Checkmarx

REPORT

The Future of

APPLICATION SECURITY

The State of

Application Security

Application development has changed.

It has moved from waterfall development with infrequent releases, to agile development and continuous delivery. Software is deployed multiple times per day, development is complex, and it is increasingly cloud-native. This has dramatically changed how organizations need to secure their applications.

There is more software deployed in more environments, and less time available to secure it.

The responsibility has shifted away from dedicated security teams and is now shared between AppSec managers and developers. Trust between CISOs, development and security teams - called #DevSecTrust - is critical if the enterprise going to successfully reduce the business risk of vulnerable applications.

Building #DevSecTrust requires a holistic approach. CISOs must understand the issues facing their AppSec and development teams while trying to gain greater visibility over their enterprise's AppSec. AppSec tools must meet the needs of multiple stakeholders, and the rising influence of developers must be recognized if organizations are going to successfully continue to improve their application security posture.

The third annual Future of Application Security survey reveals how key stakeholders are responding to this challenge. We surveyed 1504 developers, CISOs, and AppSec managers from a broad range of industries across the US, Europe, and Asia-Pacific regions.

Discover the current state of application security and areas of future investment that will support #DevSecTrust. Learn how you compare to your peers on AppSec program measurement, the AppSec tools they are using right now, and where they plan to invest in future. Explore developer experience and influence, and the challenges and concerns around cloud deployments.

92%

of companies had a breach due to an application they developed

91%

of companies have knowingly released vulnerable applications

67%

of applications are currently hosted in the cloud

Key Findings

1 Organizations are knowingly releasing vulnerable applications

92% of the organizations surveyed have suffered a breach due to a vulnerability in an application they developed. Yet, 91% have knowingly deployed vulnerable applications. Business deadlines are cited as a main reason for deploying vulnerable code.

Main breach causes

1. Stolen credentials, secrets, or weak authentication
2. Cloud resource, IaC, or container misconfiguration
3. Known and/or unknown vulnerability in code released to production

2 #DevSecTrust is critical

Team alignment and trust are crucial for a successful AppSec program. Alignment and trust between CISOs, AppSec professionals, and developers is necessary to identify and address vulnerabilities that could impact the business. Yet, there are some differences between CISOs, AppSec managers, and developers. Developers and AppSec managers focus on the things that are in their immediate control, while CISOs seem to take a more holistic approach to AppSec.

3 Developer influence is rising, making developer experience more important

Developers are increasingly powerful decision-makers in the buying process. Developer experience is a crucial when considering in any AppSec solution, with vulnerability prioritization, secure code training, and seamless AppSec integration all key focus areas.

Developers' top three security concerns

1. Security impeding development process
2. Difficulty knowing what to fix and how to prioritize risk
3. Lack of context to remediate vulnerabilities

4 Investment plans focus on consolidation, simplification, and improving the developer experience

Consolidation helps build #DevSecTrust and improve developer experience. By consolidating multiple AST solutions onto a single AppSec platform, it's easier to correlate findings, triage results, integrate with developer tooling, onboard faster reducing the learning curve, and see all your risks and vulnerabilities in a single place.

5 Cloud presents a complex, high-priority risk

67% of applications are currently deployed in the cloud and CISOs say managing cloud risk is their top priority in the coming year. AppSec managers and CISOs are concerned about data governance, identity and access management, and software supply chain risks.

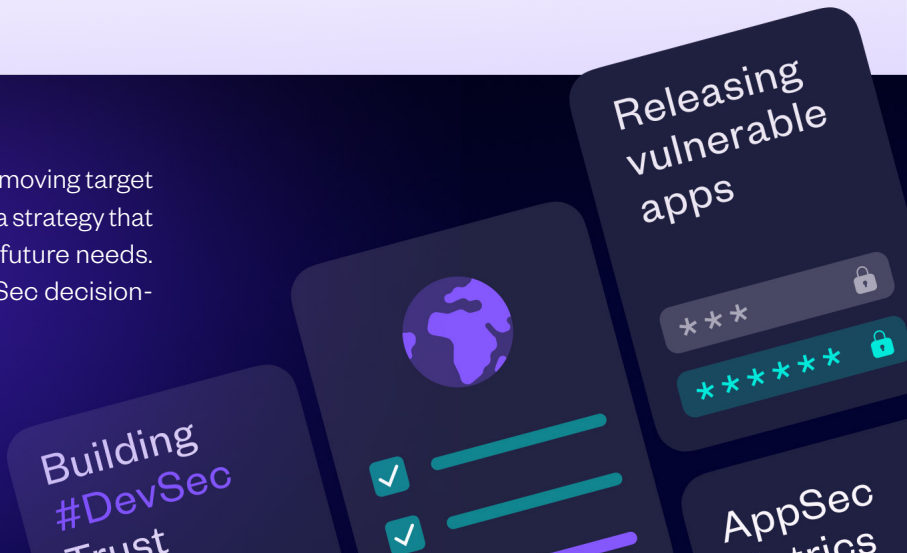
CISO priorities

1. Managing cloud risk
2. Managing AI risk
3. Increasing cyber transparency

67% of applications are currently deployed in the cloud

As the nature of applications changes, they are a moving target for AppSec programs. Organizations must devise a strategy that allows AppSec to evolve in parallel and predict future needs. To discover the full findings to inform your AppSec decision-making keep reading.

Keep reading to learn more!



Content

The State of Application Security

Known Vulnerabilities and Increasing Complexities are Driving More Breaches

Application risk is business risk. With digital transformation moving organizations' physical processes and in-person engagement online, it means that enterprises are now relying on applications more than ever. That dependency can become dangerous for businesses of all sizes when vulnerabilities enter the application landscape.

Our survey shows that business risk is rising: 92% of companies surveyed have experienced at least one security breach as the direct result of a vulnerable application they developed in the past 12 months. This is a slight increase from 88% who reported breaches last year. Concerningly, most companies have experienced more than one breach: 2.44 per organization.

92% of companies have experienced at least one security breach in the past 12 months

A Code to Cloud Approach Is a Must for Enterprises Today

The growing complexity of applications, paired with the increase in cloud-native development, has rapidly expanded the current attack surface for many enterprises. Because of this, we are seeing a shift to organizations looking to protect their entire software development lifecycle (SDLC), from the first line of code all the way to deployment and runtime in the cloud.

The increased attack surface is reflected in the range of factors that respondents said contributed to their breaches, including but not limited to: misconfigurations in cloud resources, Infrastructure as Code (IaC), containers, stolen credentials, weak authentication, and risks in software supply chains, including vulnerable APIs and open source components.

So, what does this mean? It highlights that breaches can happen anywhere across the SDLC. Modern application development requires a code to cloud approach in order to rise to the challenge of truly reducing business risk - especially when they are being developed with both custom and open source code.

