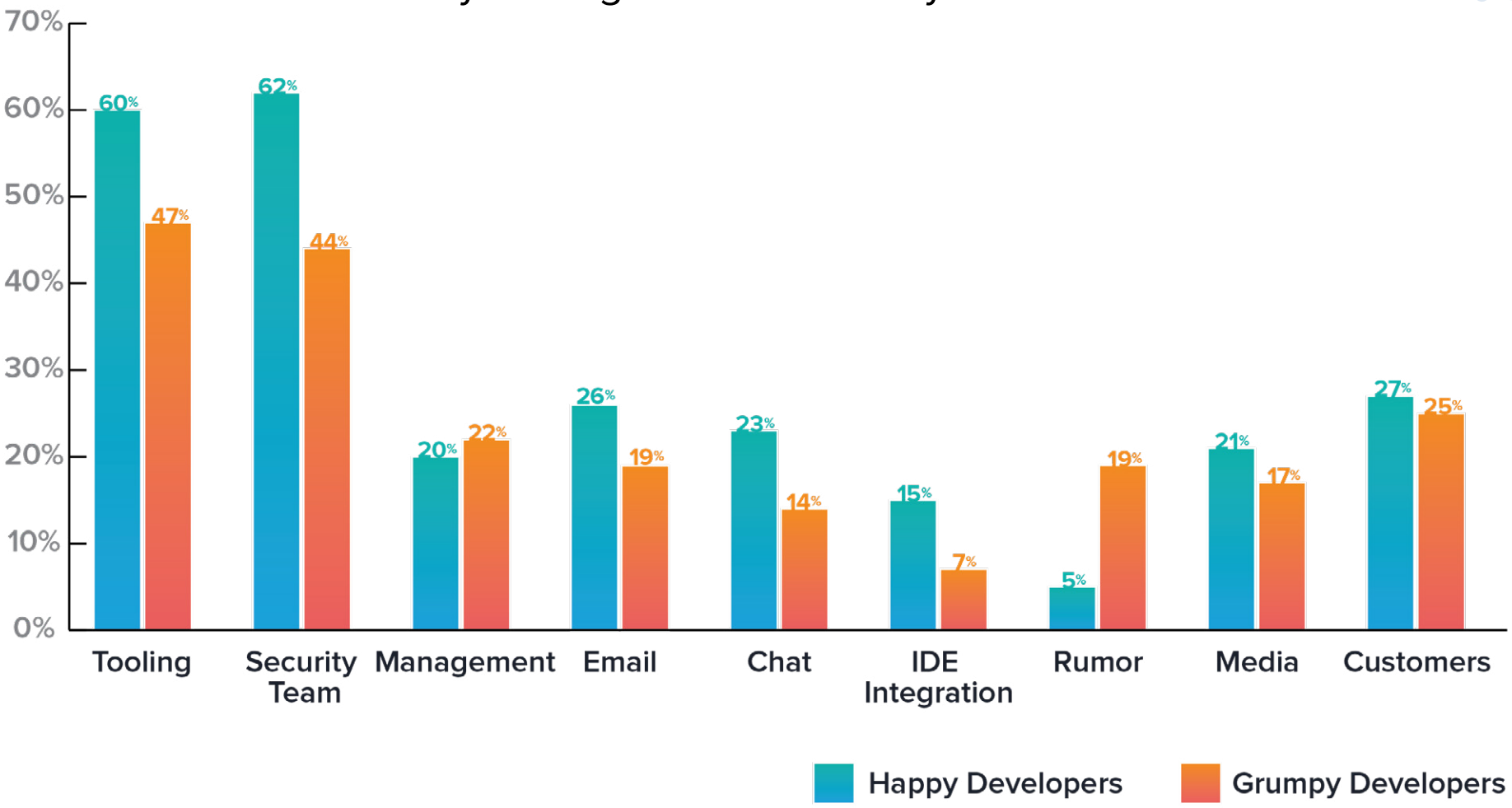
to pay attention to security.

Job satisfaction is higher in mature DevOps practices.



How are you informed of application security issues?

Happy developers are informed 1.3x more by tooling and 3.8x less by rumor.



