THE 2022 OPEN SOURCE SOFTWARE SUPPLY CHAIN SURVEY REPORT

TIDELIFT

INTRODUCTION

In December of 2021, Tidelift fielded our annual survey of technologists—including software developers, engineering executives and managers, architects, and devops pros—who build applications with open source.

Nearly 700 people shared how they use open source software to build applications today, what barriers they face, and what tools and strategies would help them use open source even more effectively. We also renamed the survey this year to reflect a heightened focus on the health and security of the open source software supply chain in organizations, government, and the media.

In this year's survey, we learned how current events like the SolarWinds and Log4Shell software supply chain exploits and new government initiatives like the White House executive order on improving the nation's cybersecurity are changing the way organizations manage open source. We explored the most urgent challenges development teams face when building applications with open source. We collected data regarding how confident technologists are in their organizations' current open source management practices, and in the open source components and languages they use more generally. Finally, we dove deep into several open source management best practices, including the use of software bills of materials (SBOMs) and repositories of approved open source components.

For more information on how we conducted the survey, please see the about this survey section at the end of the report.

TABLE OF CONTENTS

FINDING #1

Security is open source developers' most urgent challenge, while complying with government requirements is an emerging concern

HEADLINES

Security is the most common challenge application development teams face when building with open source (57%), with making good decisions about which components to use (53%) and when to upgrade them (54%) coming in right behind.

Security is also the **most urgent** challenge (30%)—and the larger the organization, the more likely it is to be the most urgent (35% of the largest organizations named security the most urgent challenge).

Almost half of the largest organizations with more than 10,000 employees are challenged by complying with government requirements (48%), with 13% naming it the most urgent challenge (almost four times more commonly cited than in smaller organizations).

The largest organizations are struggling across the board with issues related to managing open source. Every challenge we identified was cited by nearly half or more respondents.

In the largest organizations, almost all respondents (87%) struggle with making good decisions about which components and versions to use.

Comparing this year's results to our previous survey, challenges managing open source have spiked in the largest organizations. For example, "requesting to use new open source components is a lengthy or confusing process" nearly doubled in mentions (from 33% to 63%) since our last survey.

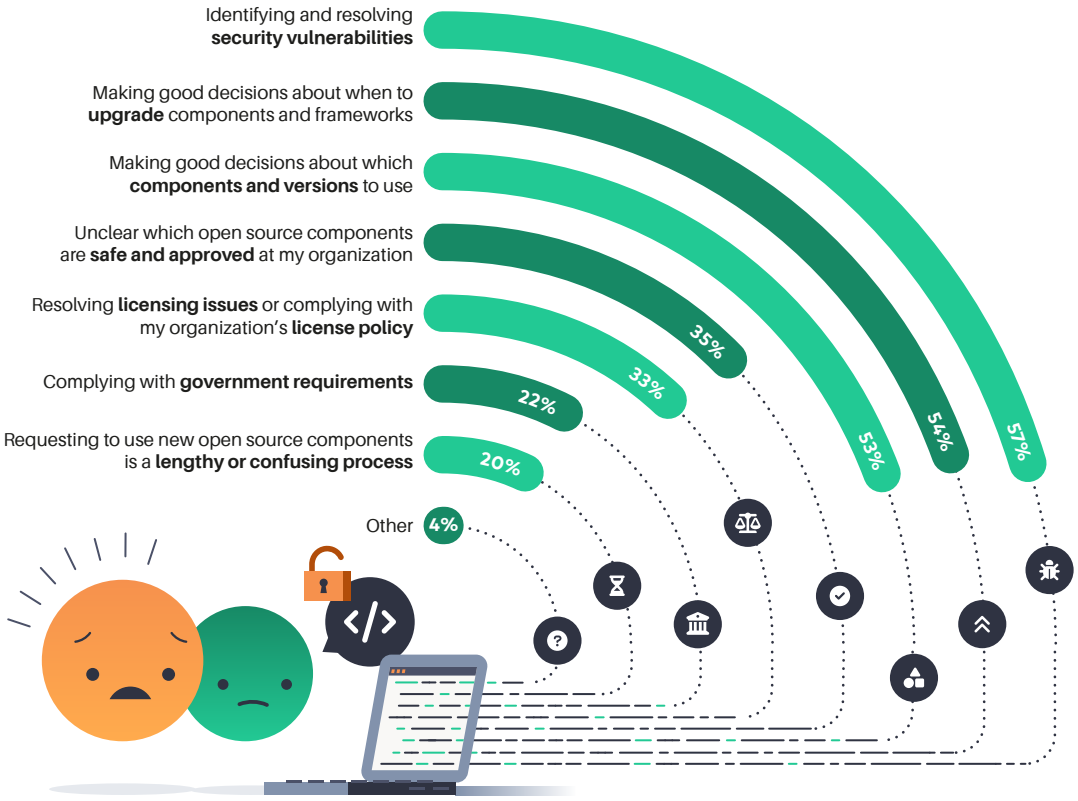
In the wake of the recent Log4Shell vulnerability, it's probably no surprise that security has taken center stage for teams developing applications with open source. (Want to learn more about what Log4Shell is and why it matters? Here's a good place to start.)

Interestingly, because our new survey was in the field as the Log4Shell crisis was unfolding, we have data from both before and after the vulnerability was uncovered. We'll share the pre- and post-Log4Shell data where it is meaningfully different.

In this year's survey, we once again asked technologists to name the challenges their teams face when building applications with open source. We've been asking similar questions for several years in these surveys, and every year, the top three challenges named by respondents are related to maintenance, security, and licensing. In our earlier survey, maintenance had been the #1 challenge, but this year—unsurprisingly—security took over the top slot.

Development teams struggle most with identifying and resolving security vulnerabilities

Which of the following challenges does your team face when using open source for developing applications? (select all that apply)



n=691

This year, 57% of respondents named "identifying and resolving security vulnerabilities" as a challenge, while just over half of respondents selected the next two challenges—"making good decisions about when to upgrade components and frameworks" and "making good decisions about which open source components and versions to use."

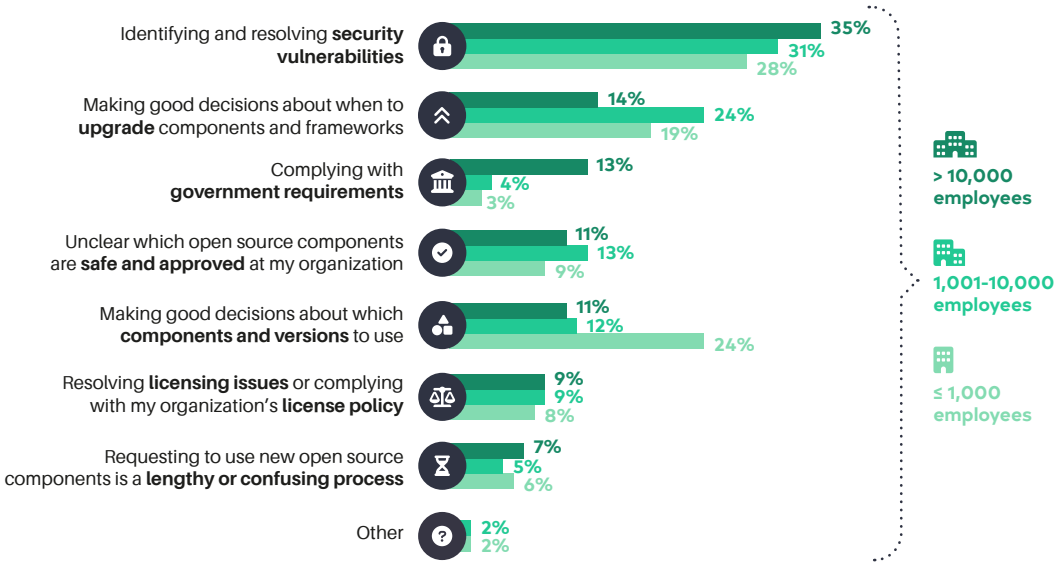
The challenges drop off after the top three, with 35% of respondents reporting that it is "unclear which open source components are safe / approved at their organization," while 33% named "resolving licensing issues or complying with their organization's license policy."

We also asked for the first time, in the wake of the White House Cybersecurity Executive Order and other ensuing government actions, if complying with government requirements is a challenge, and almost a quarter of respondents (22%) indicated that it is. This percentage rose to an astounding 48% for large organizations with over 10,000 employees.

In a follow up question, we asked respondents to select the most urgent challenge from those they had identified. For organizations of all sizes, security was the #1 most urgent challenge, and the larger the organization, the more likely it was to be selected, with 35% of respondents from the largest organizations naming it.

Identifying and resolving security vulnerabilities is the **most urgent** challenge for organizations of all sizes

Of those same challenges, which of the following is the **most urgent** to address?

