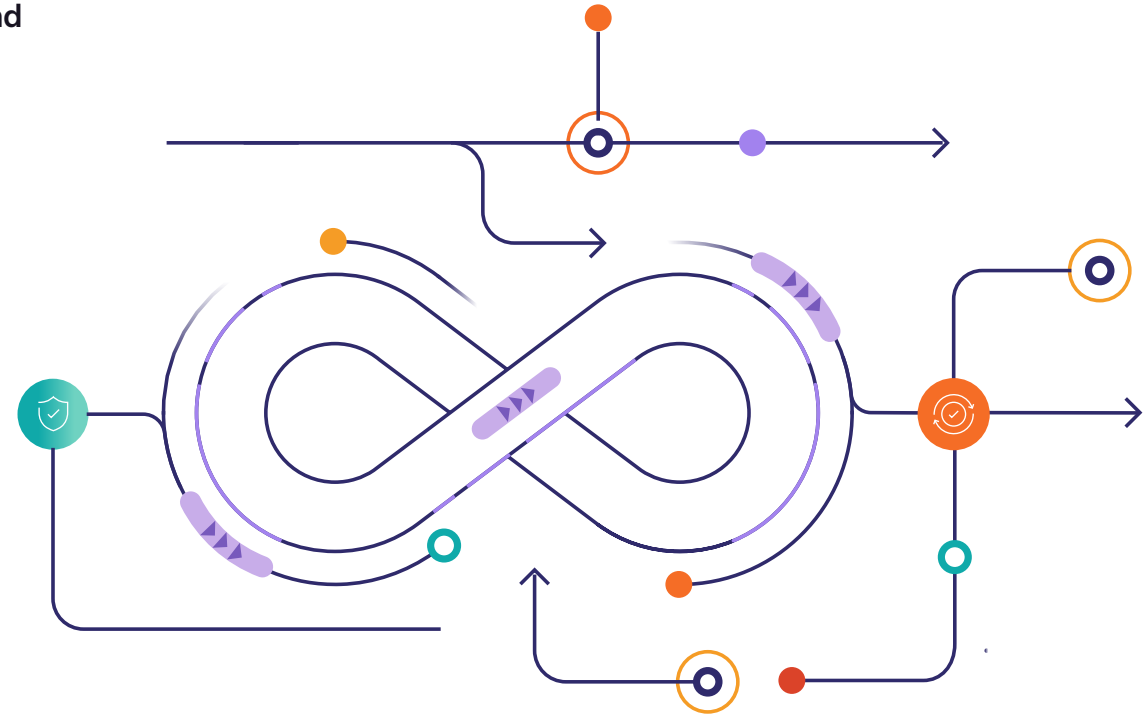
GitLab

2024 Global DevSecOps Report

Application security in the digital age

As software development booms, organizations are grappling with increasing attack surfaces and uncertainties around AI. Here's what we found in our survey of over 5,000 DevSecOps professionals worldwide.

Table of contents

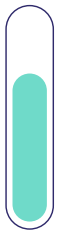


Executive summary

This report analyzes the results of a survey conducted by Omdia and GitLab in April 2024, in which we asked over 5,000 software development, security, and operations professionals worldwide about their organization's position on and adoption of DevSecOps principles and practices.

This year's survey reveals a perfect storm for security vulnerabilities: organizations are feeling more pressure to deliver software faster than ever before, so they're turning to artificial intelligence (AI) and open source libraries to accelerate development — and that, in turn, is increasing the attack surface and introducing new concerns around the security and privacy of AI tools. But our findings also highlight how organizations are getting the best of both worlds by establishing strategic application security programs that enable teams to move faster without sacrificing security.

Organizations are releasing software faster than ever



66%

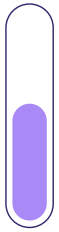
of respondents said their organizations are releasing software 2x as fast or faster than last year

Developers are increasingly relying on open source

67%

of developers said more than a quarter of the code they work on is from open source libraries — but only 1 in 5 of organizations are currently using a software bill of materials (SBOM) to document the ingredients that make up their software components

AI promises faster code — but organizations worry about security



55%

of respondents said that introducing AI into the software development lifecycle is risky; the top concerns are privacy and data security

Organizations are doubling down on application security scanning

34%

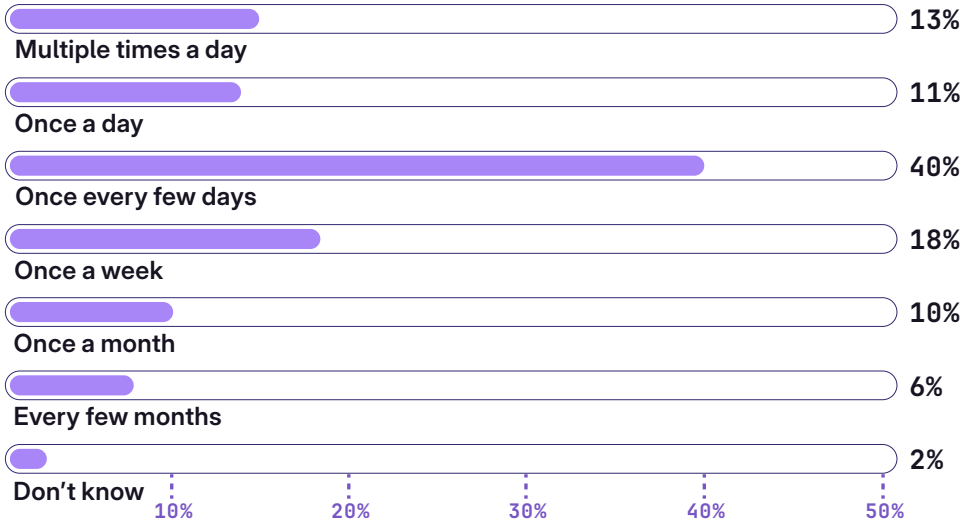
of respondents said their organizations have implemented dynamic application security testing (DAST), an 8% increase from 2023