Mature practices are

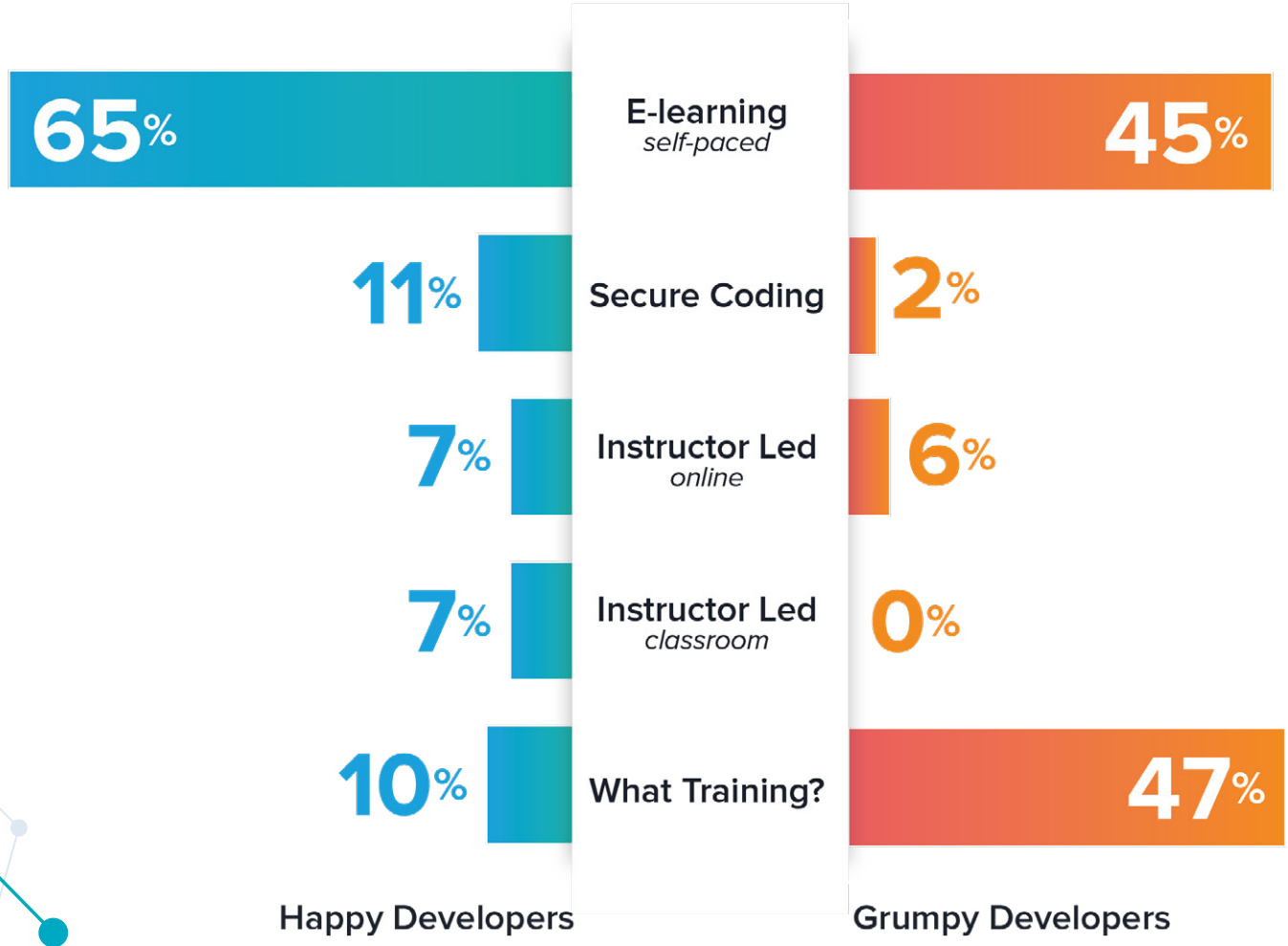
3.8x less likely to rely on rumors

when it comes to security incidents.

Instead, they're focusing on empirical evidence from better integrated tooling and security teams.

What application security training is available to you?

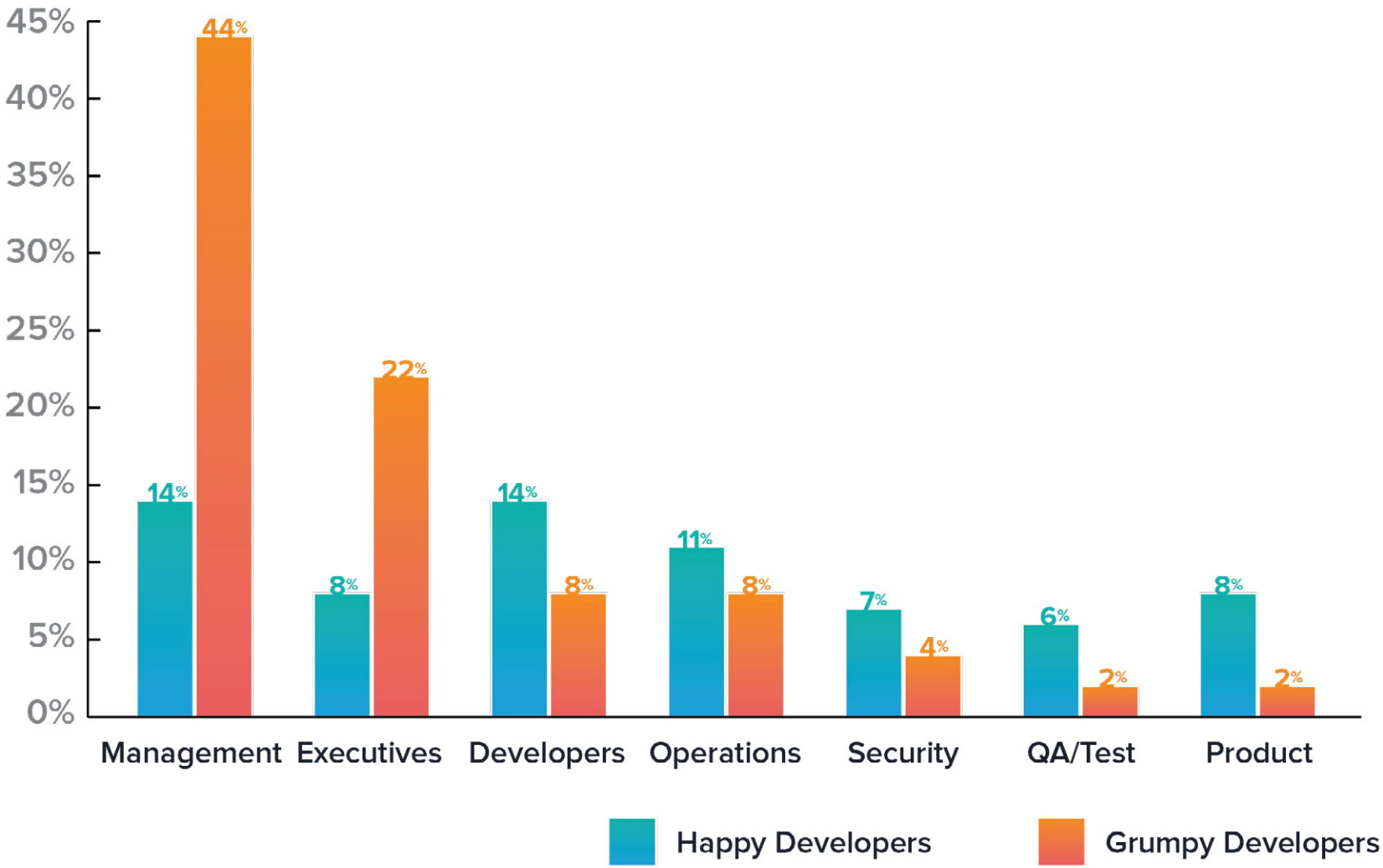
E-learning outpaces all other forms of application security training for developer education.



Developers who receive training on how to code securely are

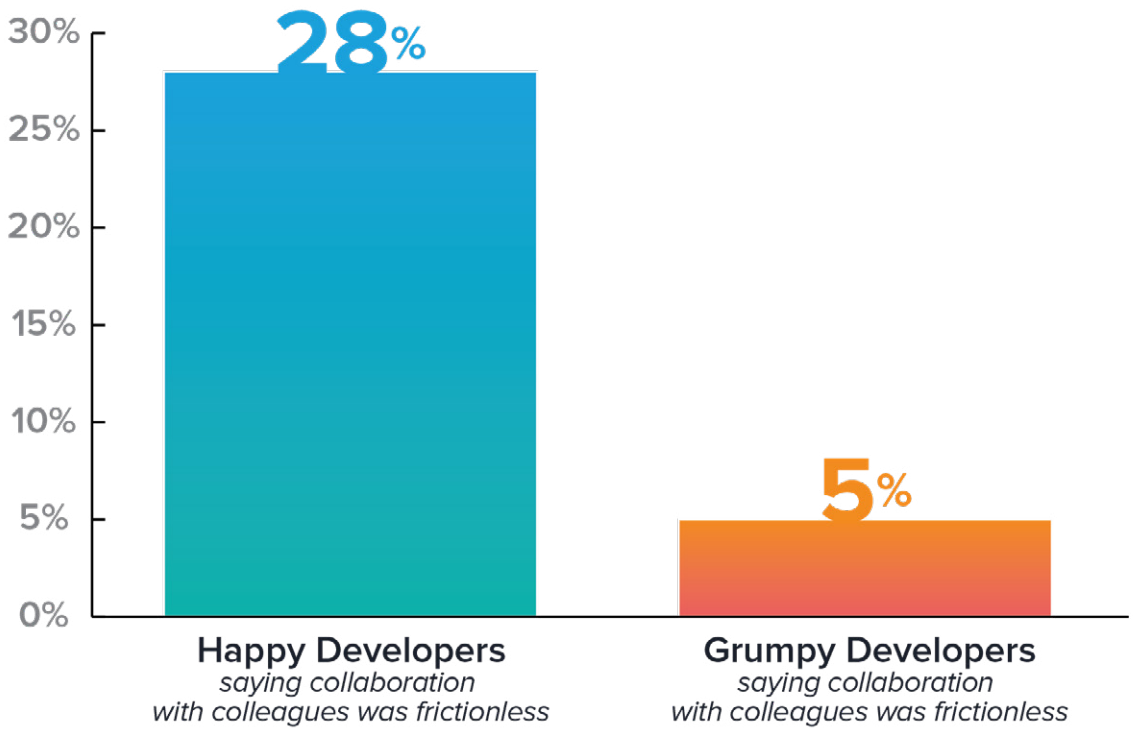
5x more likely to enjoy their work.