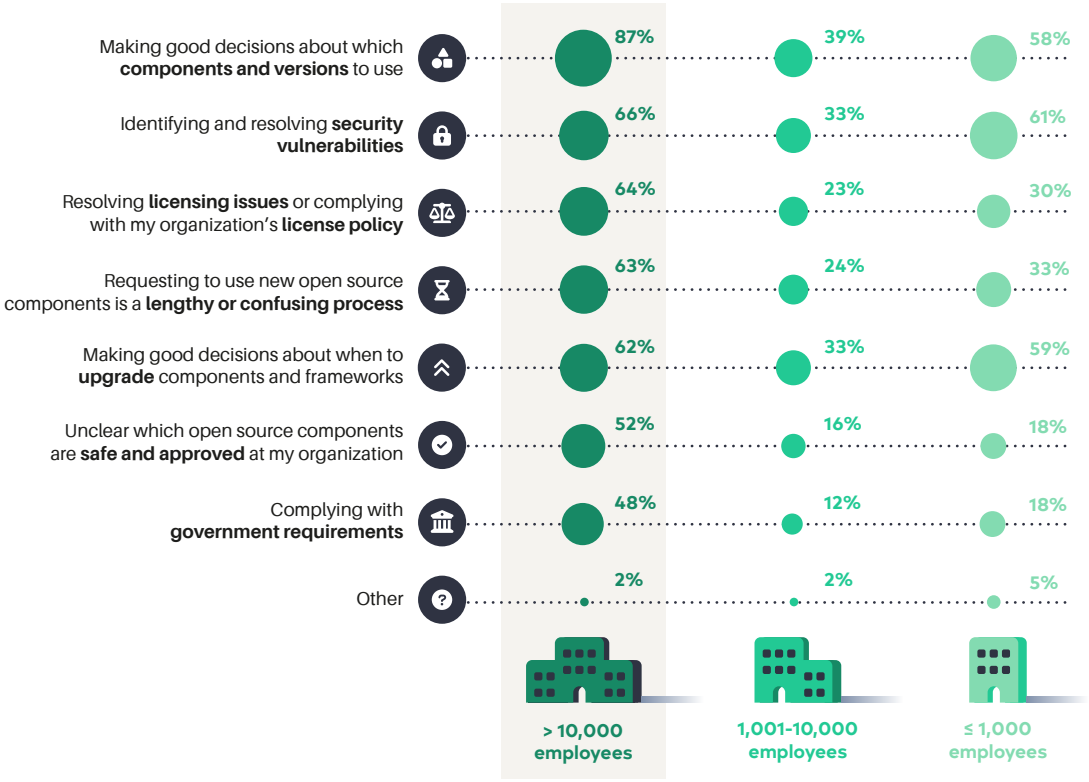


> 10,000 employees, n=122; 1,001-10,000 employees, n=151; ≤ 1,000 employees, n=418

For the largest organizations, complying with government requirements was an outlier as well; 13% of respondents named this as the most urgent challenge, almost four times higher than in smaller organizations.

Large organizations face many more challenges developing applications with open source than smaller ones

Which of the following challenges does your team face when using open source for developing applications? (select all that apply)



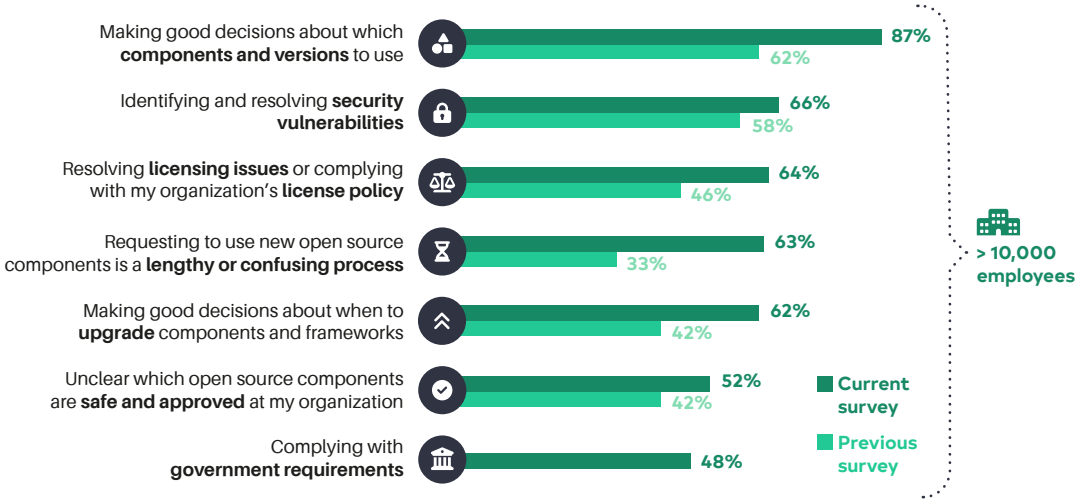
> 10,000 employees, n=122; 1,001-10,000 employees, n=153; ≤ 1,000 employees, n=421

One other top level finding: The largest organizations are simply facing more challenges developing applications with open source. The chart above shows that every single one of the challenges we named was reported by roughly half or more of respondents. Interestingly, even though it was not the most urgent challenge for large organizations, the most-cited challenge, "making good decisions about which components and versions to use," is ubiquitous, selected by 87% of respondents from the largest organizations.

We compared our data from the previous survey to see where the challenges were getting more acute in these large organizations. Across the board, the percentages rose. For example, "requesting to use new open source components is a lengthy or confusing process" nearly doubled (from 33% to 63%) since our last survey. And "making good decisions about which components and frameworks to use" stayed in first, but increased in terms of percentage of mentions from 62% to 87%.

Challenges with managing open source are increasing for the largest organizations

Which of the following challenges does your team face when using open source for developing applications? (select all that apply)



Current survey conducted in Q4 2021: > 10,000 employees, n=122;
Previous survey conducted in Q3 2020: > 10,000 employees, n=57

FINDING #2

Only 15% of organizations are extremely confident in their open source management practices; the majority have concerns

HEADLINES

Only 15% of organizations are extremely confident that the open source components they are using are up-to-date, secure, and well maintained.

The majority of respondents are somewhat confident (62%), while 22% are not very or not at all confident.

The largest organizations are still less confident in their open source management practices than smaller ones, but the differences are less pronounced than in our previous survey.

SBOM

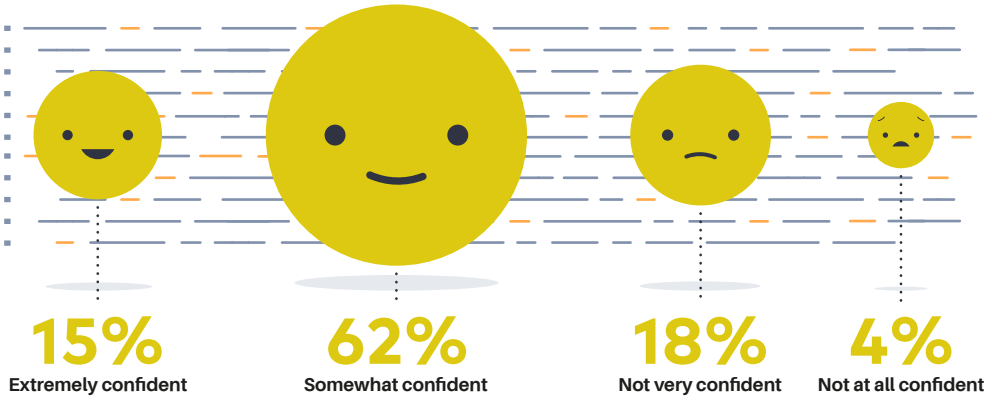
Organizations currently using software bills of materials (SBOMs) are generally more confident than those not using them.

In our previous survey, one of the most shocking findings was that the majority of respondents expressed reservations about how well their organization manages open source. In that survey we found that only 18% of respondents were extremely confident in their organization's management practices, while 24% were not very or not at all confident.

Our results this year were relatively consistent. First the bad news: in this year's survey, the percentage of extremely confident respondents dropped to 15%. The good news? The percentage reporting that they are not very or not at all confident also fell slightly from 24% to 22%. Which means that the majority of respondents are somewhat confident in their open source management practices (62%).

Only 15% of organizations are extremely confident in their open source management practices

How confident are you that the open source components your organization is using are up-to-date, secure, and well maintained?

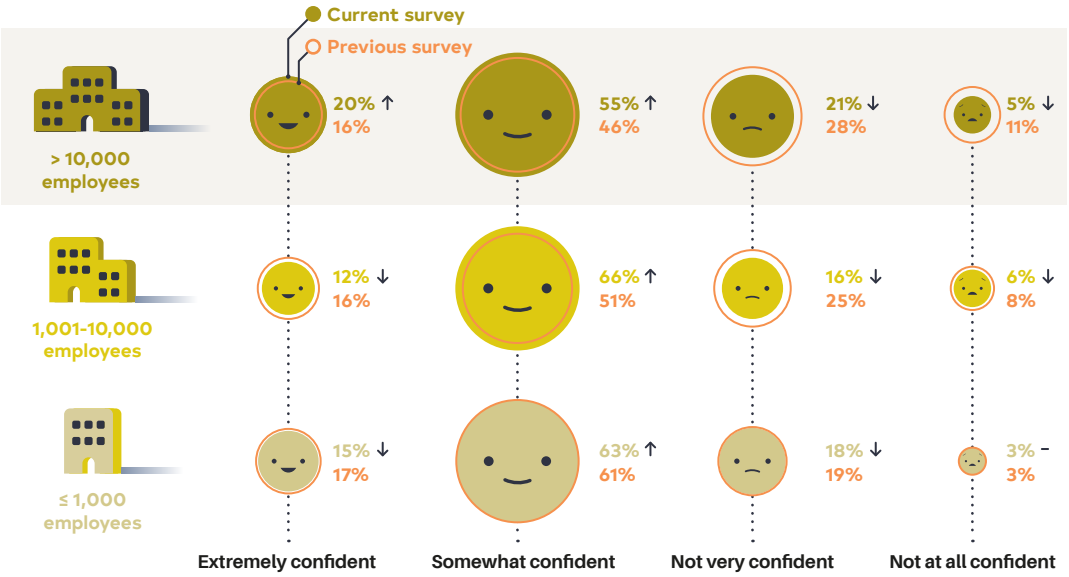


n=687

In our previous survey we found that the larger the organization, the less confident respondents were about its open source management practices. While respondents from the largest organizations were still less confident in this year's survey, the differences were less pronounced. In organizations with over 10,000 employees, 20% were extremely confident, while 26% were not very or not at all confident. This compares favorably to the previous results, where 39% reported that they were not very or not at all confident.