The application development boom

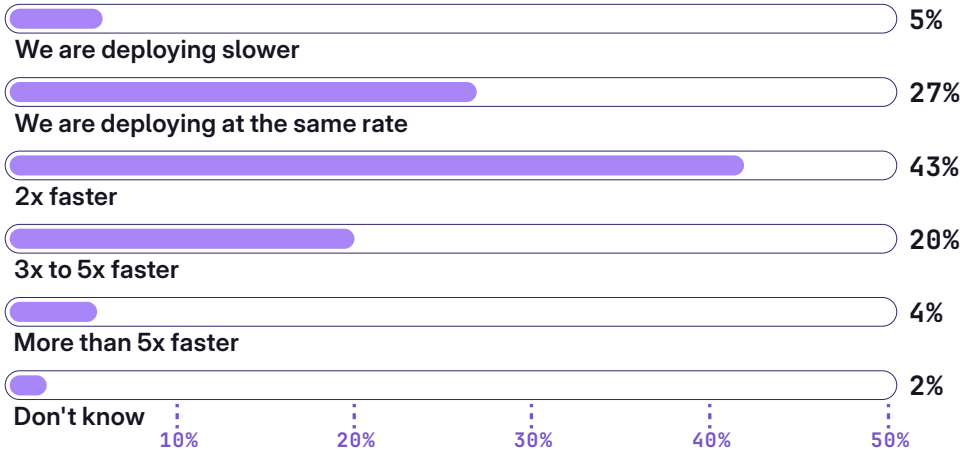
For large and small organizations in almost every vertical, the application development function has now moved front and center for business enablement and competitive differentiation. The findings from our survey underpin the assertion that software development is now critical to nearly every business: 69% of C-level respondents said that they currently monetize software as part of their business, while 77% said their business relies on software that they have developed, customized, or are maintaining internally for operations.

Competitive pressure in the commercial space and the need for better public services in the governmental domain is pushing organizations to focus more on developing their own applications — and to do so at an ever-increasing pace. A need for speed was a theme in our findings, with a quarter of developers indicating that they push code to production at least once a day and another 40% doing so once every few days. In addition, 66% of respondents told us they are releasing software at least twice as fast as one year ago, and 24% said they had sped up the process threefold or more.

Frequency of deployment to production, according to developers



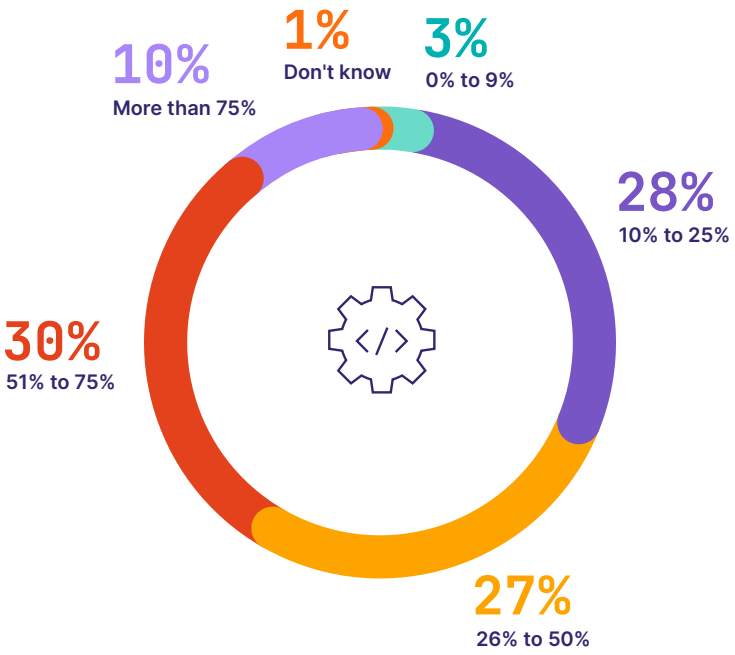
How fast is your organization currently releasing software, compared to one year ago?



The rise of open source

One way developers are keeping up with the increased demand to build software faster is to draw from open source libraries. The practice of building with open source software (OSS) is already widespread. In our survey, 67% of developers said more than a quarter of the code they work on is from OSS libraries, and 40% of developers said that OSS components represent over half of their application code. However, only 21% of respondents indicated that their organizations currently use software bill of materials (SBOM) generation to enable security in the software development lifecycle, representing a significant attack surface that must be addressed in the future.

Percentage of code from OSS libraries, according to developers



Building with open source helps organizations build and release software faster. However, because OSS is frequently a community effort, it often lacks the accountability of commercially published software. That means vulnerabilities may be introduced and persist through several software versions, with no authoritative source to alert developers to that fact before they download them. As a result, it is essential for organizations to be aware of the makeup of the software that they are producing, and to implement strategies to ensure that vulnerabilities are detected as early in the development process as possible.