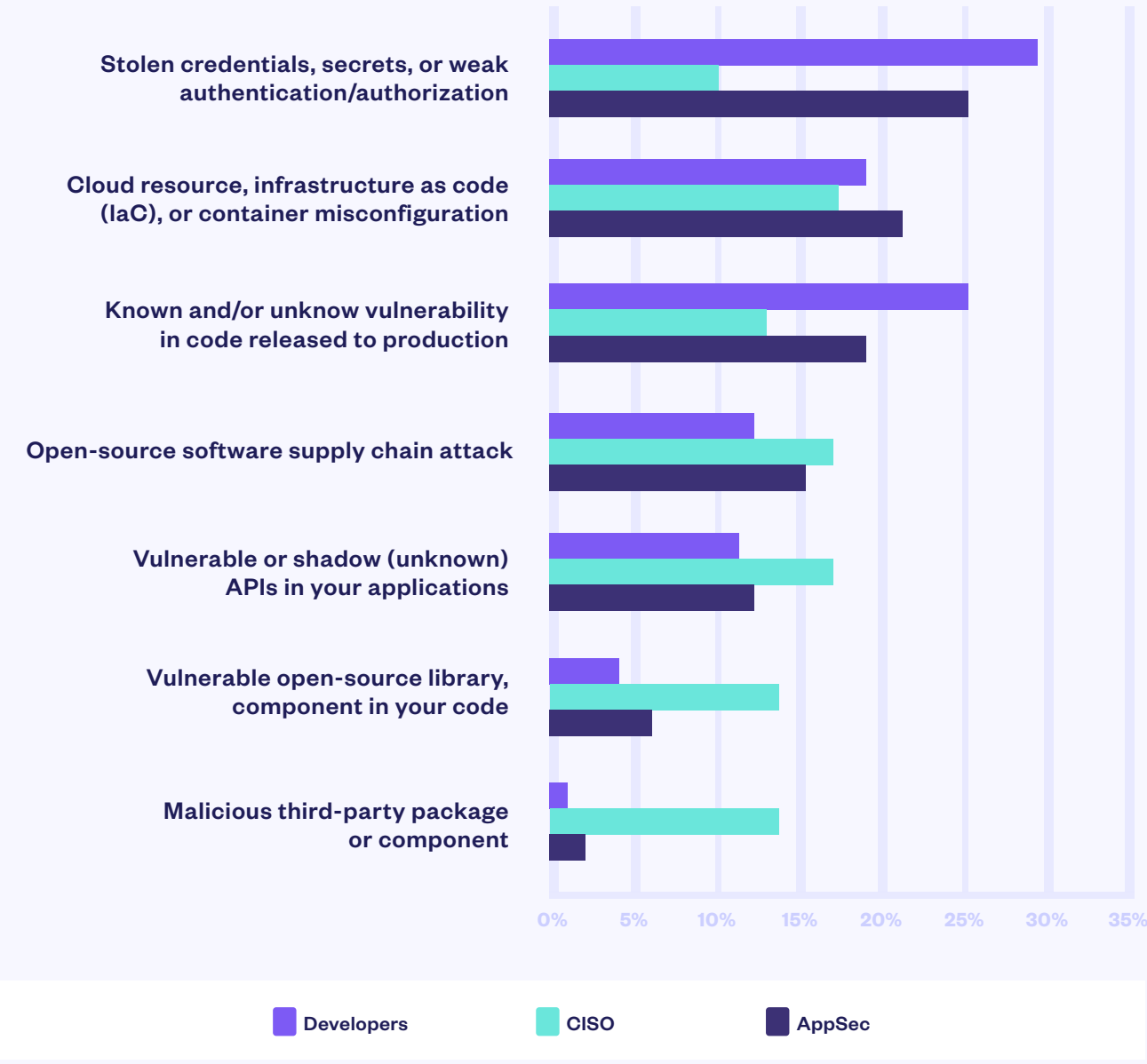
CISOs Have Their Eyes Set on the Future

When we talk about the current state of AppSec, we need to understand how our three stakeholders view AppSec today, and how that shapes their view of the future. Our respondents highlight these differences very clearly. CISOs often have their eyes set on the future – seeing the overarching picture of how AppSec goals fit into the overall business goals. AppSec managers and developers on the other hand, are very focused on the current state of things – looking directly at what they have and oversee now.

With clear communication between CISOs, AppSec managers and development teams, this can be a powerful combination. When a CISO can see the "big picture", they are able to offers AppSec and development a perspective they might not have considered, which then allows them to collectively create trust and efficiencies.

FIGURE 01

What was the main cause of your security breach?

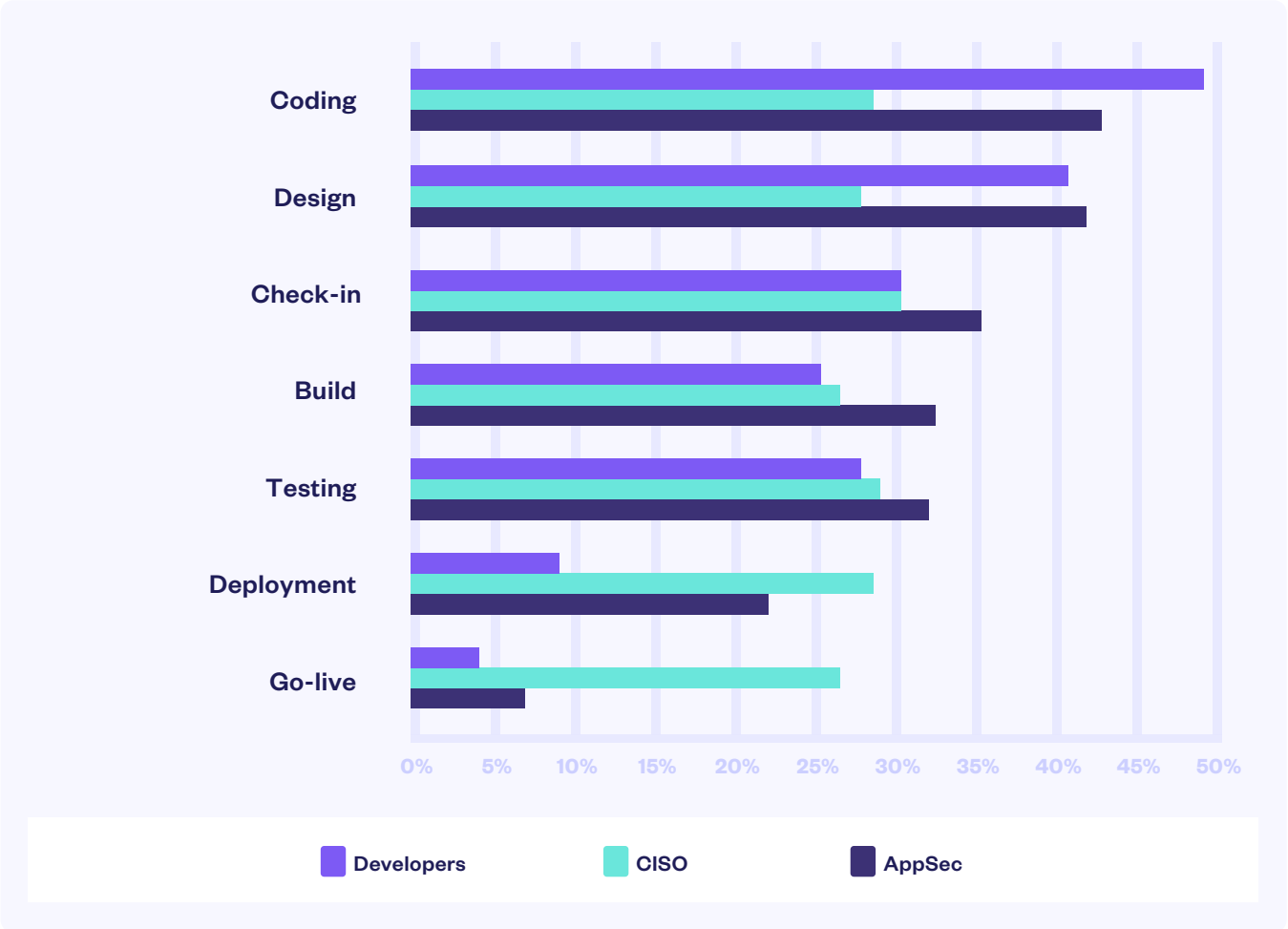


How Are Enterprises Tackling Application Security Today?

Modern application security is about finding and fixing risk across the entire software development lifecycle (SDLC). We asked respondents to tell us at what stage are of the SDLC they thinking about vulnerabilities (Figure 2).

FIGURE 02

During what stages of the SDLC do you scan for or find vulnerabilities? (Select up to three)



Developers have become adept at shifting left – we can see clearly in the data that they are still primarily thinking about vulnerabilities within the coding and design phases. AppSec managers seem to continue keeping their eyes out for vulnerabilities through the go live stage. However, CISOs seem to be embodying the code to cloud philosophy by thinking about risk throughout the entire SDLC.

When we talk about code to cloud, we are highlighting the importance of protecting your entire process.

If CISOs are thinking code to cloud, but developers are consistently only focusing within the "code" phase, how can we best work to close that gap?

This is why cloud-native AppSec matters – AppSec teams and development teams can use tools like runtime insights, and quickly find what needs to be fixed along the way, and before their application goes live.

What's in the AppSec Toolkit?

Most respondents already use, or plan to use, available AppSec solutions (Figure 3). Businesses are adopting the tools to secure their entire application development lifecycles.