Large organizations continue to be less confident in their open source management practices, although the gap has narrowed

How confident are you that the open source components your organization is using are up-to-date, secure, and well maintained?

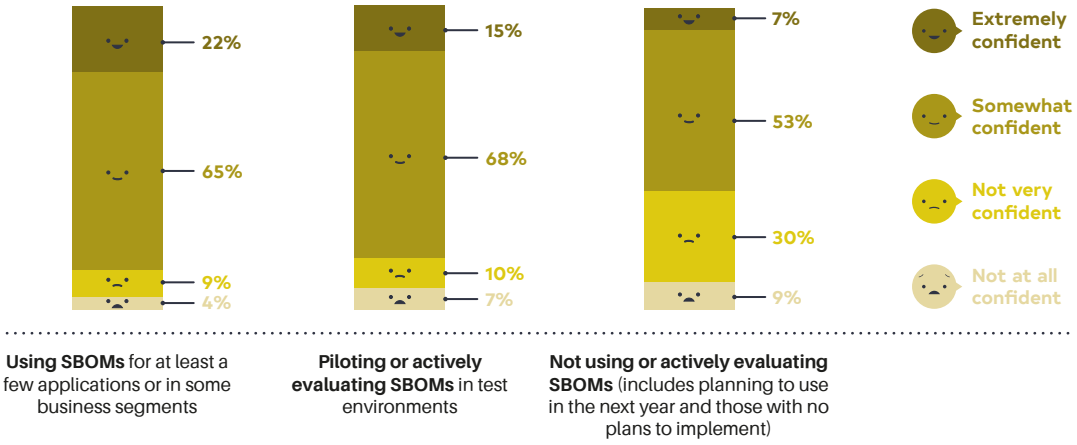


Current survey conducted in Q4 2021: > 10,000 employees, n=122; 1,001-10,000 employees, n=153; ≤ 1,000 employees, n=421; Previous survey conducted in Q3 2020: > 10,000 employees, n=57; 1,001-10,000 employees, n=65; ≤ 1,000 employees, n=193

One important factor that appears related to how confident respondents were about their open source management practices is whether their organization currently uses software bills of materials. In organizations using software bills of materials, 22% reported that they were extremely confident while only 13% reported being not very or not at all confident. Conversely, only 7% of organizations that are not using software bills of materials were extremely confident, while 39% were not very or not at all confident.

Organizations using SBOMs tend to be more confident that their open source components are up-to-date, secure, and well maintained

How confident are you that the open source components your organization is using are up-to-date, secure, and well maintained?



Using SBOMs for at least a few applications or in some business segments, n=106, Piloting or actively evaluating SBOMs in test environments, n=41, Not using or actively evaluating SBOMs, n=86 | Only respondents that were aware of a May 2021 White House executive order on cybersecurity were asked the following question: "Which of the following describe how your organization is currently using SBOMs for application development?"

FINDING #3

Of the top three open source languages, Python earns highest confidence ratings

HEADLINES

The three most-relied-upon languages are still Python, JavaScript, and Java, with a big gap between them and the next most popular languages.

Reliance on Python and Java both increased since our last survey, while JavaScript fell significantly.

Most other languages did not change much since our last survey, with the exception of C++ and Go, which both gained significantly.

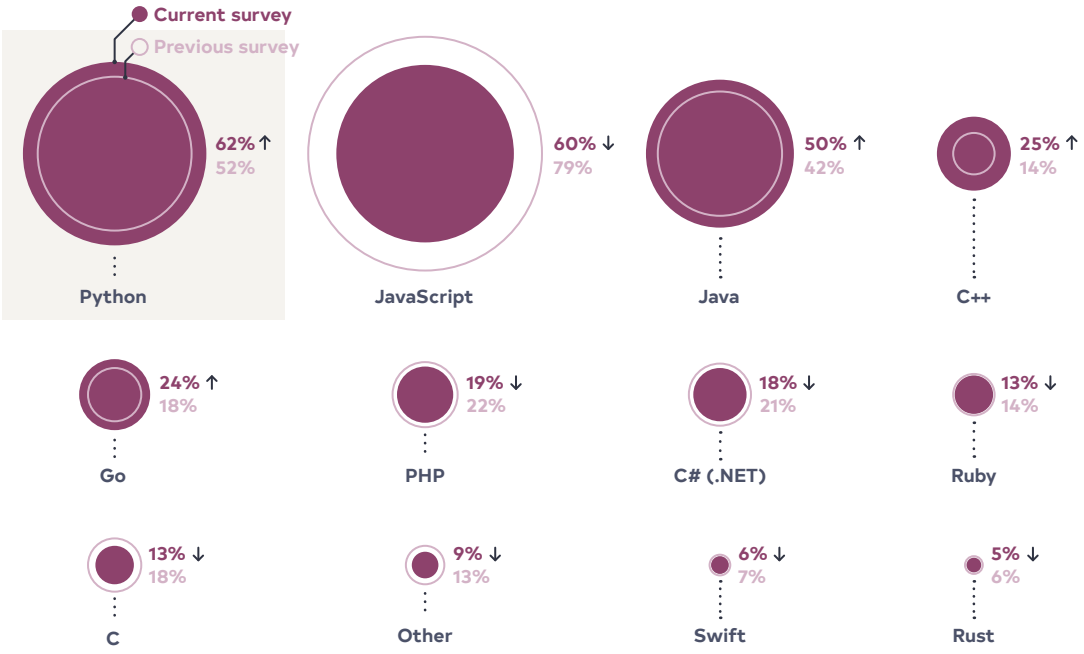
Of the top three languages, respondents expressed the most confidence in how up-to-date, secure, and well maintained Python components are, and less confidence about JavaScript components.

Confidence in Java security and maintenance declined in the wake of the Log4Shell vulnerability that impacted Log4j (a Java logging component).

In these surveys, we regularly check in to see which open source programming languages are most popular with development teams. In the past, we've found that the top three languages (JavaScript, Java, and Python) stand apart in terms of popularity from all of the rest.

Python is now the most relied-upon open source language, with JavaScript second and Java third

What are the top open source languages your organization relies upon? (select up to five)



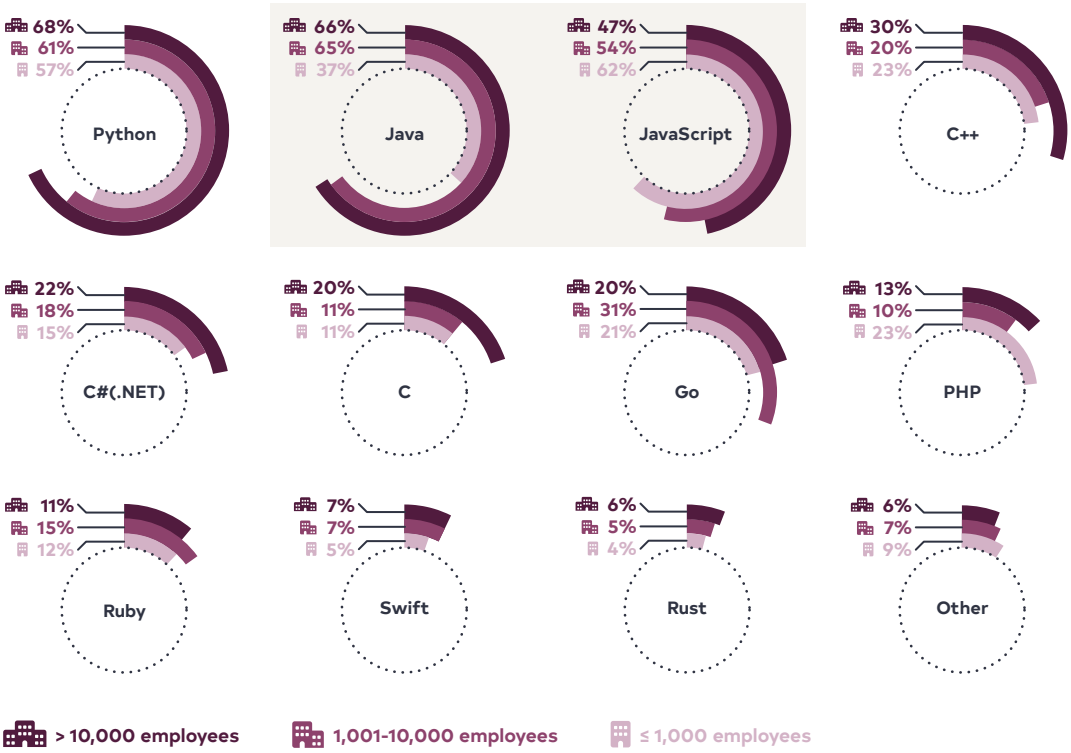
Current survey (Q4 2021), n=672; Previous survey (Q3 2020), n=487

This year was more of the same, with Python, JavaScript, and Java separated from the next highest response by over 25%. But one thing changed slightly this year; whereas in our last survey JavaScript was the top language, used by 79% of respondents and well above Python at 52% and Java at 42%, this year, the gap narrowed substantially, and Python took over the top position with 62% of respondents naming it a most-relied-upon language. JavaScript was second, dropping almost 20% to 60%, with Java coming in third, at 50%.