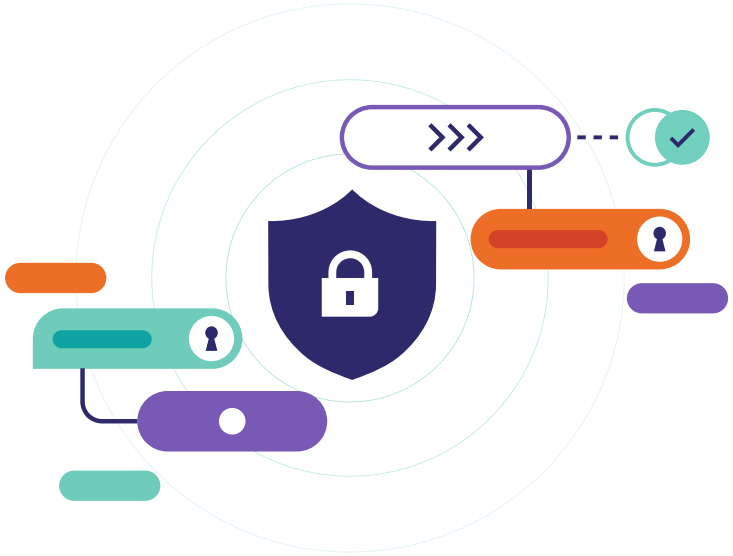
Insecure software supply chains have become a significant issue in recent years, as evidenced by high-profile incidents such as the SolarWinds breach in 2020 and the Log4j vulnerability in 2021. The perceived threat has become so severe that, in May 2021, the White House sought to address it with Executive Order 14028, entitled “Improving the Nation's Cybersecurity.” The Executive Order requires any organization doing business with the U.S. federal government to generate and present an SBOM, a list of all the components, libraries, and modules that make up the application.

SBOM generation is a way for public sector organizations to ensure compliance with government mandates. SBOMs are also becoming increasingly indispensable in the private sector to help companies manage software dependencies and improve their security and compliance posture. However, our survey suggests that SBOM adoption is still in its early stages.

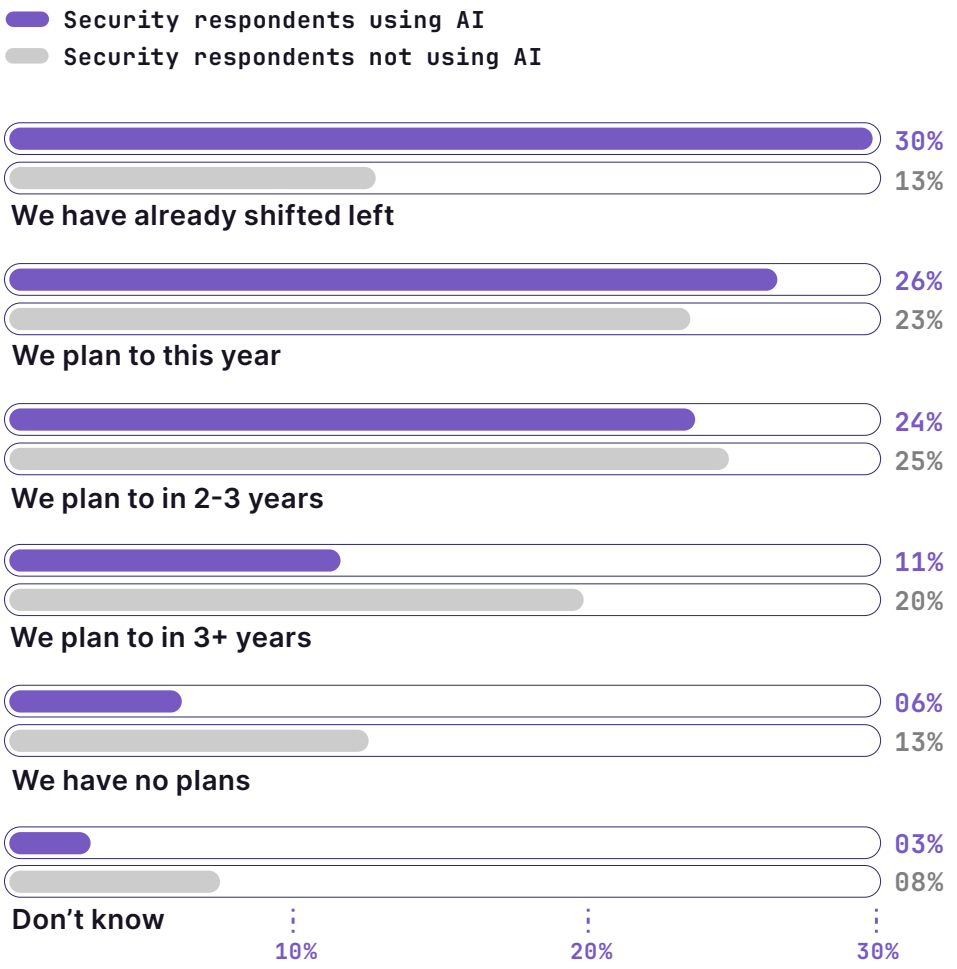
AI is now status quo — what does that mean for security?

Any survey of technology trends this year must address the artificial intelligence (AI) question, as machine learning, natural language processing, and generative AI now pervade every aspect of the tech landscape. Application development is no exception, with AI-generated code now readily available to developers and enabling even faster iteration of codebases. An overwhelming majority (78%) of respondents in our survey said they currently use AI in software development or plan to do so within the next two years. Over a quarter (26%) of those currently using AI for application development identified improved security as one of the top benefits of AI.