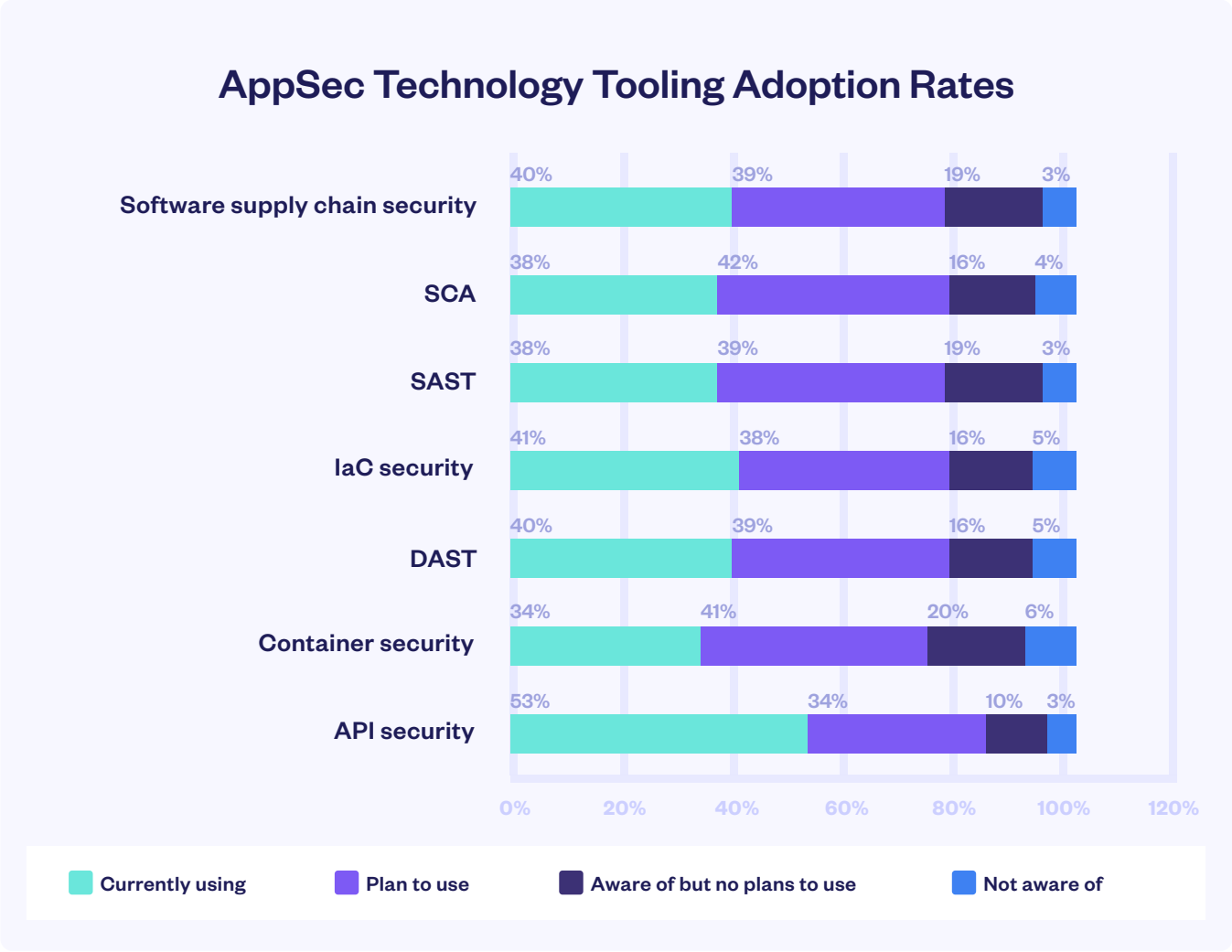
Organizations are using AppSec tools, however the tools that industry professionals assume that every organization has (like SAST) still aren't being used by a critical mass. Established tools, like SAST, DAST, and SCA still show significant potential for increased adoption – they are only in use by about 39% of respondents.

When it comes to code to cloud, there are a lot of different tools that need to be implemented, however, we cannot assume that every organization has mature tooling under their belts. It's important for organizations to take an honest look at the state of their AppSec maturity before buying separate tools that will inherently need internal buy in and support to use and maintain.

There is a lot of discussion around the ownership of AppSec tools, and it often centers around how it is ownership is shifting towards developers. While developers are increasingly being given more of a voice when it comes to purchasing decisions for AppSec tools, developers main concern will always be how they can develop applications. AppSec teams will always have the leading role when it comes to driving tool adoption, even if development teams are responsible for fixing the vulnerabilities.

FIGURE 03

Which of the following application security technologies/ approaches do you have or plan to have?



Measuring AppSec Programs

Alignment Is Key to AppSec Metrics

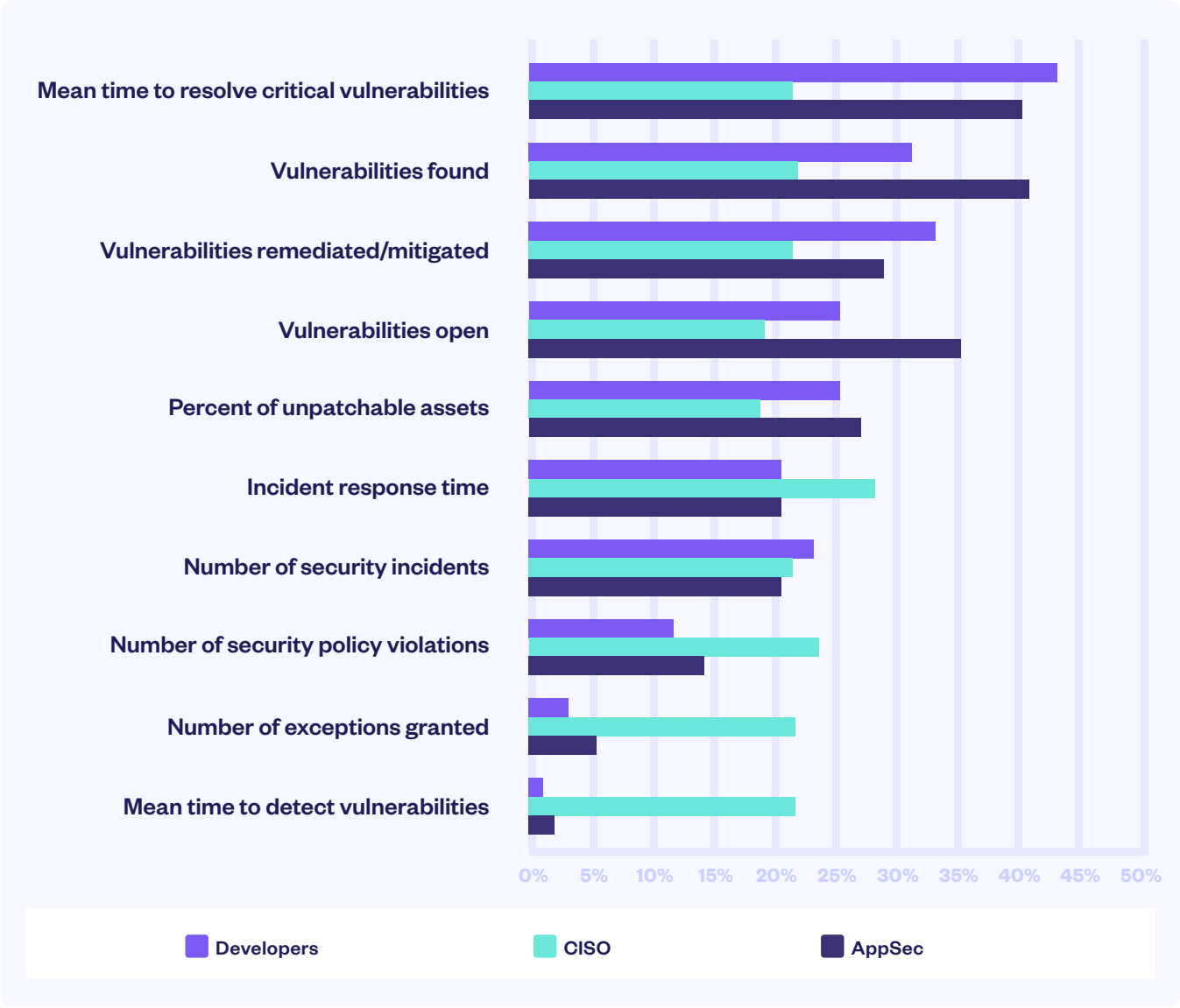
To build trust between your stakeholders, it's important that everyone is aligned to a shared set of goals and KPIs.

Unsurprisingly, AppSec and Developers report an equal focus metrics that center around vulnerabilities (Figure 4). Earlier, we talked about the fact that both teams are focused on what they currently in charge of, and that is reflected here. The industry has made progress in engaging developers in security, but there's more work ahead. With AppSec and Developer teams aligned, it's crucial to strengthen trust to meet their metrics effectively.

While CISOs continue to take an all-encompassing view when it comes to metrics, one thing is clear – finding and fixing seems to be what that all three stakeholders are aligned to.

FIGURE 04

What security metrics do you collect to show you have a successful AppSec program? (Select all that apply)



How Do You Make It Easier: Productivity Continues to Outweigh Security

What hinders vulnerability remediation? Simple – the fact that developers must stop what their primary job and goal is and find and fix a vulnerability before they can continue with their task. They are caught between the proverbial rock and a hard place. To meet the AppSec needs of their business, developers are often tasked with pressing pause on their productivity, moving to another system to scan, and then having to figure out how to fix any vulnerabilities before continuing through their development process. It's frustrating and a quick way to have trust break down between teams.