Who causes the most friction on your team?



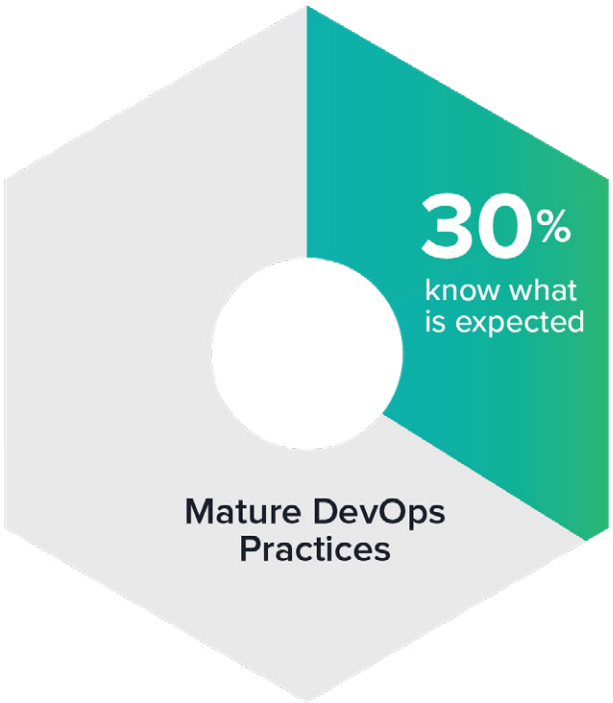
Happy developers experience less friction with colleagues.

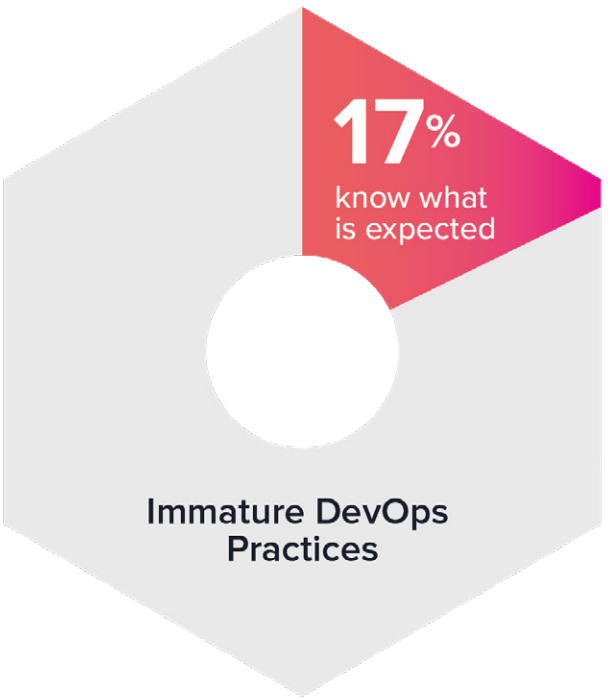
Happy developers were 5.6x more likely to say they experienced "no friction" working with various functional roles in the organization compared to their grumpy counterparts.



Developers in Mature DevOps Organizations know what to do.

They are 1.8x more likely to know what is expected of them.





> The path to success for DevOps security lies in changing the underlying culture to embrace it. Removing human stage-gated steps from the process, and adding a ‘Continuous’ element to everything is key to DevOps and Security adoption.

MALAY NAYAK, *Agile Coach, New Zealand*

Motivation

Action isn't just the effect of motivation, it's also the cause of it.

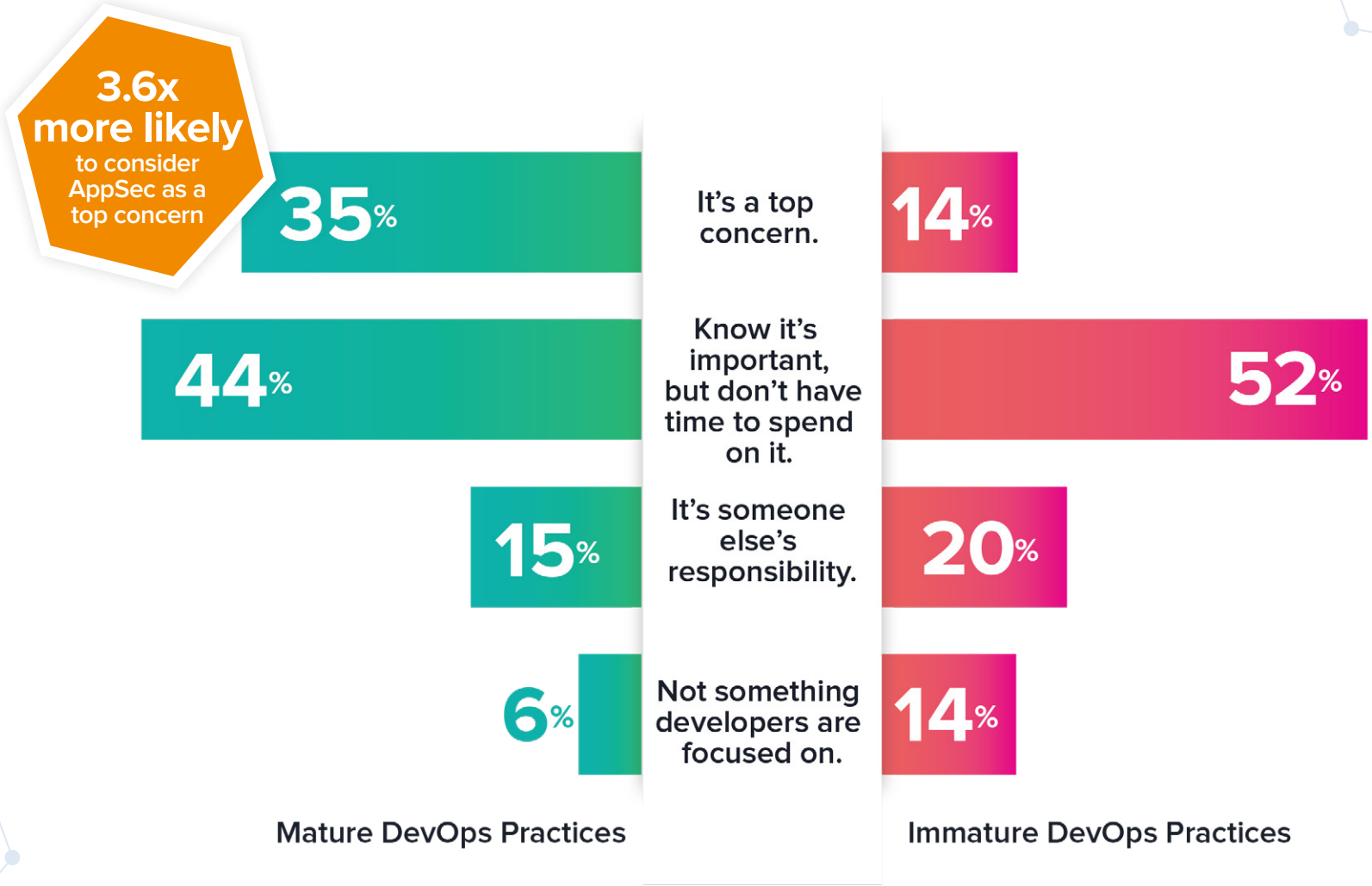
The only way for things to get done is for people to be motivated to do them. Integrating security into a software development life cycle can either be mandated or voluntary.