In addition, over half (52%) of respondents said they are interested in using, or planning to use, AI-powered explanations of security vulnerabilities. This use case is already among the most well-known applications of generative AI in security operations (SecOps), helping analysts to understand threats and respond to alerts in a timely fashion, even though the technology has only emerged into the popular consciousness over the last couple years.

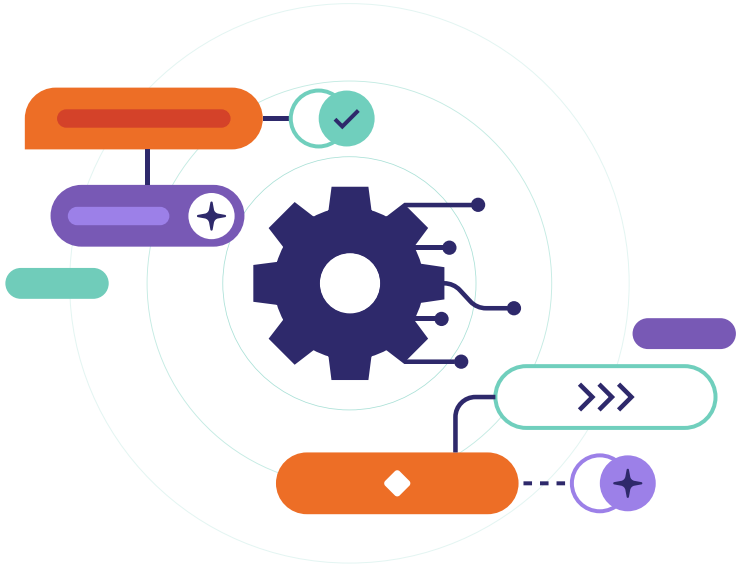


Where is your organization in your efforts to shift security left?

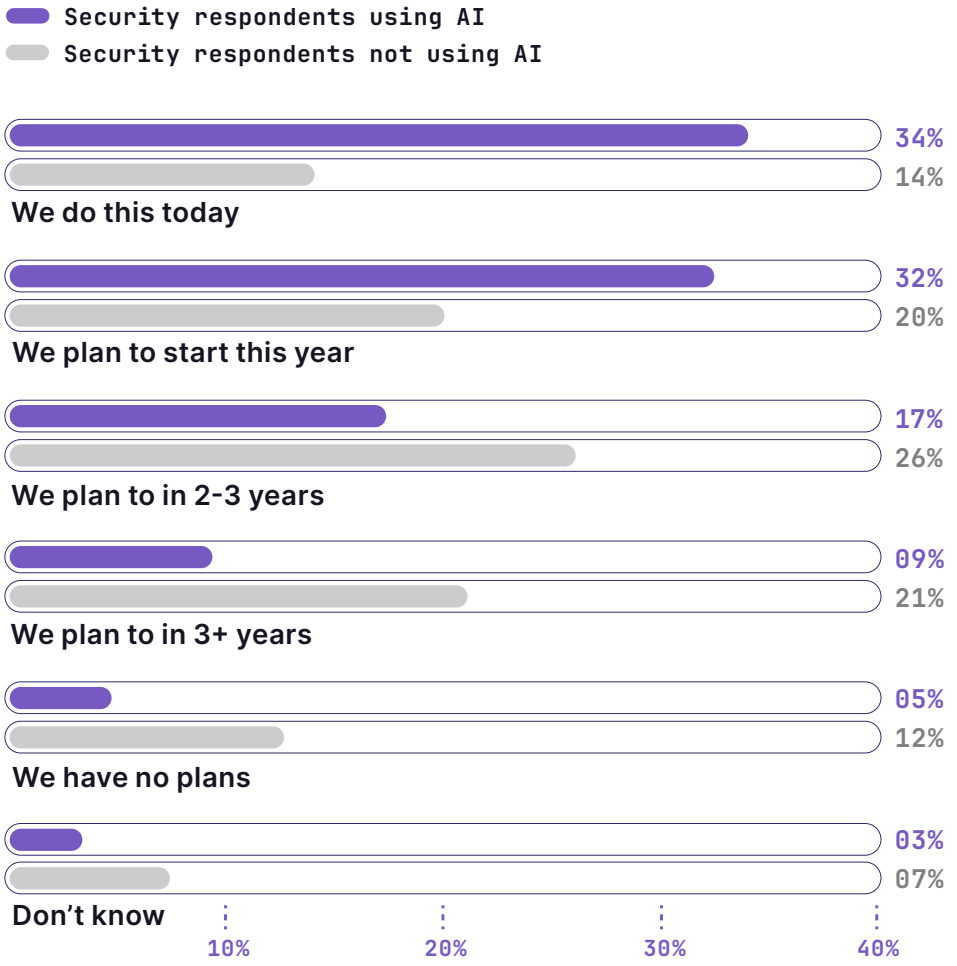


AI and the shift left

It's clear that organizations are adopting AI for use cases throughout the software development lifecycle, including security. Our survey findings also suggest that AI adoption could be a signal of DevSecOps maturity. Security respondents whose organizations are already using AI were significantly more likely than those not using AI to say that their organization has practices establishing a shared responsibility for application security, spanning both the development and security teams. For instance, 30% of those using AI said their organizations are shifting security left, compared to just 13% of those not using AI. Additionally, 34% of those using AI are educating developers about security best practices, compared to only 14% of those not using AI.



Is your organization educating developers about security practices?