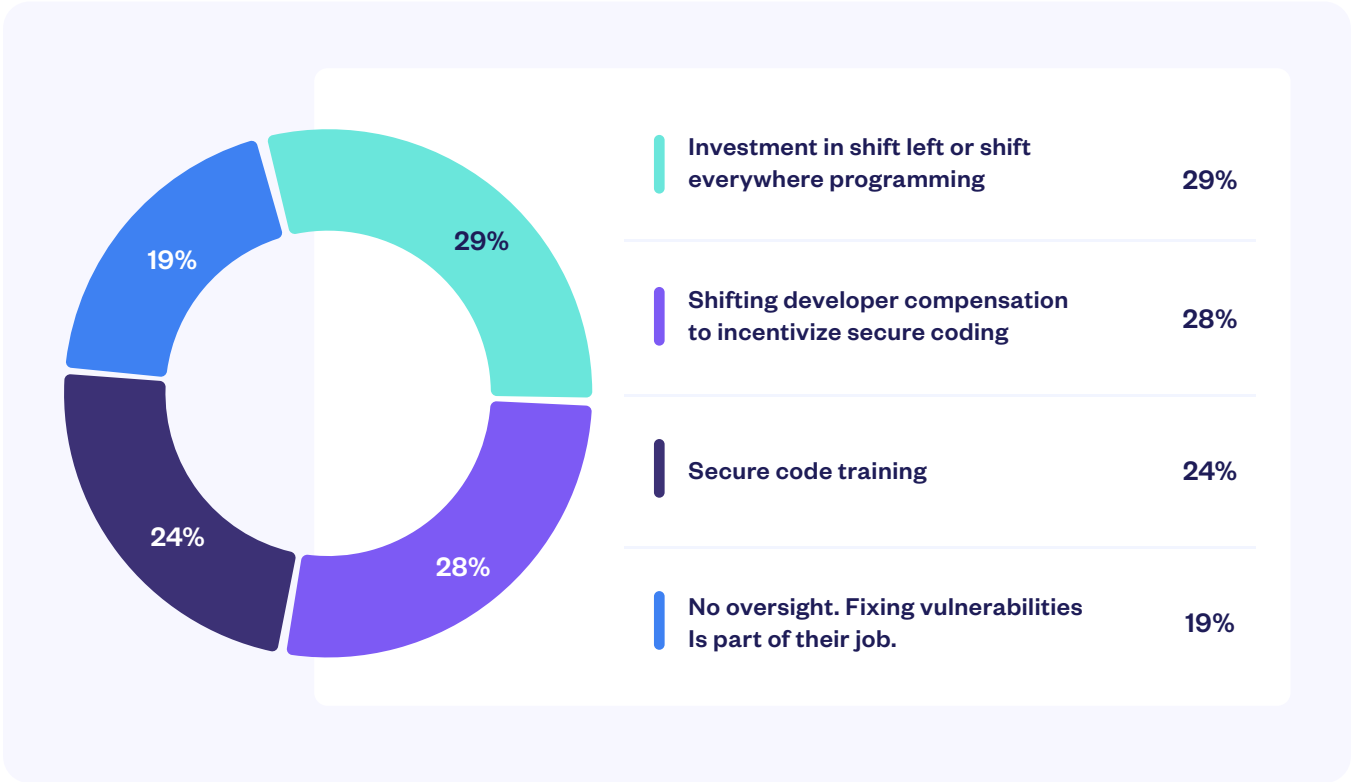
So, how are CISOs incentivizing developers to want to take a more security-focused approach to their development cycles?

The replies showed that CISOs are currently trying a little bit of everything, from offering secure code training to financial incentives (Figure 5).

Regardless of how CISOs are trying to engage developers in more secure development processes, developers are still predominantly measured on productivity, rather than security. Recent research published by Gartner echoed these results, reporting that software engineering staff were more than twice as likely to be measured on release frequency (62%) and speed of delivery (58%) than they were on the number of vulnerabilities remediated (28%) or the mean time to resolve and mitigate critical vulnerabilities (30%).

FIGURE 05

How do you ensure that your developers fix vulnerabilities in place? (CISO responses)



What Is Driving AppSec Success?

↘ Security Cannot Be a Barrier for Business Success

91% of organizations say they knowingly deploy vulnerable applications. We asked why (Figure 6).

Security knows that business is king. Business velocity rules when it comes to releasing applications. Meeting a business deadline is in the top three justifications for all three stakeholder groups.

This highlights that developers only have limited time to address vulnerabilities before demand from the business overtakes them; that time must be used wisely. To do this, security needs to be inserted seamlessly throughout the development process.

Security success cannot come at the expense of business success. Developers and AppSec teams need support when it comes to prioritizing what to fix first and remediation guidance so they can do it fast and effectively. CISOs are then tasked with finding the most efficient way to drive business forward, while also managing the risk that comes with modern day application development.

FIGURE 06

What were the top three primary reasons that vulnerable code was released to production?

	AppSec managers	CISOs	Developers
01	To meet a business, feature, or security-related deadline 29%	Hoped the vulnerability would not be exploitable 18%	Vulnerability would be fixed in a later release 29%
02	Vulnerability would be fixed in a later release 27%	To meet a business, feature, or security-related deadline 18%	Vulnerability was not critical 25%
03	Vulnerability was not critical 19%	Vulnerability was not exploitable 14%	To meet a business, feature, or security-related deadline 21%

Building #DevSecTrust Between Security and Development Teams

Trust between CISOs, AppSec managers, and developers is critical since the balance of leadership and influence has changed. Historically, AppSec managers prescribed the security rules and tools for developers to use. Now, developers have much more responsibility and influence over buying decisions.

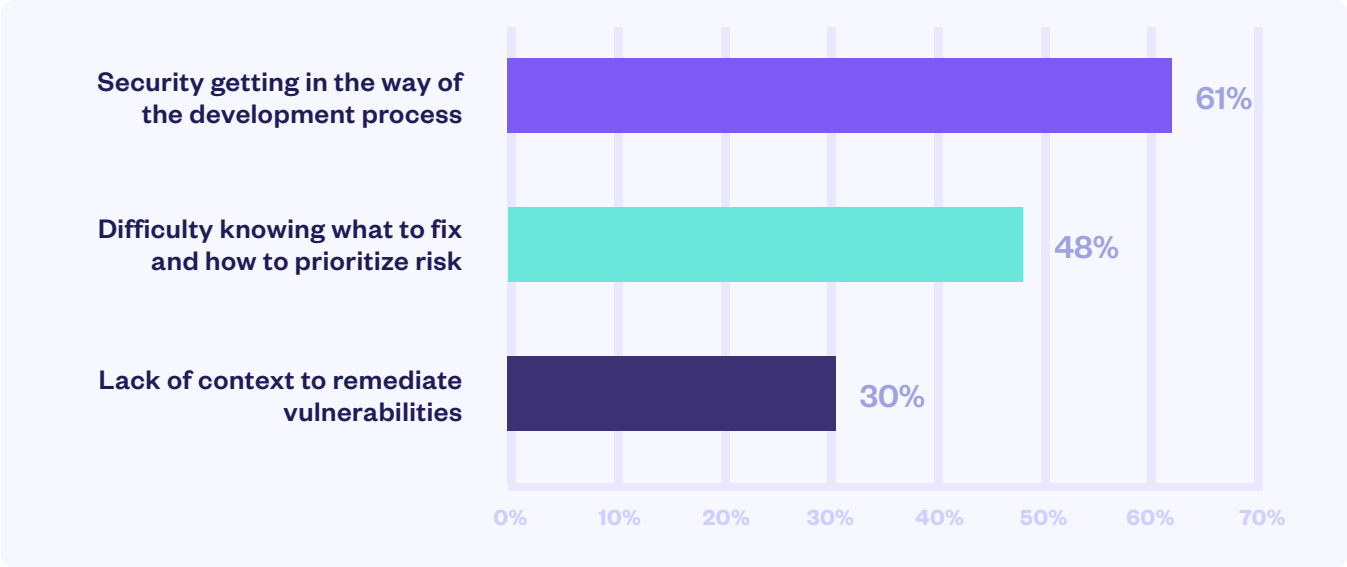
Developer experience is critical. If the AppSec program is a barrier to meeting developers' deadlines, the organization won't achieve its goals. The three stakeholder groups have an interdependent relationship. Therefore, it is important that trust is built between security and development teams.