Once again, our survey shows that Governance and Compliance considerations are the number one motivator for integrating security into DevOps practices. We also found that executives in mature DevOps practices are 2x more likely to look at the integration of security controls as a competitive advantage.

Breaches have always been a motivating factor for increasing the security protection of any application. Although organizations are striving to get ahead of breaches, developers still don't have enough time to invest in building secure code.

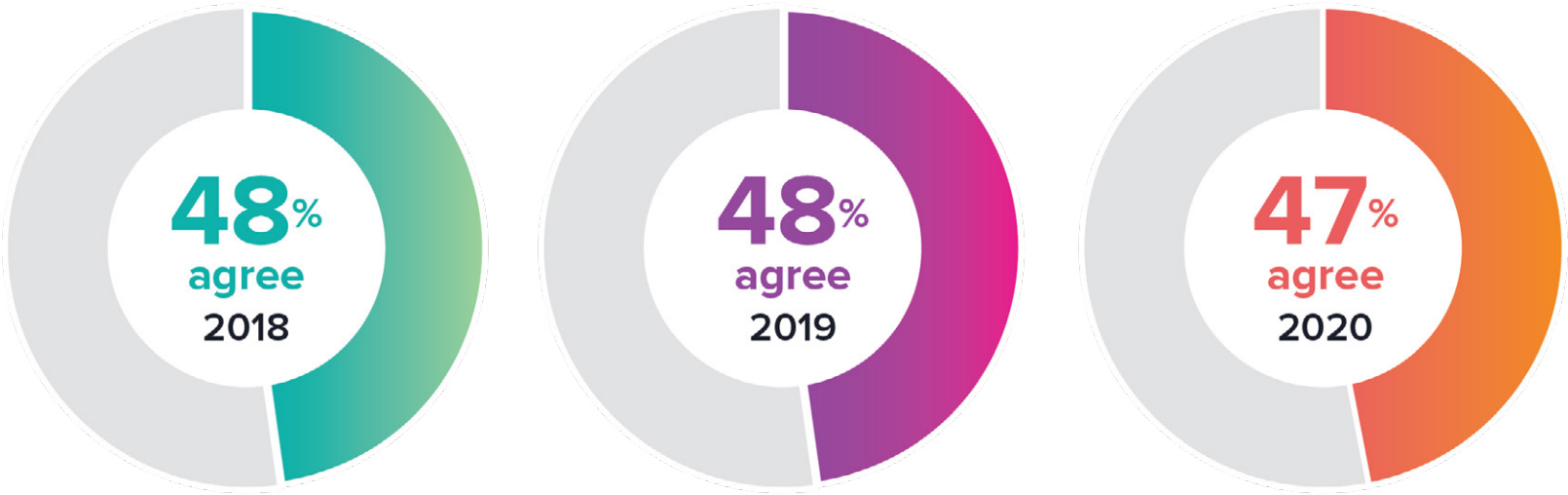
What is your team's main motivation to implement security controls?

What is your interest in application security?