Most of the other languages stayed pretty stable, with the biggest jump going to C++, increasing its percentage of mentions from 14% to 25%. Go, which went from seventh (17%) in our previous survey up to fifth (24%) this year was the other big positive mover.

Larger organizations rely more on Java, while smaller organizations rely more on JavaScript

What are the top open source languages your organization relies upon? (select up to five)



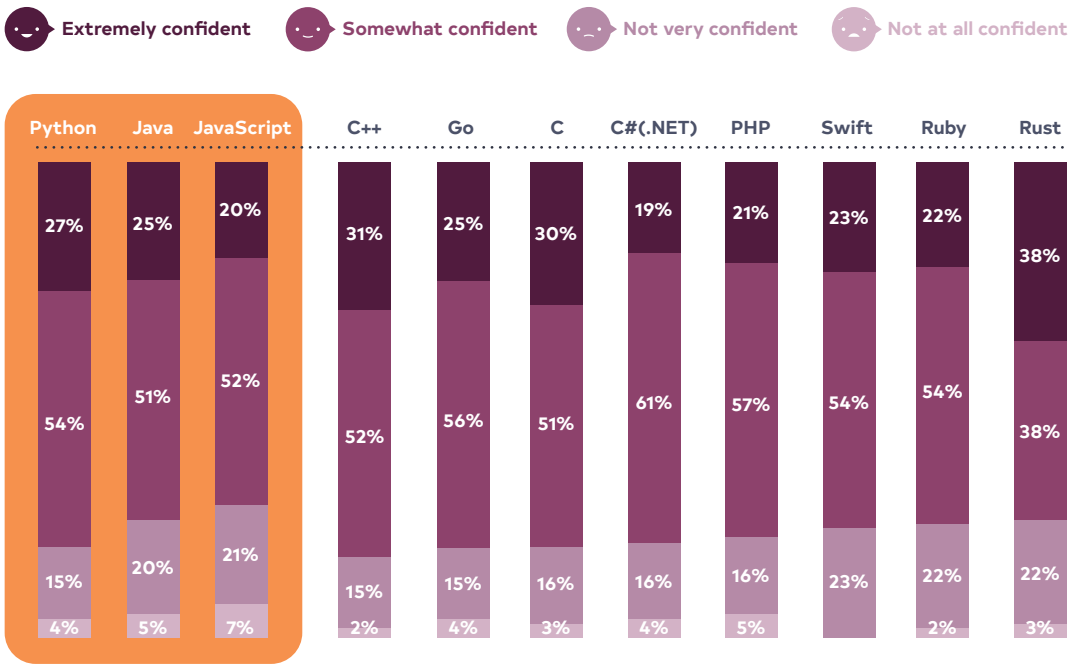
> 10,000 employees, n=122; 1,001-10,000 employees, n=153; ≤ 1,000 employees, n=421

We also took a closer look at the results by organization size. The larger organizations relied more on Java, while the smaller rely less on Java. The opposite was true of JavaScript, with large organizations relying on it less than smaller ones. But the top three languages remained the same, regardless of organization size.

A new angle we wanted to explore this year was to see if there were differences in how confident respondents were about whether the components they were using in these languages were up-to-date, secure, and well maintained.

Of the top three open source languages, Python earns highest confidence ratings

For languages their organization relies upon, respondents were asked: How confident are you that the components you are using are up-to-date, secure, and well maintained?



Python, n=403; Java, n=333; JavaScript, n=394; C++, n=163; Go, n=158; C, n=87; C# (.NET), n=113; PHP, n=129; Swift, n=35; Ruby, n=86; Rust, n=32

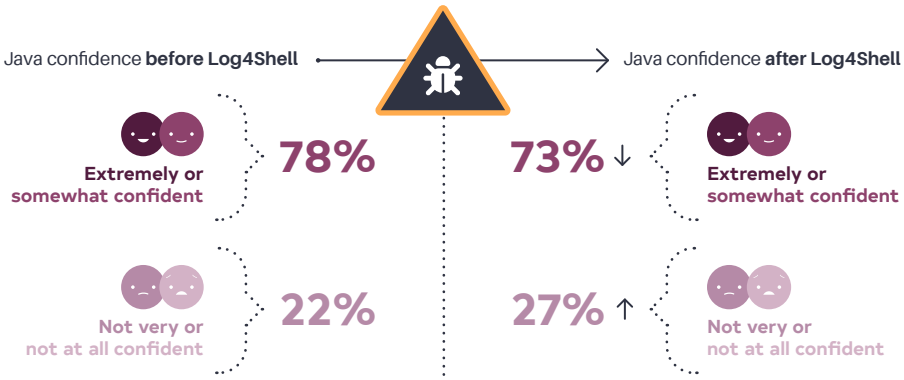
Respondents were most confident about Python, with 81% of respondents reporting they were extremely or somewhat confident and only 19% not very or not at all confident.

Next came Java, with 76% extremely or very confident and only 25% not very or not at all confident. JavaScript was third, with 72% extremely or very confident and 28% not very or not at all confident. Notably, JavaScript had the highest percentage of not very or not at all confident responses of all of the languages we asked about (28%) and second lowest percentage of extremely confident responses (20%).

In particular we also wanted to see if confidence in Java was hurt by the Log4Shell vulnerability in Log4j, a Java logging component, so we examined the answers that came in before and after the vulnerability was reported in early December.

Confidence in Java security and maintenance declined in the wake of the Log4Shell vulnerability

For languages their organization relies upon, respondents were asked: How confident are you that the components you are using are up-to-date, secure, and well maintained? (Java only, pre and post December 10).



Before Log4Shell, n=197; After Log4Shell, n=136

We saw that 78% of respondents who completed our survey prior to Log4Shell reported being extremely or somewhat confident in Java security and maintenance, and that number dropped slightly to 73% after Log4Shell. Meanwhile the percentage of respondents reporting being not very or not at all confident in Java security in maintenance rose after Log4Shell from 22% to 27%. Most notably, the percentage of respondents reporting that they were not at all confident more than doubled, from 3% pre-Log4Shell to 7% afterwards.

FINDING #4

Getting approval to use new open source components in large organizations is often slow and tedious

HEADLINES

The majority of organizations (61%) have some sort of approval process for introducing new open source components.

The remaining 38% of organizations have either no process or an informal process that does not require authorization.

In the largest organizations, an even higher percentage (78%) require some sort of authorization process for introducing new open source components while only 8% have no approval process at all.

Almost half (46%) of organizations under 1,000 employees have an informal authorization process or none at all.

Half of respondents report that it takes between one day and one week to get a new component approved, while in 39% of organizations approval takes a week or more.

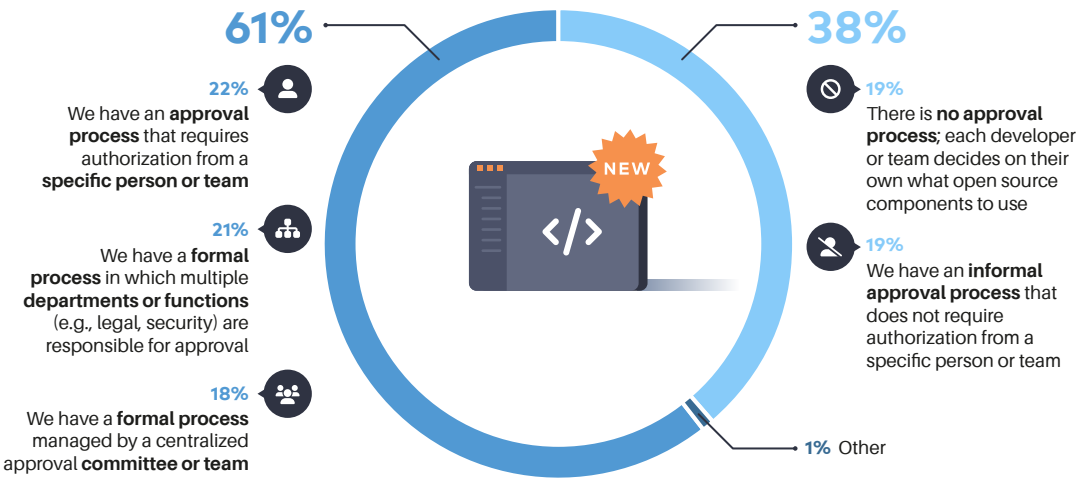
Approval takes longer in the largest organizations, with 56% of organizations over 10,000 employees saying approval takes a week or more.

In this year's survey, we wanted to understand how application development teams bring new open source components into their organization and what challenges they face when introducing these components.

First, we asked respondents to describe the evaluation or approval process currently being used to bring in new open source components. The majority of organizations employ some sort of process requiring authorization (61%) while 38% do not have an approval process or do not require authorization.