We asked developers questions that explore their challenges, concerns, and preferences around enterprise AppSec programs.

Their responses show a gap between what they'd like and what they currently experience (Figure 7). They are worried about productivity being compromised by security, and struggle to prioritize what to fix first, as we touched on earlier. These problems might be addressed if developers received timely, trustworthy data from AppSec tools, in their IDEs and development environments, guiding them to the most important vulnerabilities.

FIGURE 07

What are your biggest concerns around developing secure code? (Select up to two)



How Do We Make AppSec Easier for Developers?

Developers want AppSec solutions that let them do their job. They want to see scan results directly in their IDE and don't want to switch to tools outside of their development workflow (Figure 8).

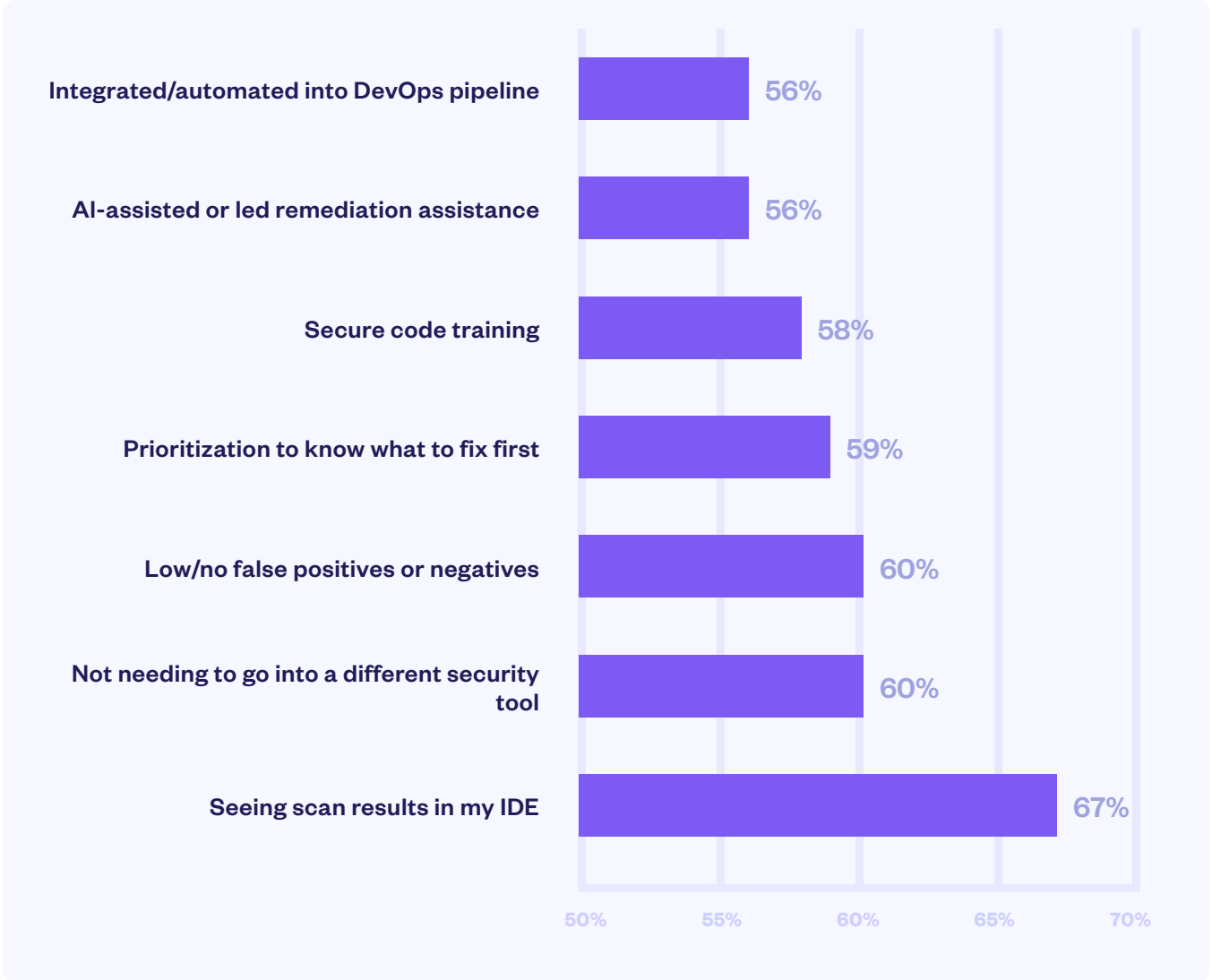
Let's take a moment to think about how developers work. They typically have their preferred systems that they work within, and so it's no surprise that they would prefer to work out of that one single space. 67% of developers want to see scan results directly into their IDE of choice – giving them the ability to figure out what they need to prioritize quickly, without leaving their development environment.

Developers don't want to hop from tool to tool – they want one tool that fits seamlessly within their existing workflow.

If CISOs and AppSec teams want to get developers on board with prioritizing security, that's where they should focus their efforts. This is even more important as we shift our sights to cloud-native application development. With the risk surface continuing to grow by using open source code in cloud-native application development, it's important to remember that developers are critical in remediating all potentially business-critical vulnerabilities. Supporting their ability to do their job efficiently will only help your organizations overall AppSec posture.

FIGURE 08

How important are the following items in your AppSec solution? (Developer responses)



Gaps in Secure Code Training Affect Developer Experience

Poor developer experience is compounded by a lack of training. However, there is a conundrum: your developers don't currently have training, and you want to make sure they receive it. However, even if you give them training today, it is not immediately impactful.

So, how do you give your development team security training in a way that allows them to utilize it sooner rather than later? Only half of developers say that they have access to formal security training, and just slightly more (55%) are provided with tools that offer security guidance within their IDE (Figure 9).

Guidance directly within the IDE is extremely helpful for those developers who don't have any training. Since we know that developers already prefer to stay within their IDEs, incorporating guidance within their preferred environment can result in an immediate impact on developers security knowledge. Meeting developers where they are is an important part of improving your developer experience, and is a critical pillar when thinking about developing #DevSecTrust.

FIGURE 9

Do you have a program or tools in place to train your developers in writing more secure code? If so, what? (Select all that apply)

The Future of AppSec

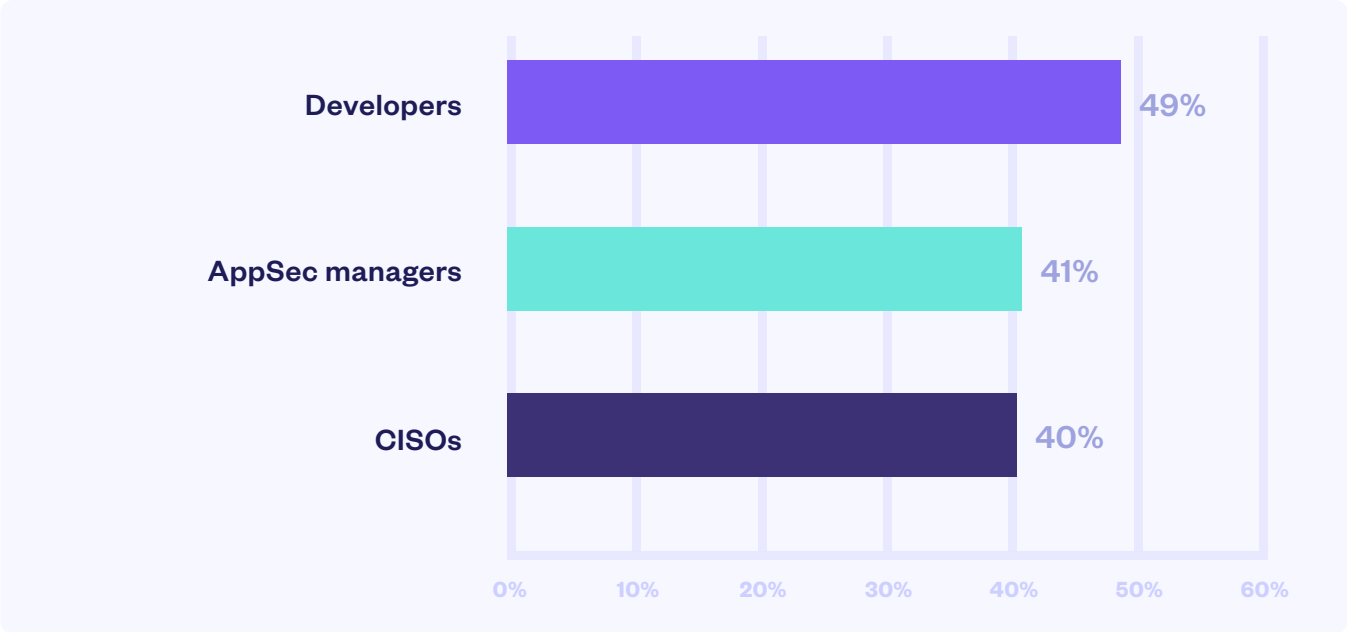
↘ Who Influences AppSec Tool Selection?