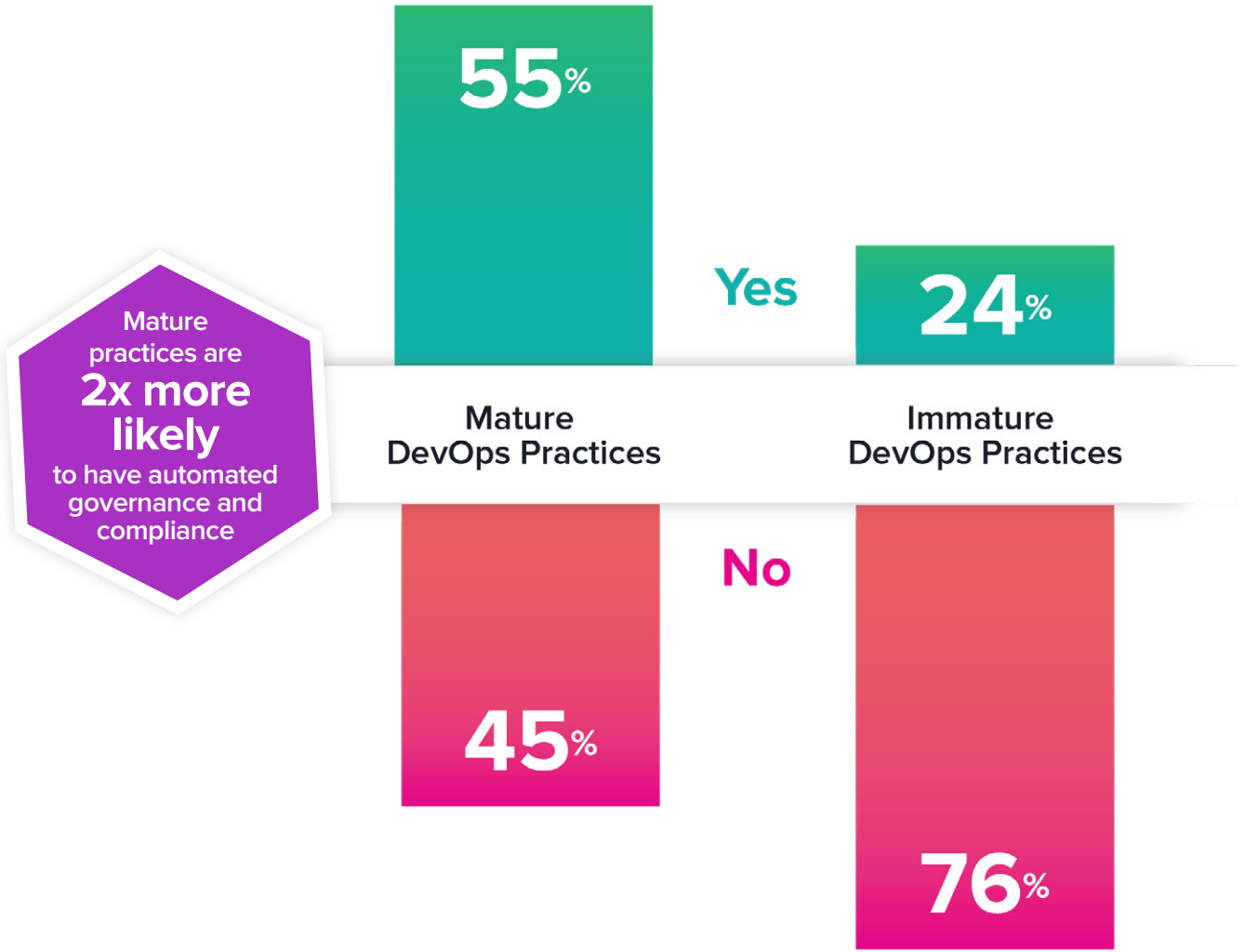


Developers know security is important, but they don't have time to spend on it.

A comparison of all survey responses 2018 – 2020



Are governance and compliance automated in your team's development process?



“The time to market is shorter every year and older security practices slow down development. Teams had to find a way to speed up without compromising security. This is how DevSecOps started. The ultimate goal is to unite security teams and developers while ensuring fast, safe delivery of code.”

ANAND PATIL, *Architect, CTS, Australia*

Breaches

Some findings in our annual survey generate more conversation than others, and breaches tend to top the list.

This year, 24% of respondents confirmed or suspected breaches tied to their application development practices.

When reviewing this year's analysis, keep in mind that developers and DevOps professionals made up a significant portion of our participants while 6% identified as information or application security.

Our survey has tracked breaches tied to open source components used in applications since 2014. That year, 14% of respondents had confirmed or suspected breaches — it was the year of OpenSSL. Breaches identified by our community peaked in 2018 at 31% — the year Equifax made headlines. As post-Equifax investments pay dividends, participants in 2020 reveal that open source related breaches are down 30% from their high. That is good news.

As with many findings, we took a deeper dive to better understand breach activity. As you will see, results varied from 19% – 28% depending on the maturity of development practices employed. Consistent with our 2019 findings, those with mature DevOps practices suggested more breaches were identified during the past 12 months. Why would mature organizations experience more breaches?

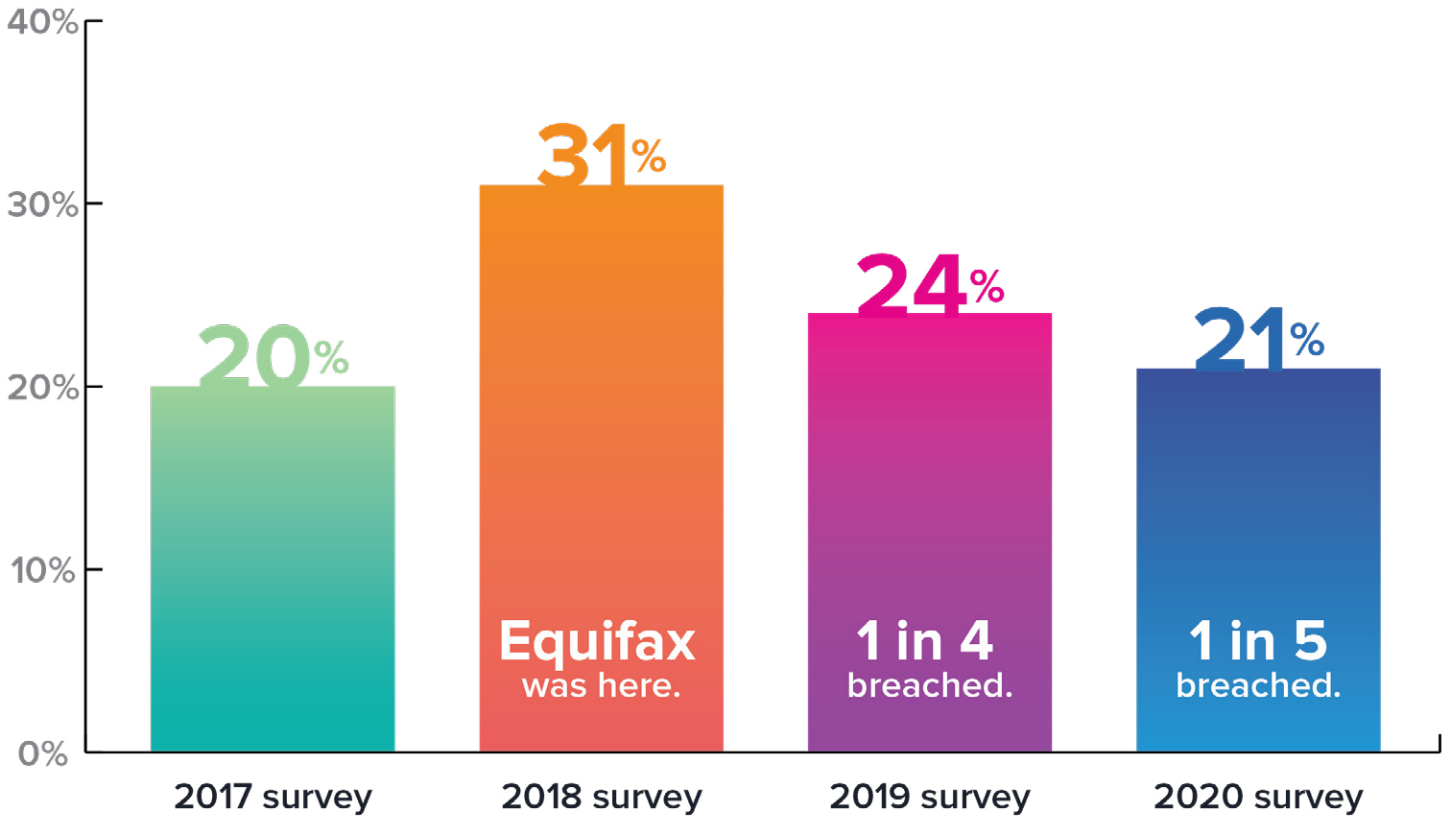
DevOps practice and thought leaders continue to suggest that mature DevOps cultures supports scenarios where information is actively sought, new information is welcomed, and bridging functional groups is a rewarded behavior. Failures are not silent in mature DevOps practices, but rewarded. For mature DevOps practices, awareness is one of the best agents for driving change.