The majority of organizations have a formal approval process for introducing new open source components

Which of the following best describes the evaluation or approval process your organization uses to introduce new open source components?



n=637

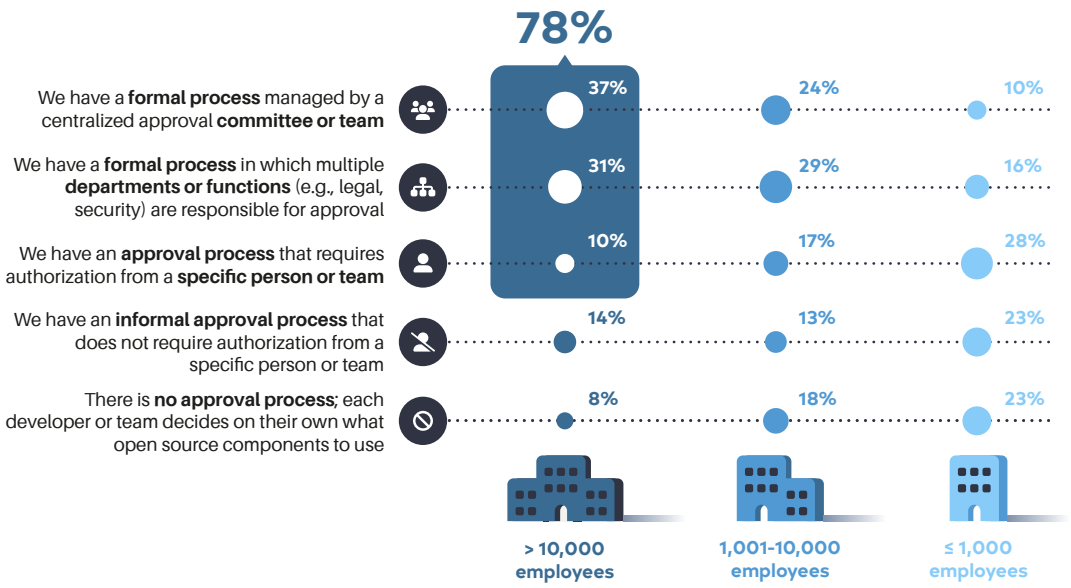
Of the 61% of organizations that require approval, 22% require authorization from a specific person or team, 21% require authorization by multiple departments, and 18% have a formal authorization process managed by a centralized committee or team.

Of the 38% of respondents not requiring authorization, 19% have no approval process at all and 19% have an informal approval process that does not require authorization.

We refer to the no-authorization-required organizations as the "move fast" camp and the authorization-required organizations as the "stay safe" camp, and it was interesting to see that the majority of organizations fell into the "stay safe" camp.

78% of the largest organizations have a formal approval process for introducing new open source components

Which of the following best describes the evaluation or approval process your organization uses to introduce new open source components?



> 10,000 employees, n=111; 1,001-10,000 employees, n=136; ≤ 1,000 employees, n=390

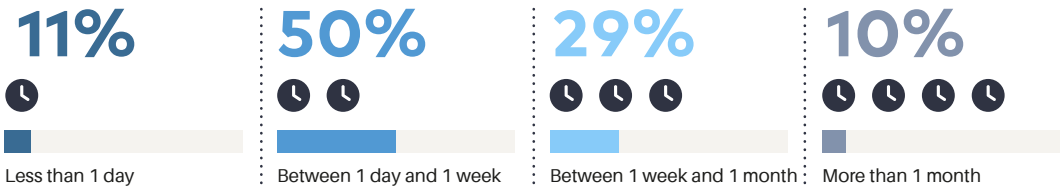
The differences became even more stark when looking at the results from the largest organizations with over 10,000 employees. A whopping 78% of respondents from these organizations have a process requiring authorization, led by 37% that have a formal process managed by a committee or team, another 31% with a formal process requiring multiple departments or functions for approval, and only 10% requiring authorization from an individual or team.

Only 22% of the largest organizations do not require authorization, with 14% of those having an informal approval process and 8% having no approval process at all. Not surprisingly, smaller organizations under 1,000 employees are twice as likely to not require authorization, with almost half (46%) of respondents reporting an informal process or none at all.

Next, we wanted to understand, for those organizations with some sort of authorization process, how long it typically takes to get new components approved. Only 11% of respondents get new components authorized in less than a day. For half of the respondents (50%) it takes between one day and one week. For 29% it takes between one week and one month. And in 10% of organizations, it takes a month or more.

Half of respondents report that it takes between one day and one week to get a new component approved

In general, how long does it take developers in your organizations to get approval to use a new open source component?

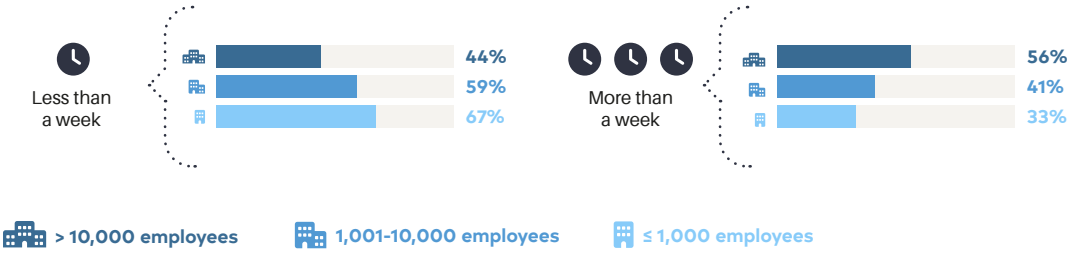


n=636

As one might expect, approval takes longer in the largest organizations. Whereas 39% of all respondents said it takes a week or more for approval, in organizations over 10,000 employees, that percentage shoots up to 56%, with 19% of respondents saying it takes more than a month to get new components approved. By comparison, only 6% of respondents from organizations with 1,000 or less employees said approval takes more than a month.

Approval takes longer in the largest organizations, with 56% of organizations over 10,000 employees saying approval takes a week or more

In general, how long does it take developers in your organization to get approval to use a new open source component?

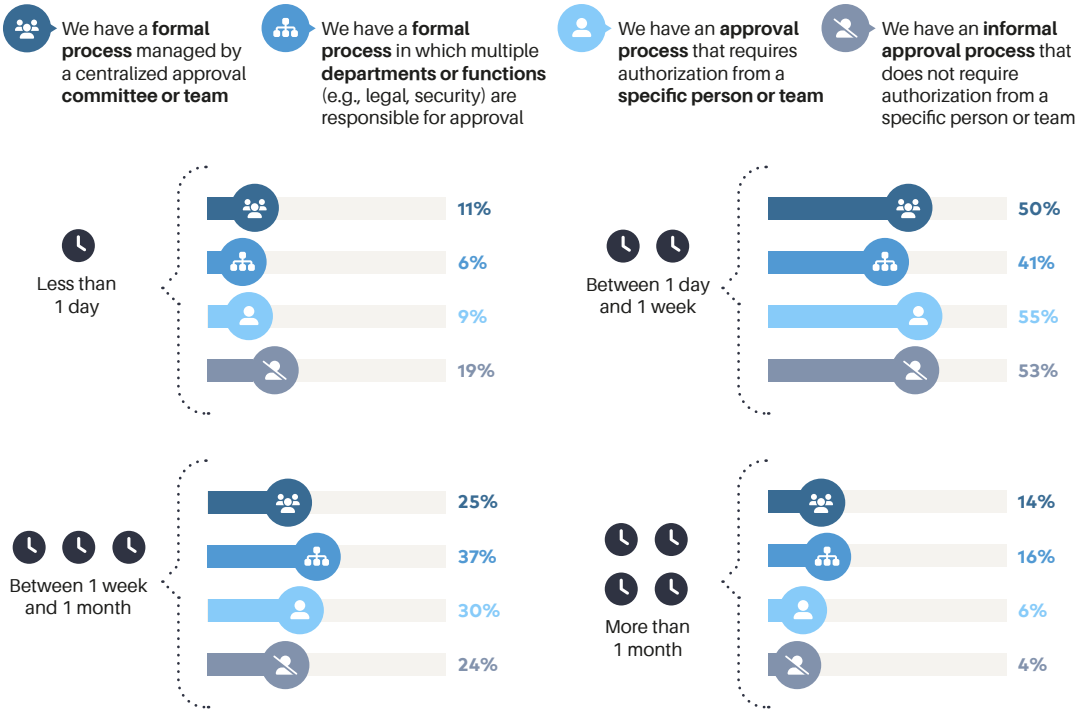


> 10,000 employees, n=102; 1,001-10,000 employees, n=112; ≤ 1,000 employees, n=301

Finally, we broke down the length of time it takes to get approval by the type of process the organization has in place. The results were stark, but intuitive. The most common process in organizations that approve components in less than a day is an informal process that does not require authorization from a specific person or team. Almost double the percentage of respondents who reported they use an informal process (19%) said approval takes less than a day.

Organizations with a formal approval process are much more likely to approve new open source components slowly

In general, how long does it take developers in your organization to get approval to use a new open source component?



We have a formal process managed by a centralized approval committee or team, n=112; We have a formal process in which multiple departments or functions (e.g., legal, security) are responsible for approval, n=134; We have an approval process that requires authorization from a specific person or team, n=142; We have an informal approval process that that does not require authorization from a specific person or team, n=122

Conversely, the organizations reporting that authorization to use a new component took more than a month typically have a formal process requiring approval from multiple departments or functions (16%) or a centralized committee or team (14%).

FINDING #5

The best practice of centrally managing a repository of approved open source components is growing rapidly

HEADLINES

65% of organizations are already using or actively piloting centralized repositories of approved open source components.