Security and privacy concerns remain top of mind

Despite the perceived and real benefits of AI for application security, our survey respondents also voiced a number of concerns related to the use of AI. More than half (55%) of respondents said that introducing AI into the software development lifecycle is risky, and privacy and data security represented the number one concern.

Top obstacles related to using AI in software development

34%

Concerns around **privacy** and **data security**

31%

Lack of appropriate skill set to **employ AI** or **interpret AI** output

30%

Lack of **knowledge** about AI

29%

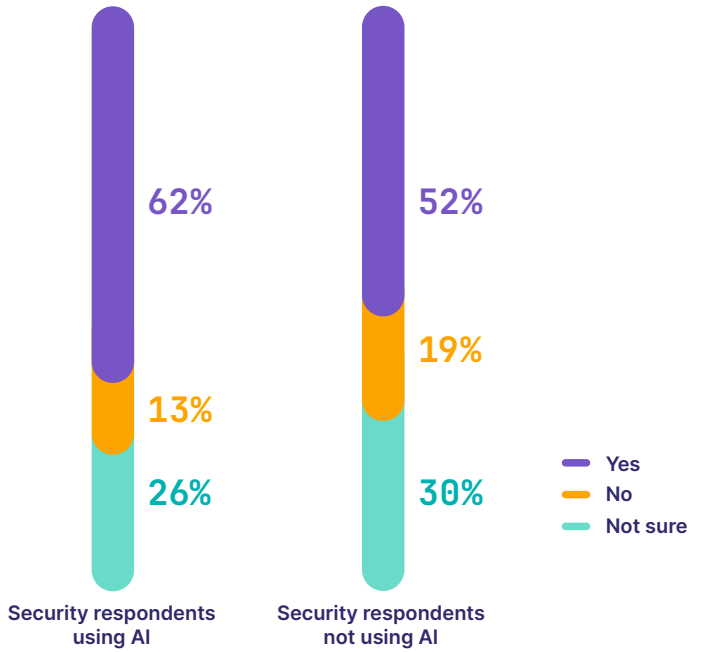
Difficulty **procuring AI tools** (securing legal approval, etc.)

27%

Lack of confidence in **AI-generated output**

In addition, a quarter of respondents who are currently using AI expressed concern about security vulnerabilities in software built using AI. Digging into this further, we found that 62% of security respondents whose organizations are currently using AI said vulnerabilities are mostly discovered by their security team after code is merged into a test environment, but only 52% of those not using AI said the same. Certainly, security vulnerabilities being found late in the development process are a problem with or without the involvement of AI; however, this finding suggests that the use of AI could be creating more issues for SecOps to find, or pushing the identification of vulnerabilities towards the end of the development process — or both.

Are security vulnerabilities in your organization mostly discovered by the security team after code is merged into a test environment?