24% suspect or have verified

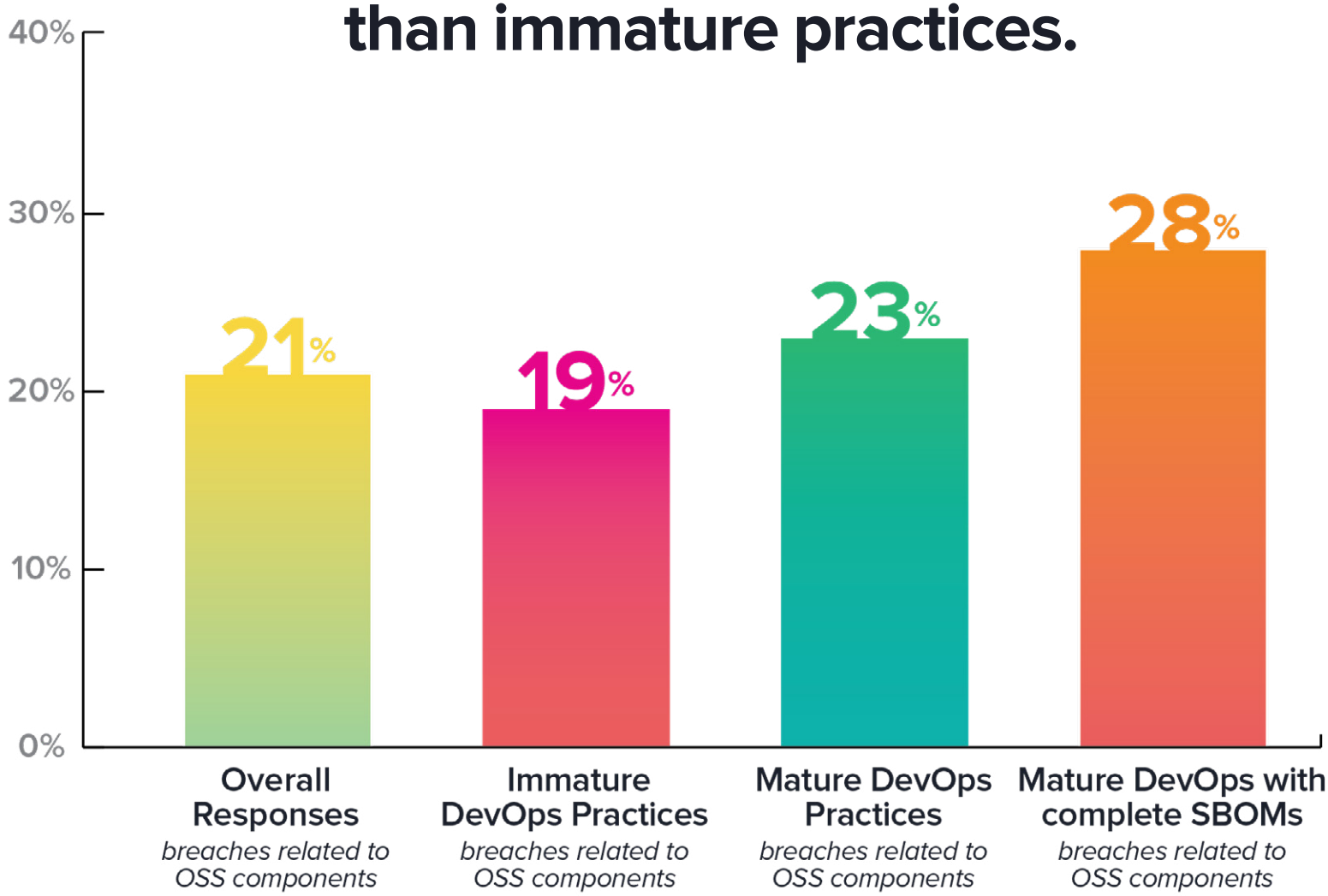
a breach in the last 12 months.

Open source component related breaches continue to drop, but still occur much too often.

A comparison of all survey responses 2017 – 2020



Mature DevOps practices are more aware of breaches than immature practices.



“The time between a vulnerability announcement and its exploits appearing in the wild is just three days, so being proactive is now a must.”

MITESH SHANBHAG, *Assistant Vice President, Nomura International PLC, UK*

Open Source Governance

Workarounds to policy are common, but hard to ignore when more automation is present.

As seen in the “Practices” chapter, open source governance is widely used by both mature and immature DevOps teams, but just because tools and policies exist, it doesn’t mean compliance is enforced.

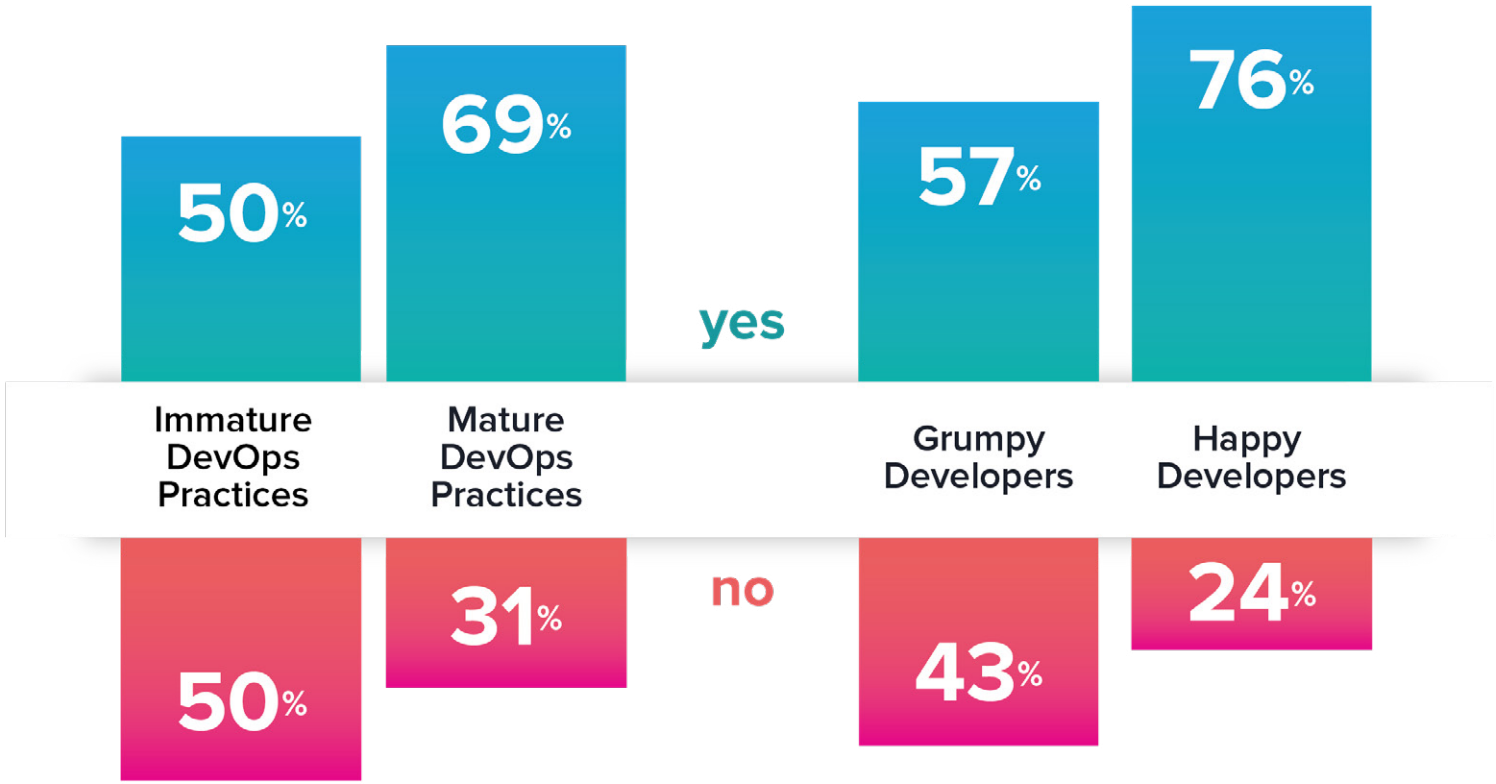
For the second year in a row, we have seen more developers following their open source governance processes in mature DevOps organizations. In mature DevOps practices, those who followed their open source governance policies jumped 6 percentage points since our 2019 survey to 68%. More impressively, those with no or immature DevOps practices saw a 25 percentage point increase to 50%.