This percentage rises to 75% for the largest organizations.

Only 26% of organizations have no plans to use centralized repositories.

75% of organizations with over 10,000 employees are already using centralized repositories to track open source components or are piloting their use today.

Meanwhile, 32% of the smallest organizations have no plans to use this approach.

Over the past few years, several analyst firms including Gartner and IDC and leading open source management experts have recommended that organizations interested in more effectively managing open source security, maintenance, and licensing should consider creating and maintaining a centralized repository of approved open source components. The core benefits of this approach are:

1.

DEVELOPERS CAN MOVE FASTER

When pulling from the approved repository, developers don't get bogged down by a slow approval process like we saw many large organizations have today in our previous survey findings. When introducing new components, they are only vetted once, then after they are approved, can be used by developers across the organization without having to go through approval again. This makes the entire development team more efficient as the repository of approved components grows over time.

2.

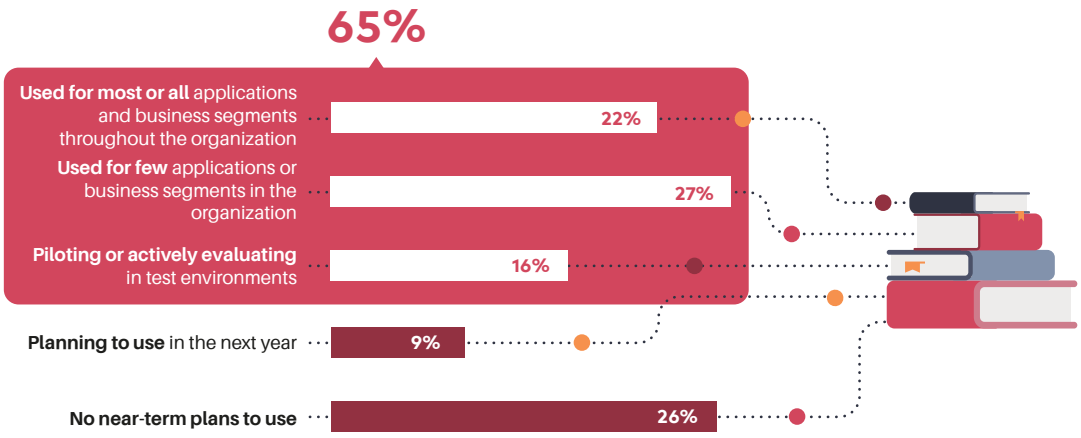
OPEN SOURCE SECURITY IMPROVES

When a vulnerability like Log4Shell emerges, rather than a slow search-and-remediate mission throughout the organization, a central repository can help quickly identify where the impacted components are being used. Then a consistent remediation recommendation for impacted applications can be applied quickly, everywhere the impacted component is in use. A centralized repository also gives development leaders one place to track components and versions that have already been pre-vetted to meet the organization's security, maintenance, and licensing standards and policies. Rather than expecting individual developers to become experts regarding these complex issues, decisions are made centrally, for the entire organization at once.

In this year's survey we wanted to see how much the centralized repository of approved open source components best practice is already in use in organizations.

65% of organizations are already using or actively piloting centralized repositories of approved open source components

How widely are centralized inventories and/or repositories used to track open source components **being used**?

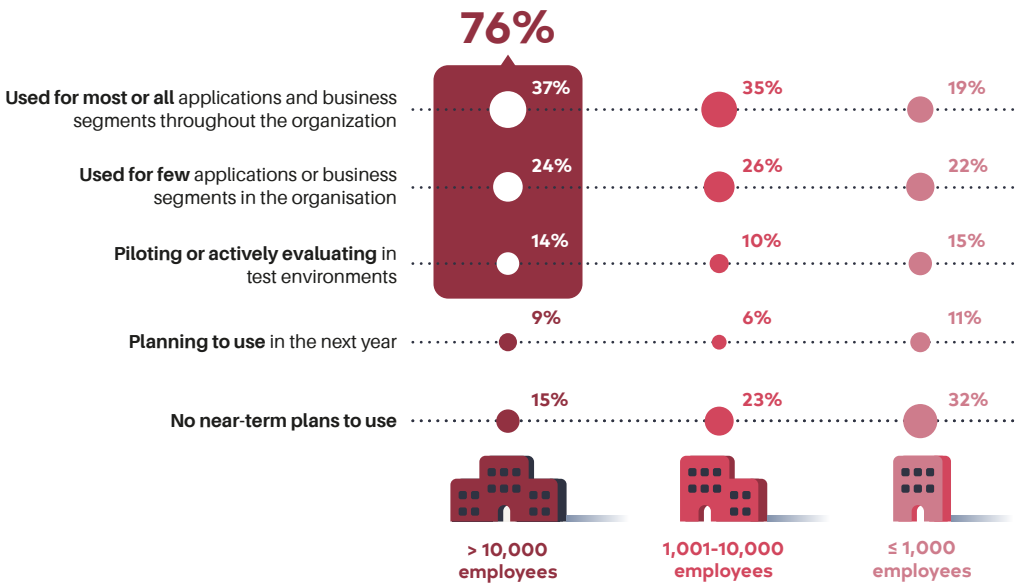


n=637

We found that 65% of organizations are already using centralized repositories to track open source components, whether for just a few business segments within the organization (27%), for most or all applications (22%), or are piloting or actively testing this approach (16%). Only 26% of respondents report that their organization has no near term plans to use centralized repositories to track open source.

76% of large organizations are already using centralized repositories to track open source components or are piloting their use

How widely are centralized inventories and/or repositories used to track open source components **being used**?



> 10,000 employees, n=111; 1,001-10,000 employees, n=136; ≤ 1,000 employees, n=390

As with many of the other questions in this survey, we also broke the results down by organization size. Of note, 75% of organizations with over 10,000 employees are already using centralized repositories to track open source components or are piloting their use. And 37% of these large organizations are already using centralized repositories for most or all business segments.

Meanwhile, smaller organizations are much less likely to be using centralized repositories, with only 19% using them throughout the organization and 32% with no near-term plans to use them.

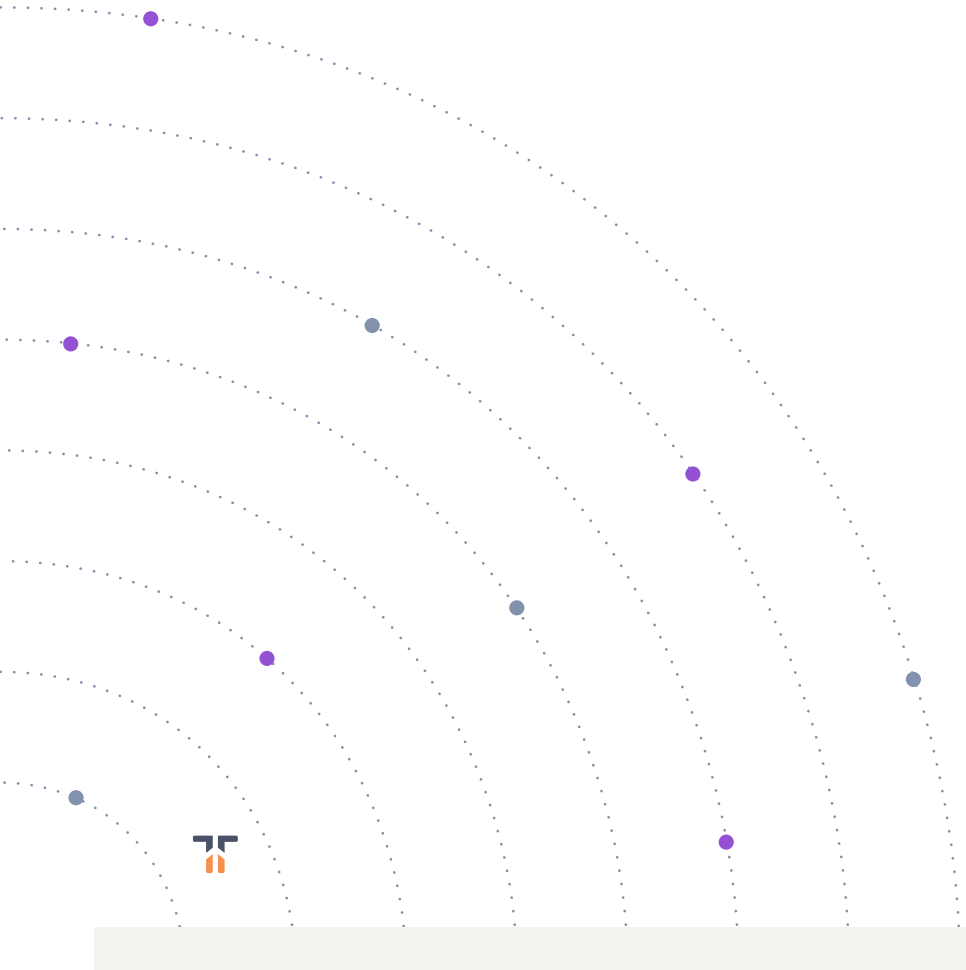
FINDING #6

Only 37% of organizations are aware of new government software supply chain requirements around security and SBOMs

HEADLINES

37% of organizations are aware of the White House executive order on cybersecurity.

Many of these respondents (42%) report current software supply chain security incidents like SolarWinds have had a large or extremely large impact on how their organization approaches application security.