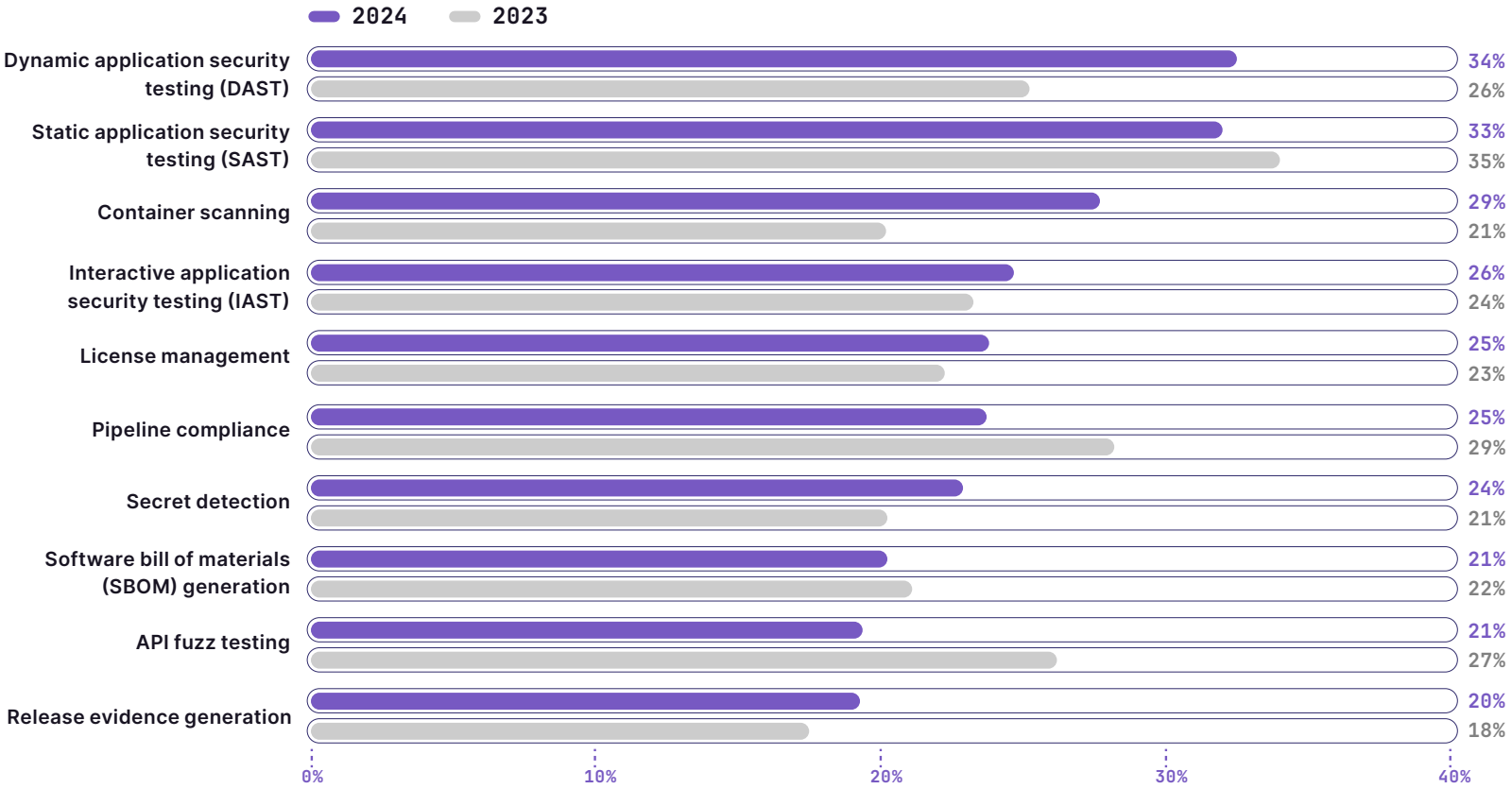


Balancing speed and security

Given the increase in software output and the corresponding increases in the attack surface, how are organizations balancing speed and security in the software development lifecycle?

When we asked this year's respondents how they are enabling security in the software development lifecycle, their top answer was dynamic application security testing (DAST) (34%), followed by static application security testing (SAST) (33%). In addition, DAST showed a marked increase from 2023, up from just 26% last year, suggesting that organizations are prioritizing both DAST and SAST in their application security strategies. Container scanning (from 21% to 29%) and secret detection (from 21% to 24%) also showed significant year-over-year increases.

How does your organization enable security in the software development lifecycle?



Code quality and security have traditionally been the concerns of different teams within an organization and have been monitored separately, with code quality frequently tested at various points in the development lifecycle. In contrast, security checks have traditionally been carried out towards the end. However, Omdia suggests that the two should be dealt with together, using the same technology — such as a DevSecOps platform — to detect security issues and highlight areas where code quality can be improved throughout the development process.

Our survey supports that line of thinking: of the survey respondents currently using a DevSecOps platform, more than a quarter (27%) identified more secure applications as one of its top benefits. This benefit ranked third, after better code quality and greater operational efficiency. In addition, respondents who were using a DevSecOps platform (68%) were significantly more likely than those not using a platform (57%) to feel confident in their organization's approach to application security.

Top benefits of a DevSecOps platform

28%
Better code quality

27%
Greater operational efficiency

27%
More secure applications

25%
Greater developer productivity

25%
Faster iteration

As organizations continue to accelerate their software development processes, it will be important for them to make the right investments in areas like AI and application security scanning to ensure that newfound speed doesn't come at the cost of security. Our survey findings reinforce that implementing a robust DevSecOps approach — including a DevSecOps platform — can help organizations balance speed and security, bringing teams together to proactively address vulnerabilities and ensure the highest quality code is being released.

Demographics and methodology

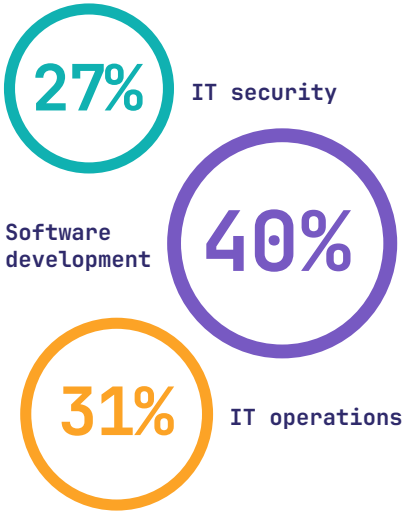
We collected a total of 5,315 survey responses in April 2024 from individual contributors and leaders in development, IT operations, and security across a mix of industries and business sizes worldwide.

We used two sampling methods for the data collection:

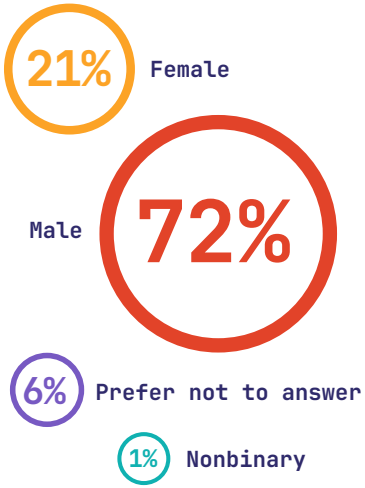
- We distributed the survey via GitLab's social media channels and email lists.
- A third-party research partner, Omdia, conducted panel sampling, which reduces bias in the sample. Omdia used its proprietary access to lists, panels, and databases to gather quality responses and cleaned the data throughout fielding to ensure data quality.