AppSec was previously viewed as the sole responsibility of the security team. Today, it's clear that there is a true buyer committee when it comes to organization's security investments.

Why? The "find and fix" goal is the reason why organizations seem to be shifting to a committee-based decision.

FIGURE 10

Which departments are involved in the purchasing of key applications security solutions? (All "decision maker" responses)



Respondents could select multiple decision makers:

- 50% of developers nominated themselves as key decision-makers.
- AppSec managers are more likely to say that developers are key decision-makers (63%) than themselves (57%).
- CISOs were mostly likely to list their own role as key decision-maker, followed by AppSec managers.

For the foreseeable future, AppSec managers will continue to be the ones who make the purchase. However, they will need significant buy-in from the development teams because if the developers won't use the AppSec tool, then all is for naught.

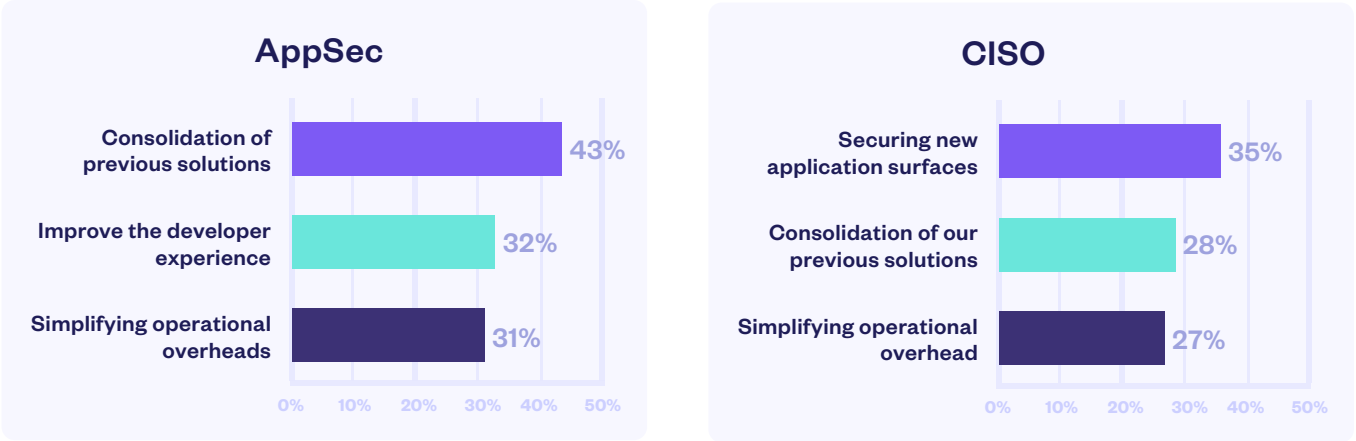
The real question that AppSec managers must consider when making their purchase is: "What do your CISOs, and developers actually care about?"

What Factors Influence AppSec Tool Selection?

Every stakeholder has slightly different motivations for looking into, and purchasing, certain AppSec tools. We asked respondents the top three reasons for choosing or recommending their most recent AppSec solution (Figure 11).

FIGURE 11

What are the top reasons for choosing or recommending your most recent AppSec solutions? (AppSec and CISO responses)



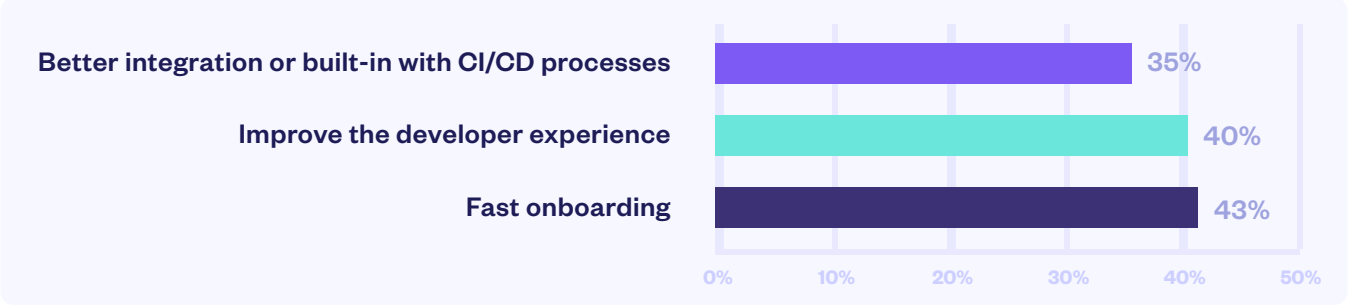
Consolidation is a priority for both AppSec managers and CISOs, and that comes as no surprise.

With breaches rising and application development becoming increasingly complex, organizations are scanning at multiple points across the SDLC (see Figure 3 on p. 9). The result? Companies purchase many different tools to cover different security requirements (see Figure 4 on p. 10). This is not ideal for developers, who want AppSec tools that show them results directly in their IDE and not log in to a separate security tool (Figure 9 on p. 15).

All of these issues can be addressed by consolidating multiple tools into a single platform. Consolidation allows security tools and strategies to be streamlined for stronger, more coherent defense. It reduces overlaps for developers, assists with compliance, and cuts costs. A unified and consolidated approach aligns team efforts with key vulnerabilities and reinforces the overall security framework. In addition, when you allow all three stakeholders to utilize the specific tools they need and allow for cross-team transparency.

FIGURE 12

What are the top reasons for choosing or recommending your most recent AppSec solutions? (Developer responses)