In May of last year, the White House released an executive order on improving the nation's cybersecurity, in part influenced by the software supply chain vulnerability that impacted SolarWinds and its customers, including many in the United States government. The executive order was seen by some as a strategy to use the purchasing power of the government to improve the way cybersecurity is addressed around the world.

Over the past year, the executive order has increased momentum inside and outside of government around the importance of applications having up-to-date software bills of materials (SBOMs) and has technology leaders asking themselves tough questions about how they can improve the health and security of the open source software supply chain.

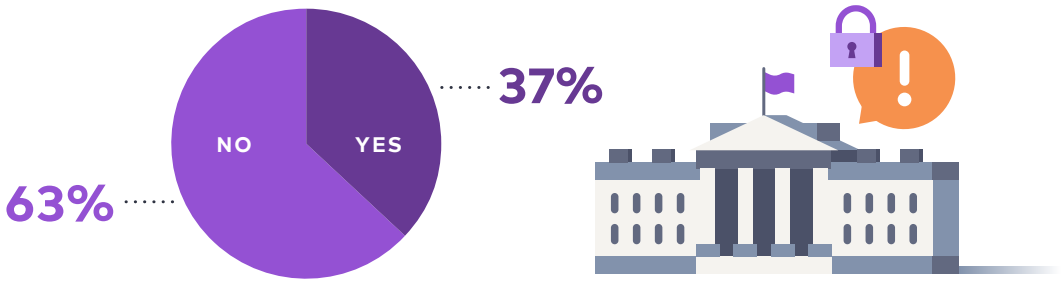
Many organizations are now investigating how to document and maintain an SBOM for their software applications, and they are also researching how to meet other requirements like attesting to the security and provenance of the open source software they are shipping as part of their products.

In this year's survey, we wanted to see if there was broad awareness around the White House executive order on cybersecurity and some of the requirements it imposes on organizations.

Just over one third of respondents (37%) were aware of the executive order while almost two thirds (63%) were not.

Only 37% of organizations are aware of the White House executive order on cybersecurity

Before this survey, were you aware of the May 2021 White House executive order on cybersecurity?



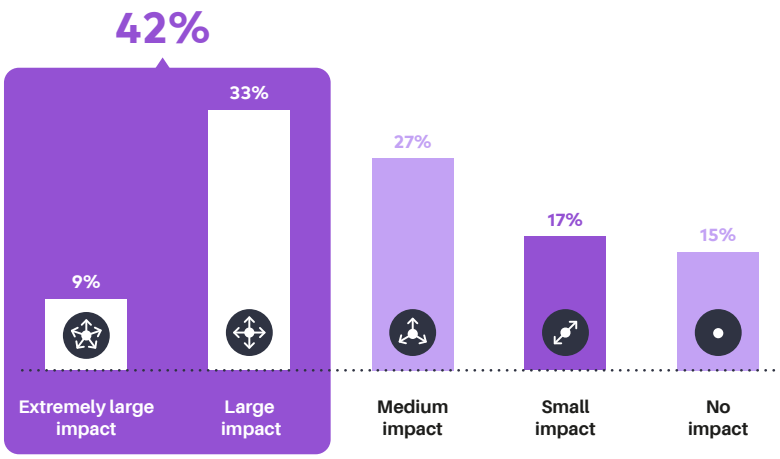
n=631 | respondents were shown the following text: "A May 2021 White House executive order on cybersecurity

We also wanted to see if their organizations' approach to managing application security has been impacted by recent software supply chain security events like the SolarWinds attack, so we asked this as a follow up question to those respondents aware of the White House executive order on cybersecurity.

Not surprisingly, of these organizations, 42% report that current software supply chain security events like SolarWinds are having a large or extremely large impact on how they approach application security. Only 15% of organizations see no impact at all.

42% percent of organizations report that current software supply chain security events like SolarWinds are having a large or extremely large impact on how they approach application security

If respondents were aware of the White House executive order on cybersecurity, they were asked the following question: Which of the following best describes the impact current events related to software supply chain security like the SolarWinds supply chain attack have had on how your organization approaches application security?



n=233

FINDING #7

78% of organizations are already using SBOMs for application development or have plans to in the next year

HEADLINES

SBOM

78% of organizations are already using SBOMs or have plans to in the next year.

Conversely, only 22% have no plans to use SBOMs.

In the largest organizations with over 10,000 employees, an even higher percentage of respondents (84%) are actively using SBOMs or plan to within the next year.

In our previous finding, we shared how the White House executive order on cybersecurity accelerated a conversation that was already happening in many organizations about the importance of creating and maintaining accurate software bills of materials (SBOMs).

As part of this year's survey, we wanted to understand more about how organizations are using SBOMs today. So we asked a follow up question to respondents who indicated they were familiar with the White House executive order on cybersecurity.

The vast majority of these respondents (78%) reported that they are already using SBOMs in some way or have plans to in the next year. Almost half (46%) already use them for a few, most, or all applications, while an additional 18% are piloting or actively evaluating in test environments. Only 22% of respondents have no plans to use SBOMs.

78% of organizations are already using SBOMs or have plans to in the next year

If respondents were aware of the U.S. May 2021 executive order on cybersecurity, they were asked the following question: Which of the following describe how your organization is currently using SBOMs for application development?

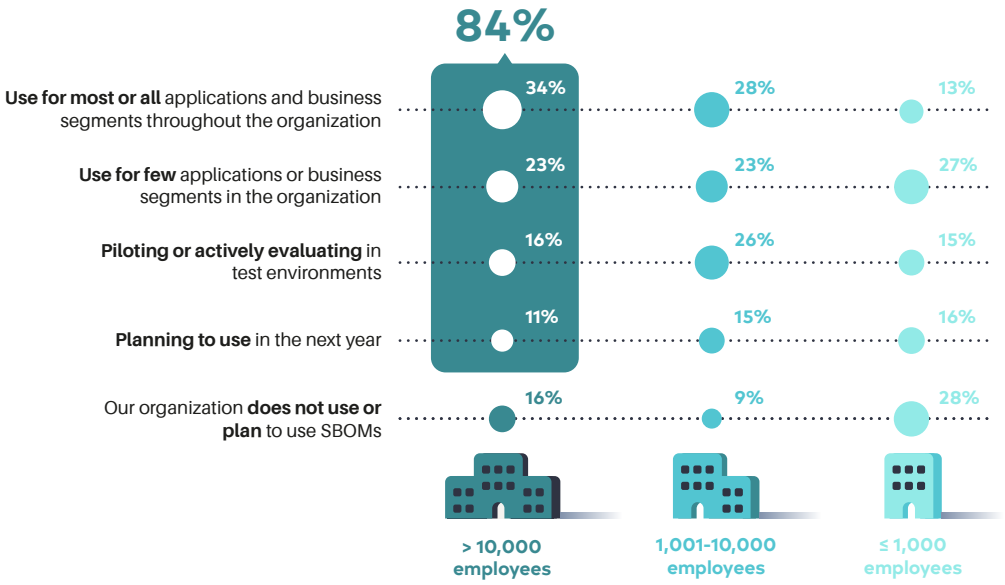
n=232 | the respondent was presented the following definition: "SBOMs are nested inventories that identify and list software components, information about those components, and supply chain relationships between them."

In the largest organizations with over 10,000 employees, an even higher percentage of respondents (84%) are actively using SBOMs or have plans to in the next year.

Meanwhile, 28% of the smallest organizations have no plans to use SBOMs, as compared to 16% in the largest organizations.

84% of the largest organizations are already using SBOMs or plan to in the next year

If respondents were aware of the U.S. May 2021 executive order on cybersecurity, they were asked the follow up question: Which of the following describe how your organization is currently using SBOMs for application development?



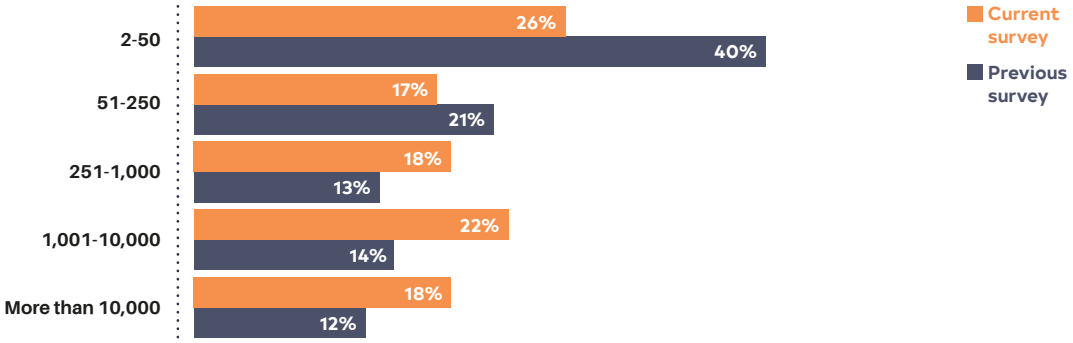
> 10,000 employees, n=142; 1,001-10,000 employees, n=47; ≤ 1,000 employees, n=44 | the respondent was presented the following definition: "SBOMs are nested inventories that identify and list software components, information about those components, and supply chain relationships between them."

This marks the fourth year Tidelift has conducted a survey to answer our most pressing questions for technologists using open source to develop applications. If you are interested in looking at previous reports, here's where you can download the 2020, 2019 and 2018 survey results, plus the groundbreaking 2021 open source maintainer survey.