Here's a closer look at the survey respondents:

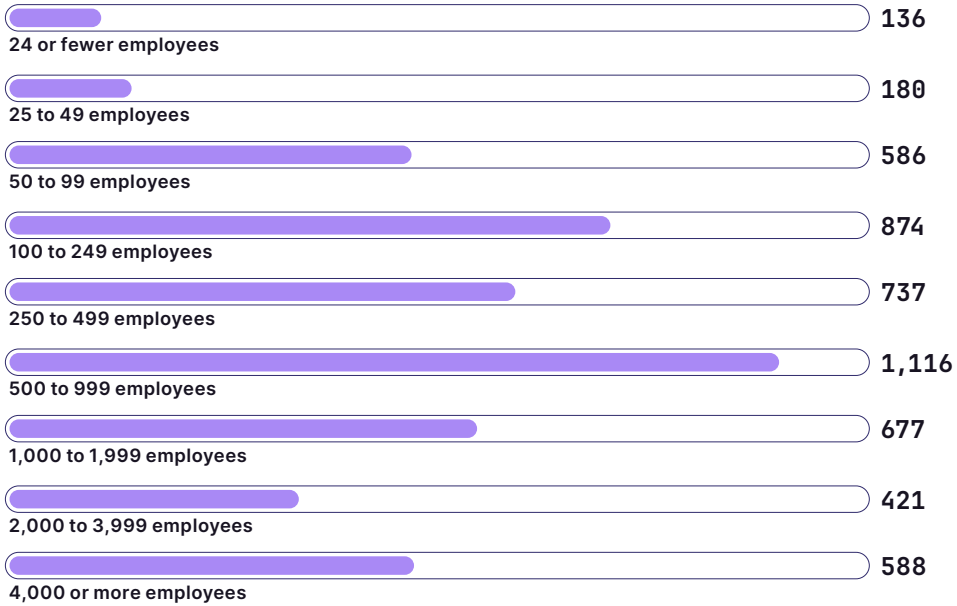
Functional area



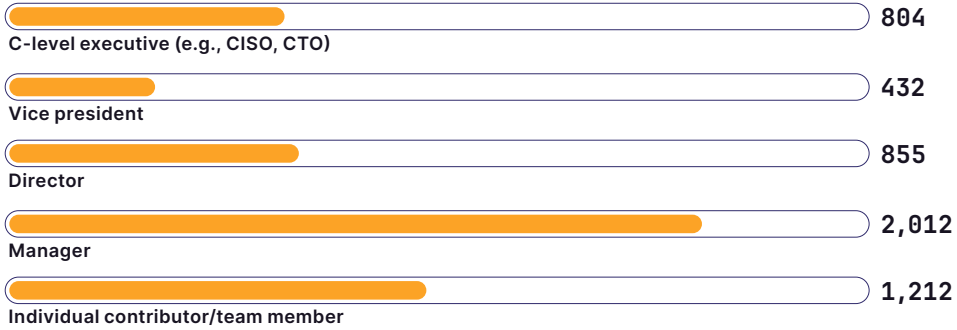
Gender



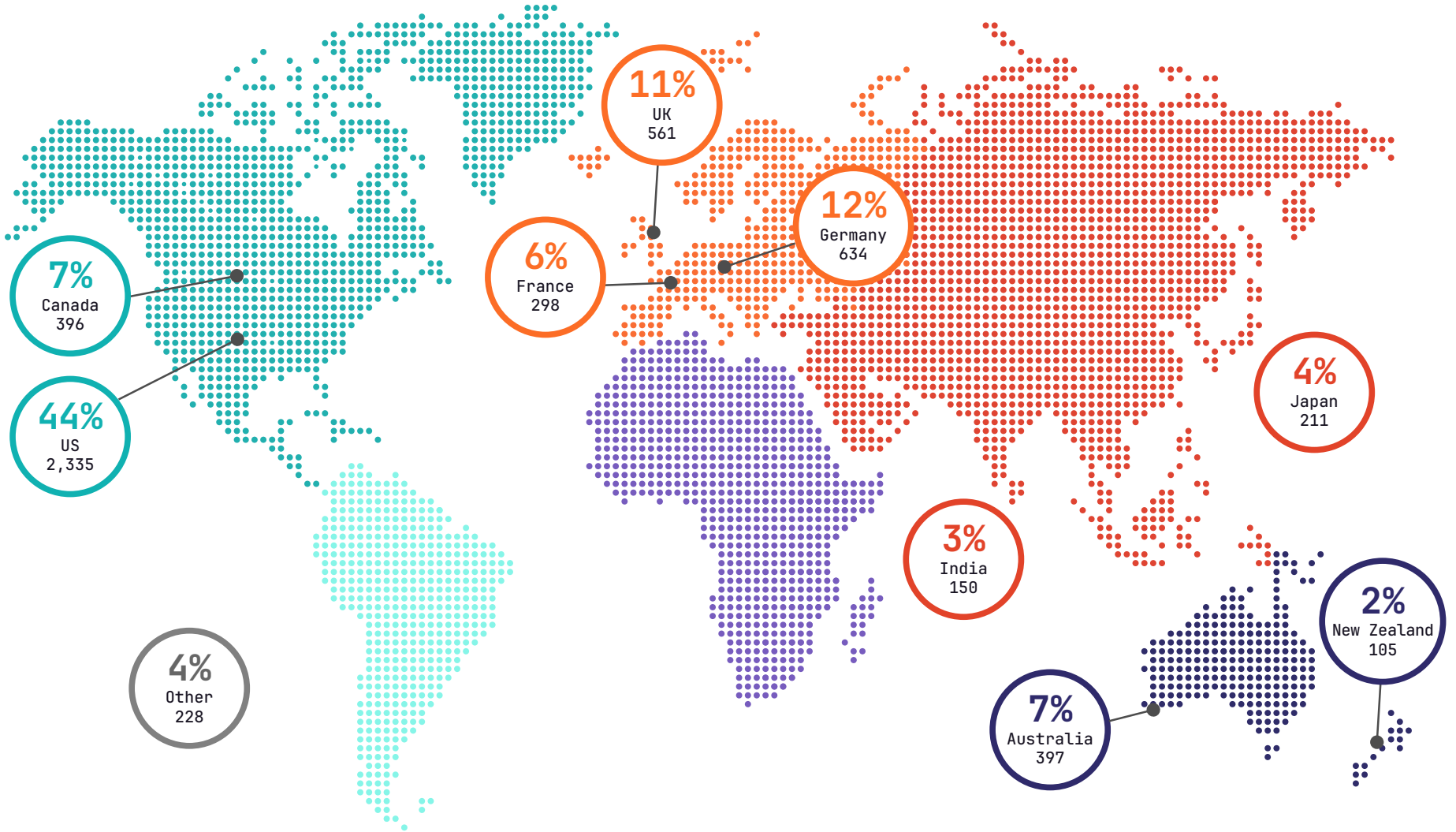
Organization size



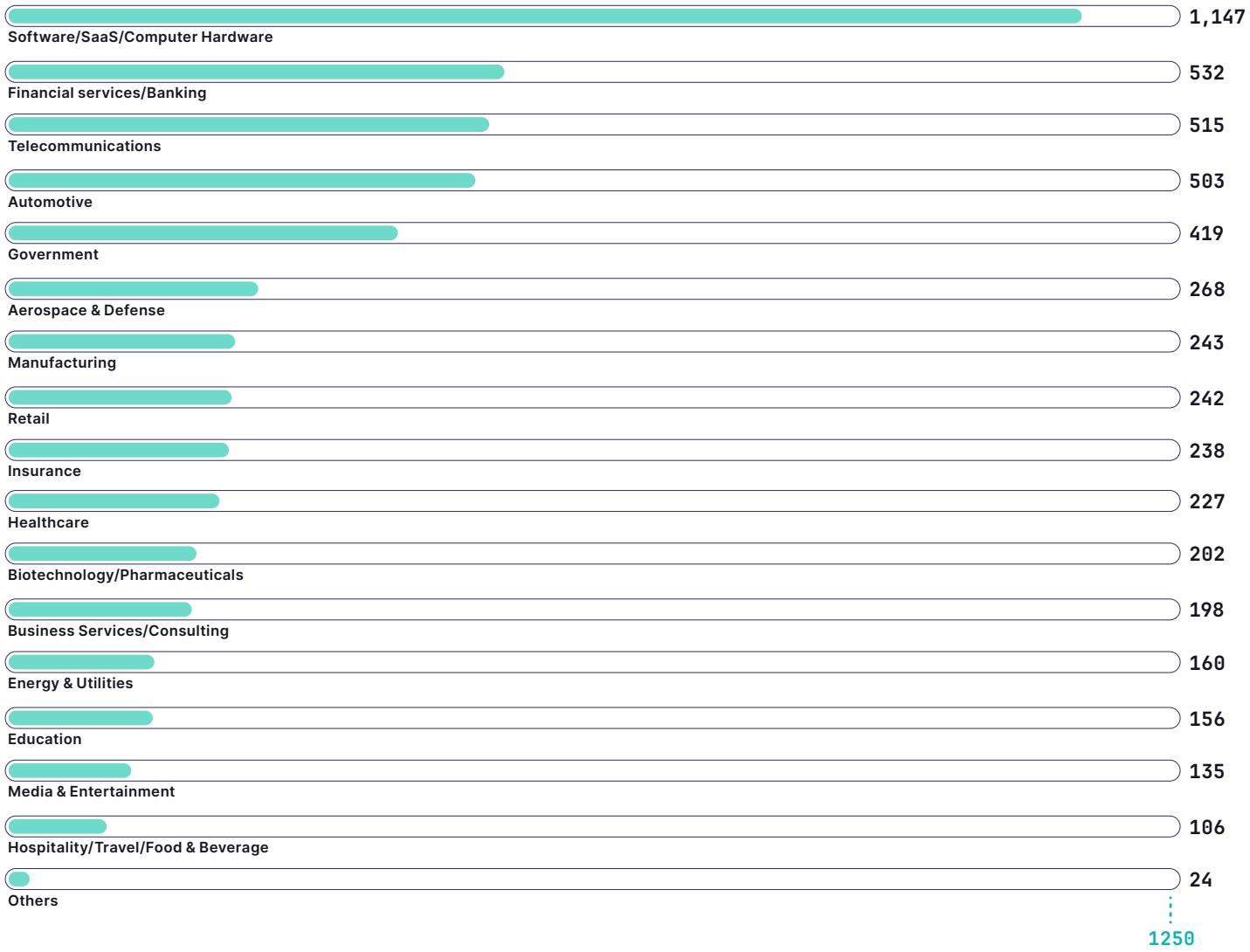
Job role



Geography


11%
UK
561
12%
Germany
634
6%
France
298
7%
Canada
396
44%
US
2,335
4%
Other
228
4%
Japan
211
3%
India
150
2%
New Zealand
105
7%
Australia
397

Industry


Software/SaaS/Computer Hardware
1,147
Financial services/Banking
532
Telecommunications
515
Automotive
503
Government
419
Aerospace & Defense
268
Manufacturing
243
Retail
242
Insurance
238
Healthcare
227
Biotechnology/Pharmaceuticals
202
Business Services/Consulting
198
Energy & Utilities
160
Education
156
Media & Entertainment
135
Hospitality/Travel/Food & Beverage
106
Others
24
1250