Open source compliance is not tied to automation alone. Developer job satisfaction demonstrates a strong correlation to compliance. Happier developers were 1.3x more likely to follow their policies compared to grumpy developers.

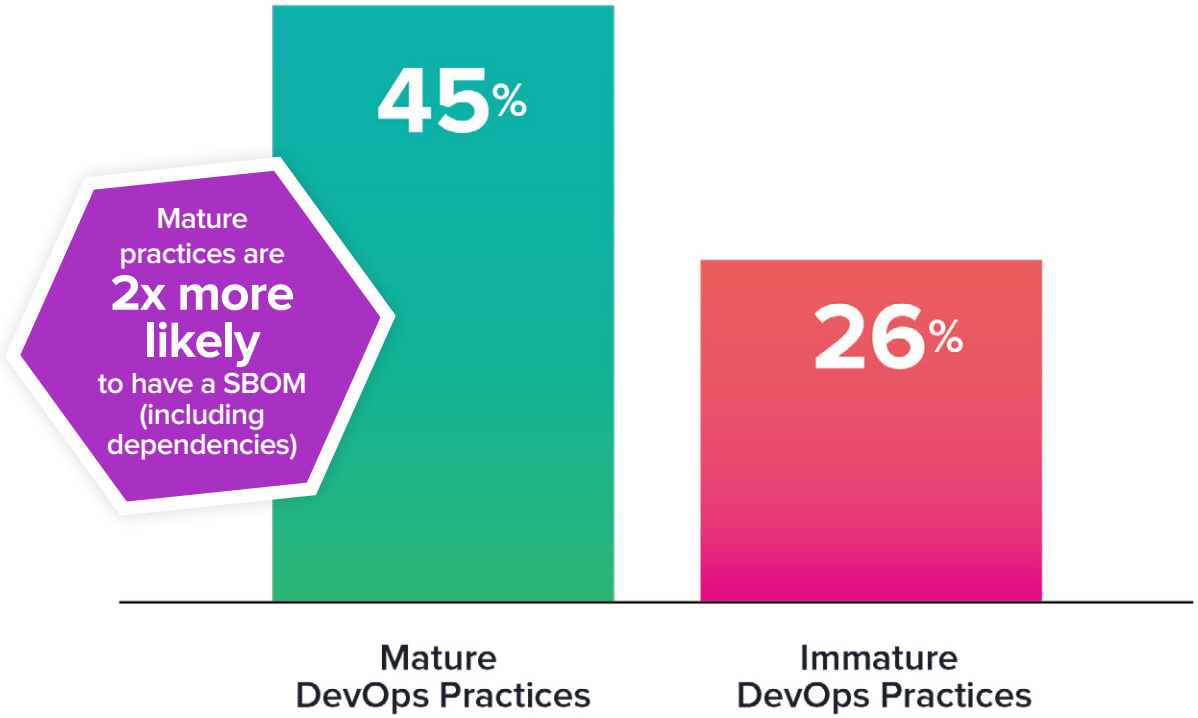
With 80 – 90% of an application code base assembled from open source components, it’s nice to see the growing interest and rigor around managing software supply chains.

Do you follow your open source governance policy?

Happy developers and mature DevOps practices are more likely to follow policies aimed at keeping code secure.



Do you keep a full Software Bill of Materials (SBOM) for open source components used in your applications?



44% of mature DevOps practices

integrated automated OSS Governance into their SDLC.

“

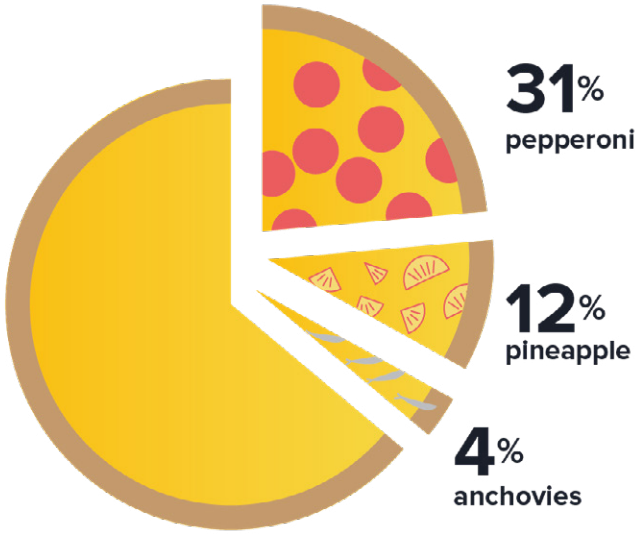
Doing less with more, doing it faster and more securely, and getting to only the essentials is a valiant goal. Who wouldn’t want to be a part of that?

”

THOMAS PORTER, *Aetna, United States*

Fun Facts

A little more about the survey participants...