Participants were contacted via Tidelift's email lists and social media. We screened respondents to make sure they were both employed and that they use open source to build applications at work. The full survey sample was 696 respondents. A t-shirt was offered as an incentive for participation.

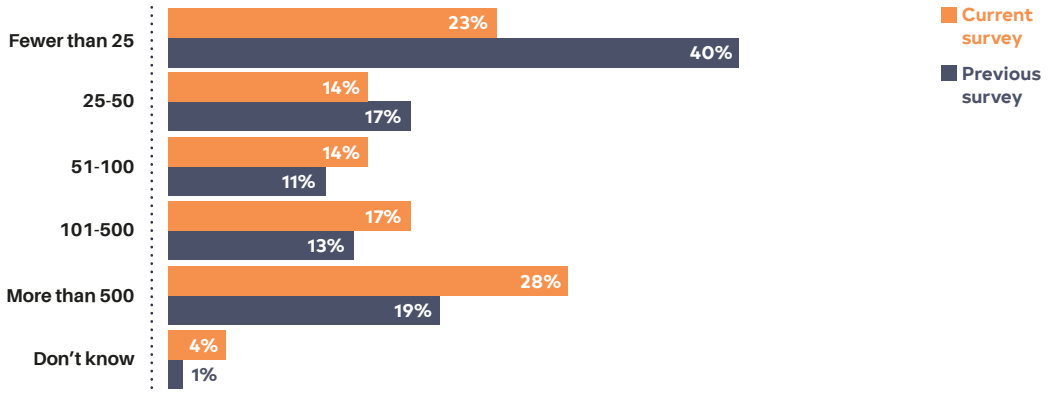
Here's more detail about the survey demographics, compared to our last technologist survey from 2020.

How many employees work for your organization?



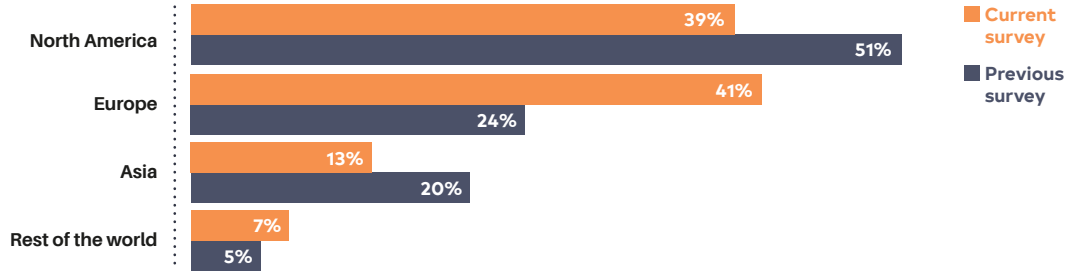
Current survey (Q4 2021) n=696; Previous survey (Q3 2020), n=477

How many people work in and around software development at your company?



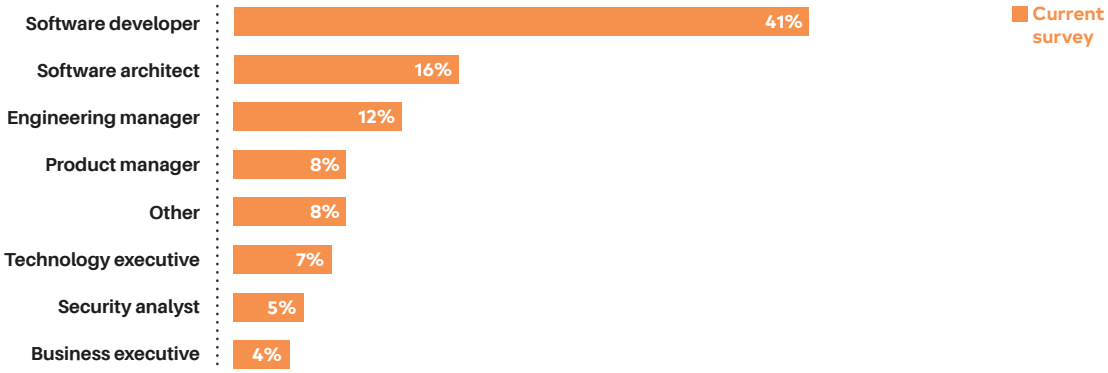
Current survey (Q4 2021) n=624; Previous survey (Q3 2020), n=476

What geographic region are you located in?



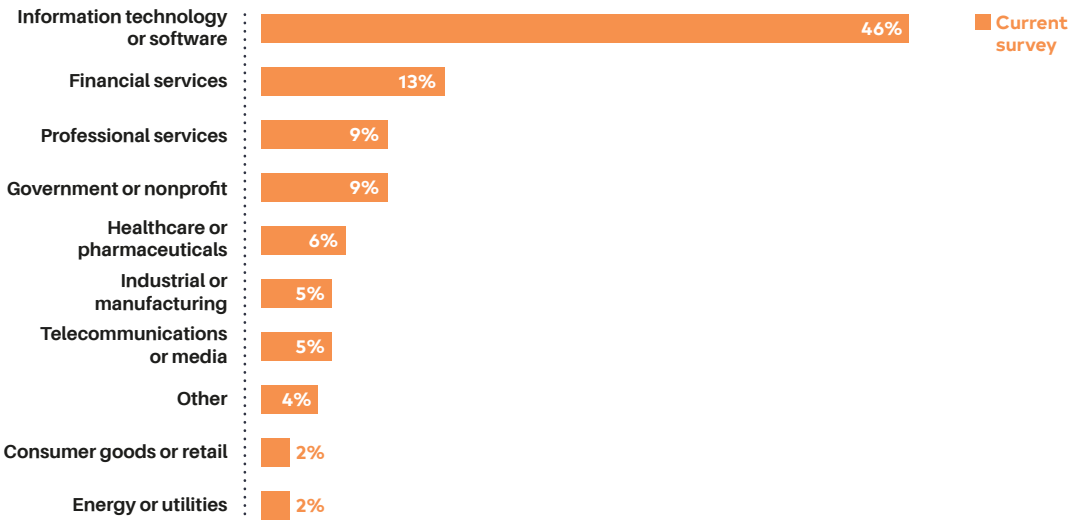
Current survey (Q4 2021) n=625; Previous survey (Q3 2020), n=477

Which job category most closely matches your role?

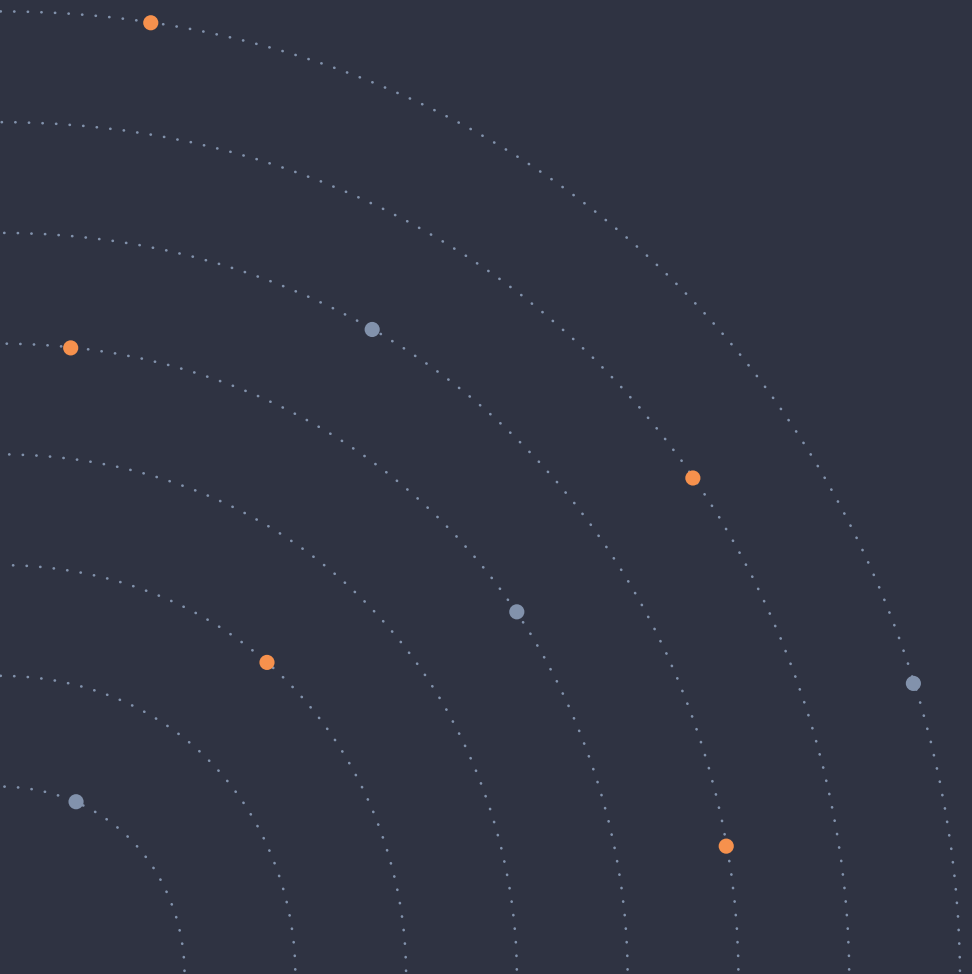


n=626

Which of the following best describes your enterprise's industry vertical?



n=625



TIDELIFT