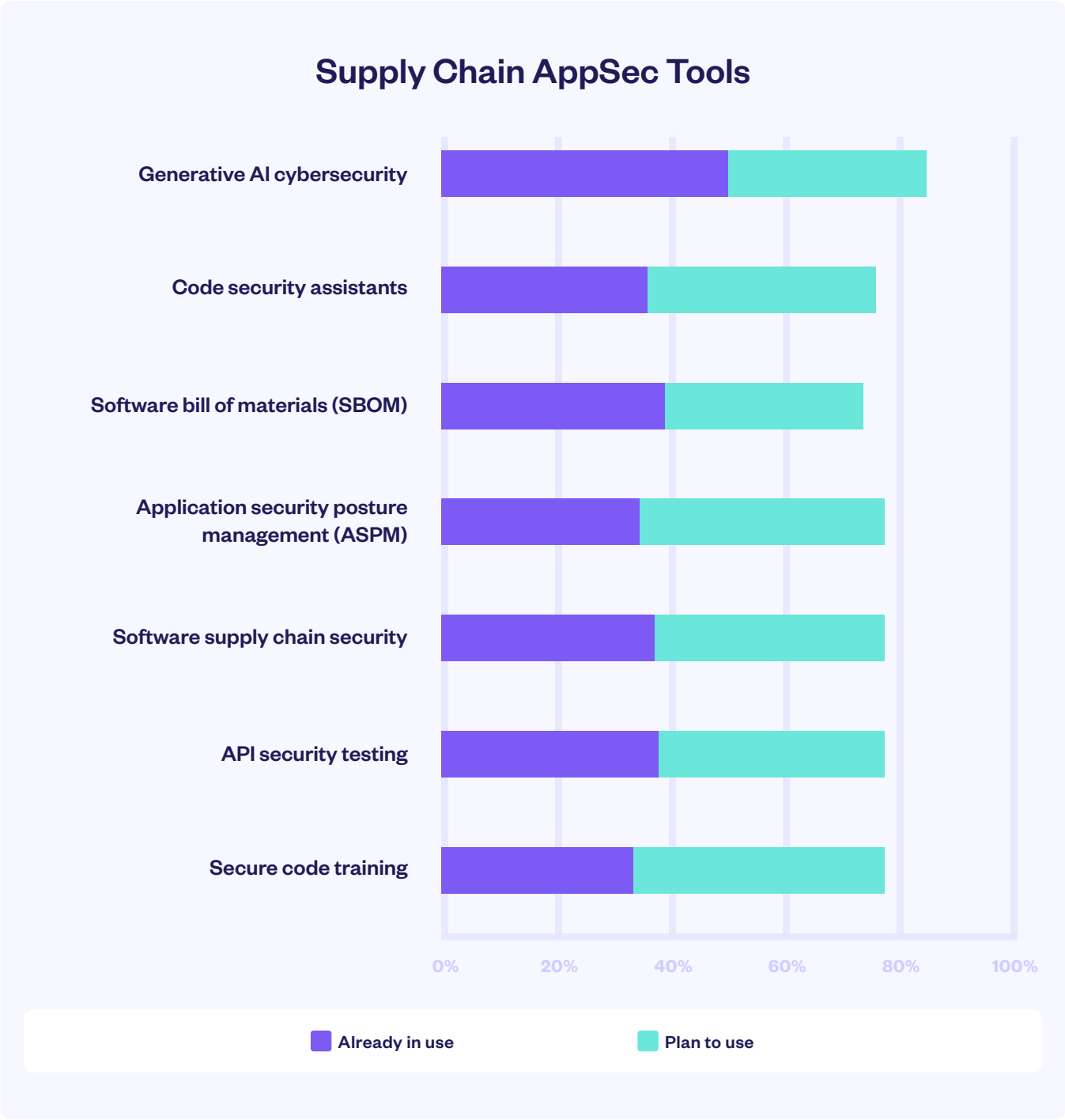


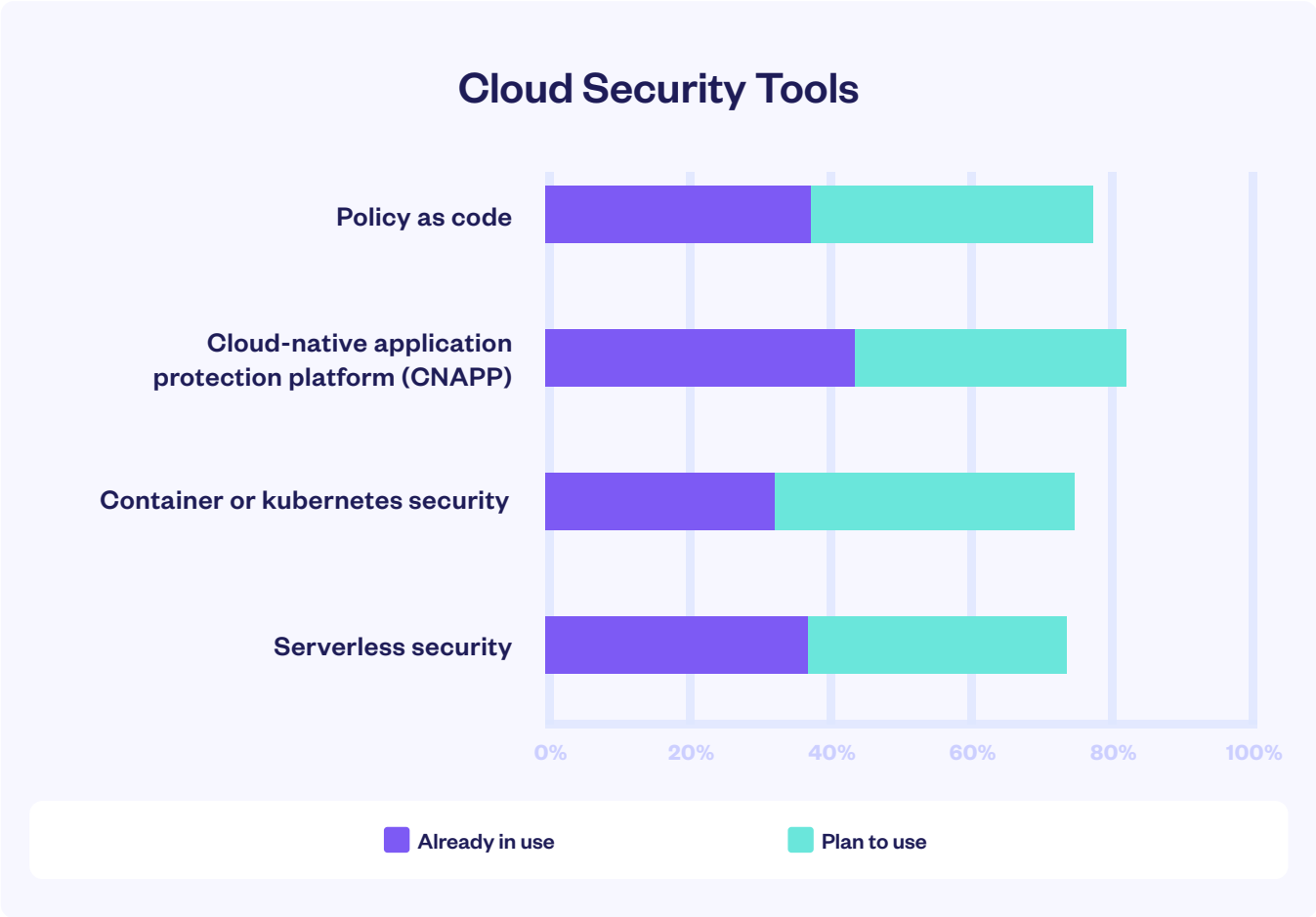
Future AppSec Investment

As application development grows more complex, new technologies are emerging to help developers, improve compliance, and enhance security programs. We asked respondents what new technologies they are using, or plan to use, in the coming year (Figure 13).

FIGURE 13

Which of the following technologies do you use or plan to use in the next 2-3 years? (All responses)





What is the future of AppSec? That depends on who you are, and what your organizations goals are. Companies are at different places with their AppSec based on industry. So, as you start making AppSec investments, there are many use-case specific tools to consider. Checkmarx's AppSec Program Methodology & Assessment (APMA) digital offering is a great resource in understanding your AppSec program's maturity and what steps you can take to improve your security posture.

Our survey shows that AppSec tools are a key feature in organizations' future investment plans. When we look at the variety of tools that are in the "plan to use" phase, we must take a moment to consider how we can consolidate on a single platform, to make sure that all stakeholders get what they need out of each piece.

The future of AppSec no longer relies on cumbersome individual point solutions that difficult to manage – it relies on simplifying processes and finding efficiencies between tools and teams.

Earlier, we talked to the fact that legacy tools were not as widely adopted as we might believe. The current adoption rate for new technologies (Figure 13) matches the adoption rate of legacy tools at under 40%. This might be a symptom of a few things: tool sprawl, lack of AppSec program maturity, under developed #DevSecTrust, or even misguided buying decisions.

At the end of the day, every organization should be able to take an honest look at their AppSec program, set goals, and then make the proper decisions to help meet and exceed those goals.

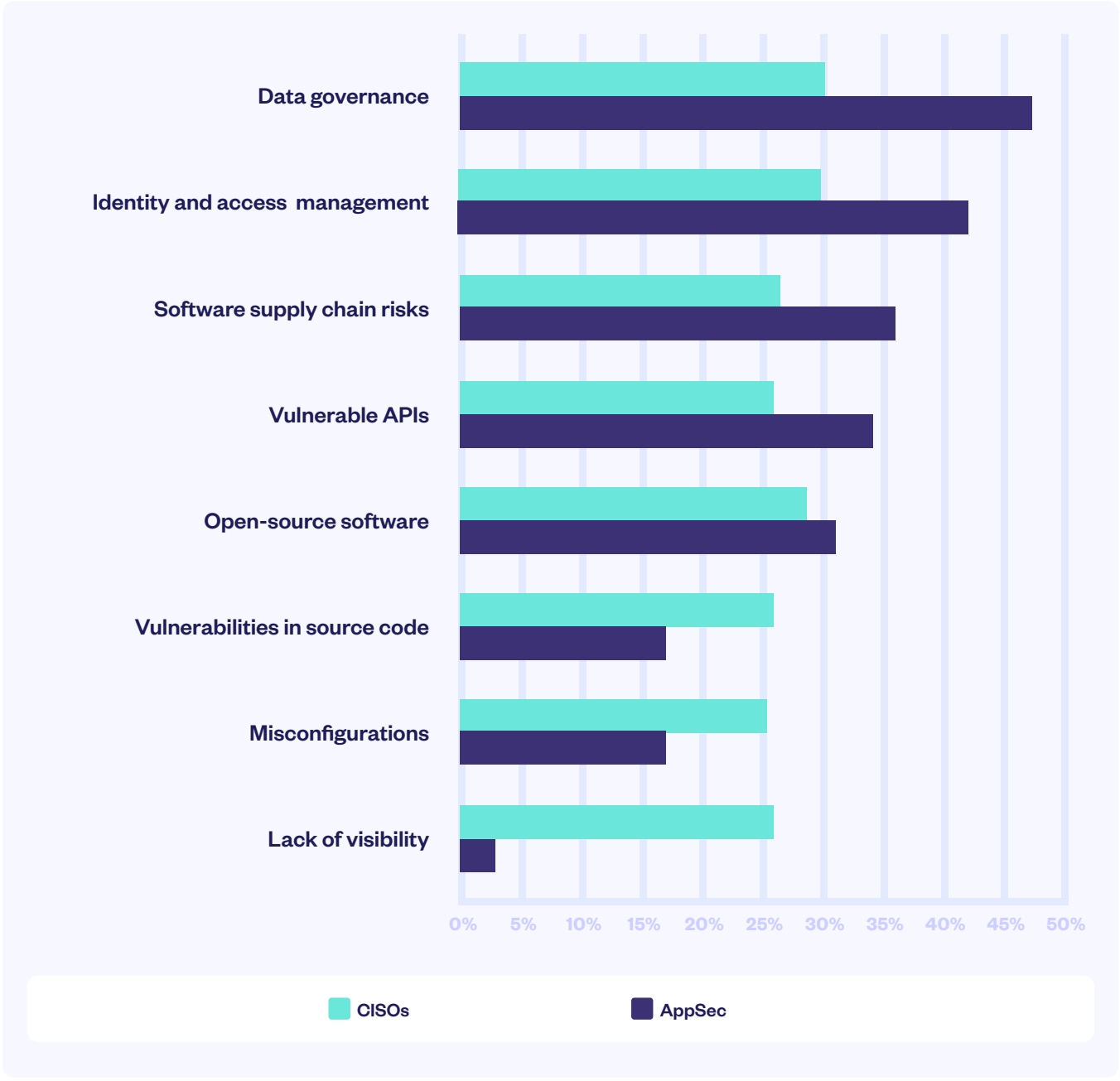
Cloud Deployment Dominates, but Concerns Remain