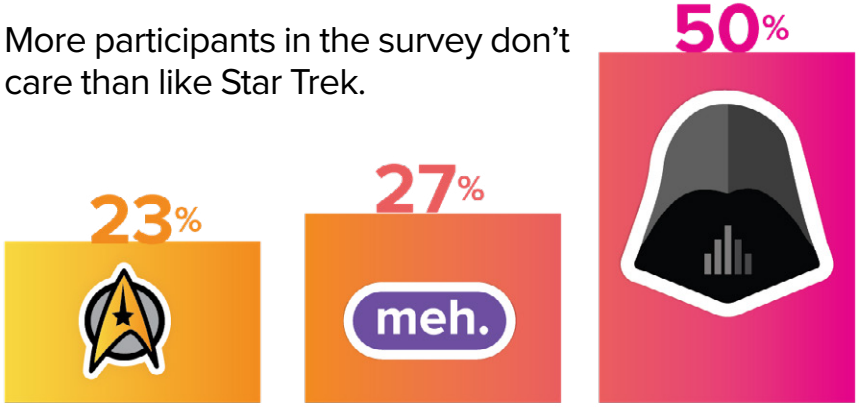


They like pepperoni.

Almost a third of participants said it was their favorite pizza topping.

The Force is strong.

More participants in the survey don't care than like Star Trek.



Captain Deadpool! No, just Deadpool.

Under duress, 100% of participants agreed that Deadpool is their favorite mercenary.

About This Survey

DevOps practices are growing. Release frequency is improving. Security culture is growing in development. And security practices are being built in. As a result, we're seeing more developers embrace security rather than push it away. Where they embrace security, happy developers thrive.

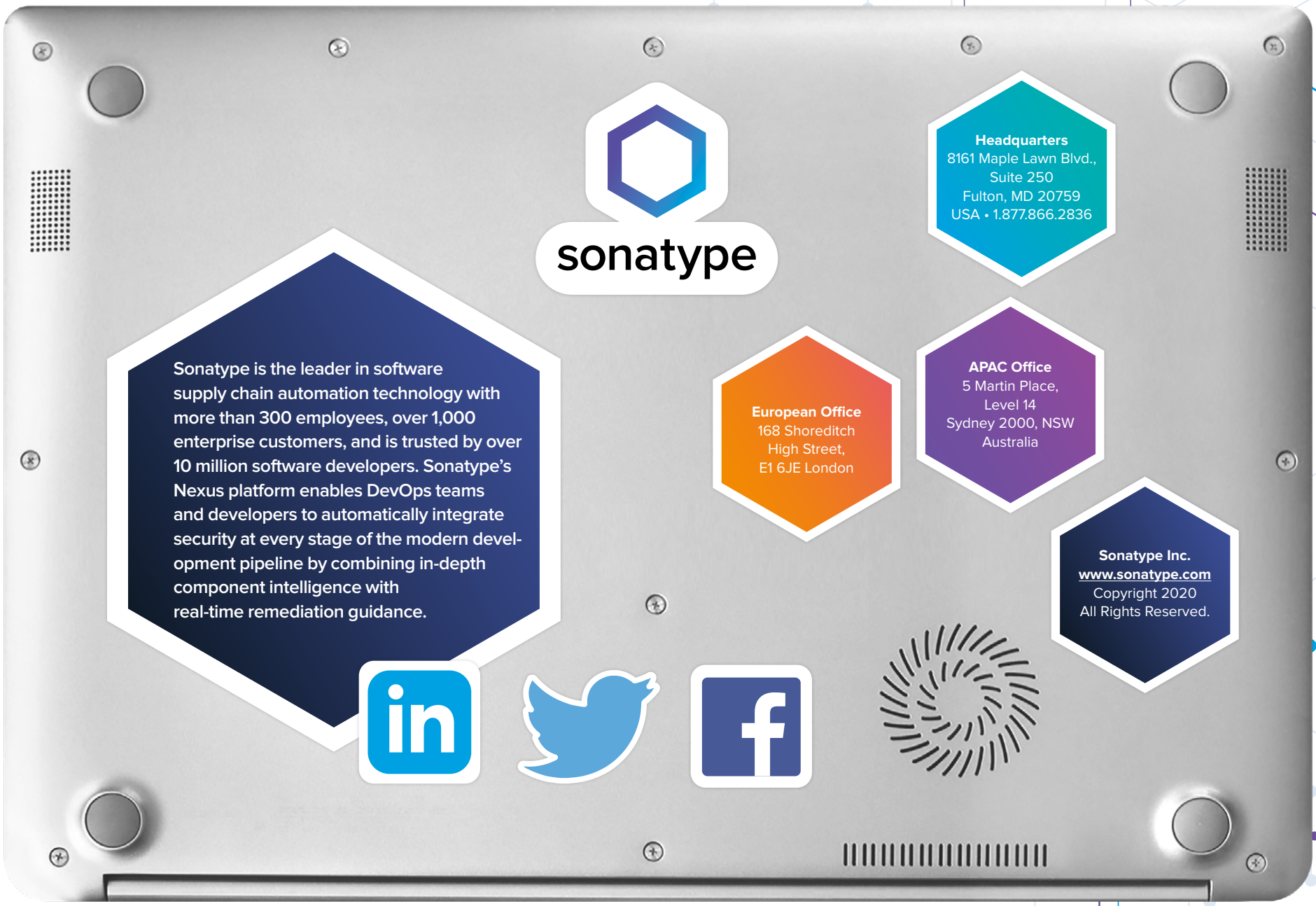
Over the years, we've analyzed our survey results to share better insights as to how organizations are adapting, what challenges they've overcome, and what approaches they are prioritizing. Share these results with your peers and use them to ignite conversations that continue to evolve and transform your own practices.

This is the seventh such survey conducted by Sonatype since 2014, focused on application development and security practices that have recently evolved into what we now call DevSecOps. The results reported in the survey came in response to 34 questions asked by Sonatype and our DevOps community advocates including DevOps Institute, NowSecure, DevOps.com, Security Boulevard, Verica, CloudBees, and Carnegie Mellon's Software Engineering Institute. The online survey was conducted between January 29, 2020 and February 27, 2020.

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, 5,045 IT professionals responded to the survey with 4,348 (79%) 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" or "Not sure" responses in the final results. To establish historical trends, some of the questions in our 2020 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. This year, we saw 47% of respondents live in North America, 25% live in Europe, 17% live in Asia, and the remainder of the people participated from other regions of the world. Overall, IT professionals from over 102 countries participated.

The survey's margin of error is ±1.226 percentage points for 5,045 IT professionals at the 95% confidence level.


sonatype
Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype's Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.
Headquarters
8161 Maple Lawn Blvd.,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836
European Office
168 Shoreditch
High Street,
E1 6JE London
APAC Office
5 Martin Place,
Level 14
Sydney 2000, NSW
Australia
Sonatype Inc.
www.sonatype.com
Copyright 2020
All Rights Reserved.