Cloud-native applications require different things, and they require them across the entire SDLC. As enterprises invest in a code to cloud approach to AppSec, they are also moving their focus to the later stages of the development lifecycle.

Our survey found that 67% of applications are currently deployed in the cloud. It is not surprising that the CISOs we surveyed also said that maintaining and managing cloud risk is one of their top priorities for the year ahead.

FIGURE 14

When it comes to applications deployed in the cloud, what are your biggest security concerns? (Select up to three)



As organizations invest in the code-to-cloud philosophy they must adapt their AppSec accordingly. Key concerns about cloud deployment vary between AppSec managers and CISOs, with CISOs again showing their more holistic approach (Figure 14).

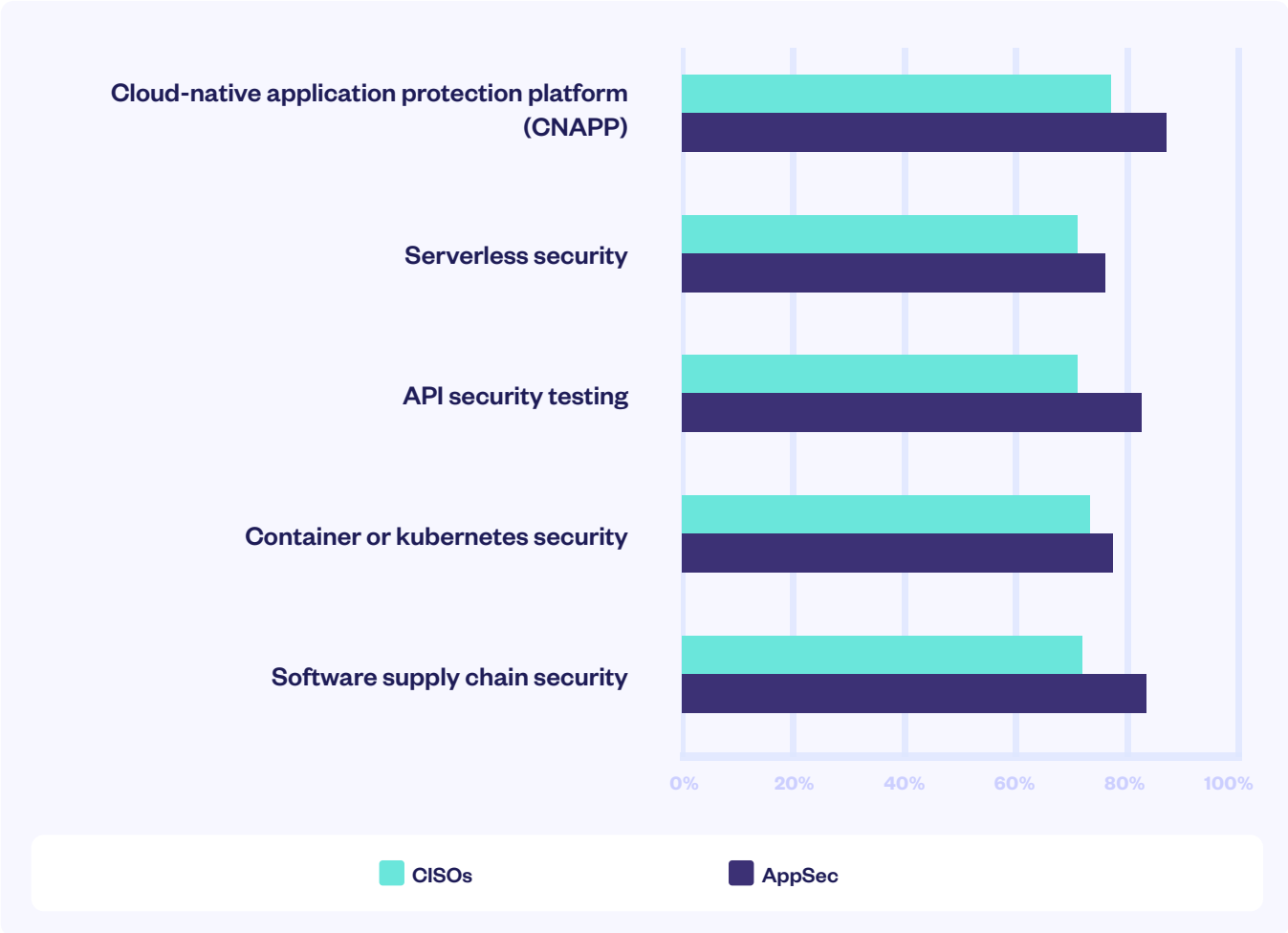
To address these concerns, organizations are deploying cloud security approaches. More than 70% are using, or planning to use, cloud-related security tools (Figure 15), with AppSec managers more likely to say these are already in use.

As AppSec programs become more complex, consolidating all their AppSec tools into one central platform will be critical for success.

It's important to remember that stakeholders, especially CISOs, are constantly thinking about securing their applications from code to cloud. We expect a greater focus on cloud-native application security that is focused on bringing AppSec directly to cloud-native applications, while also still securing the rest of the application footprint.

FIGURE 15

Which of the following technologies do you use or plan to use in the next 2-3 years? (Using or planning to use responses)



Conclusion

Breaches and the deployment of vulnerable applications reflect unmanaged application risk in organizations and the deadline pressure on AppSec managers and developers.

Overcoming this requires key stakeholders to become better aligned and more aware of each other's needs and priorities. CISOs should explore what AppSec managers and developers need to carry out their work effectively.

Build #DevSecTrust

Creating #DevSecTrust means achieving organizational alignment across your entire organization, breaking down siloes and ensuring transparency, including a shared set of KPIs, between CISOs, AppSec, and developers.

Focus on developer experience

Improving the developer experience will improve AppSec posture. Look for solutions that let enterprises prioritize results for the greatest business impact, meet developers where they work, and equip developers with the tools and knowledge to build secure applications.

Prepare for cloud-native application security

Applications are moving to the cloud. This introduces new risk and increases pressure on developers. Ensure that your application security program secures applications from code to cloud.

Take a holistic platform approach to AppSec investment

When planning AppSec investment, seek opportunities to consolidate existing tooling and introduce multifunctional platforms that meet current and future AppSec needs for all the key stakeholders.

Methodology

Checkmarx commissioned Censuswide to conduct a survey among 1504 developers, CISOs and AppSec managers in companies from 1000-10,000+ employees from North America, Europe and Asia-Pacific. The survey took place in December 2023.

Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.

Checkmarx

Checkmarx helps the world's largest enterprises get ahead of application risk without slowing down development. We end the guesswork by identifying the most critical issues to fix and give AppSec the tools they need, all while letting developers work the way they want. From DevSecOps to developer experience, security and development teams can now work better together. That's why 1700+ customers rely on Checkmarx to scan over 1 trillion lines of code annually, improve developer productivity by 50%, and deliver 2X AppSec ROI.

Checkmarx. Always Ready To Run.