Enterprise Strategy Group™
by TechTarget

The Growing Complexity of Securing the Software Supply Chain

Melinda Marks | Practice Director, Cybersecurity
ENTERPRISE STRATEGY GROUP

FEBRUARY 2024

Research Objectives

Software is increasingly composed of open source software (OSS), with the majority of organizations reporting it constitutes more than half of their code composition. While it saves time for developers when they can utilize existing third-party code to build and run their applications, security teams need to understand the software components to put the processes in place to secure the applications.

Consequently, many organizations are worried about having a high percentage of code that is open source, with some expressing concerns about the specific possibility of being victims of hackers targeting popular/commonly used OSS. Organizations are challenged with increased vulnerability across the software supply chain and with understanding how to effectively mitigate risk in light of recent targeted attacks. Organizations need effective software supply chain security solutions that can support the demands of cloud-native development.

To gain further insight into these trends, TechTarget's Enterprise Strategy Group surveyed 368 IT, cybersecurity, and application development professionals at organizations in North America (US and Canada) responsible for evaluating, purchasing, and utilizing developer-focused security products.

THIS STUDY SOUGHT TO:

Gauge the extent of current and expected third-party software components, including OSS, and the associated security implications.

Determine the impact of software supply chain attacks and the challenges victimized organizations have experienced responding to them.

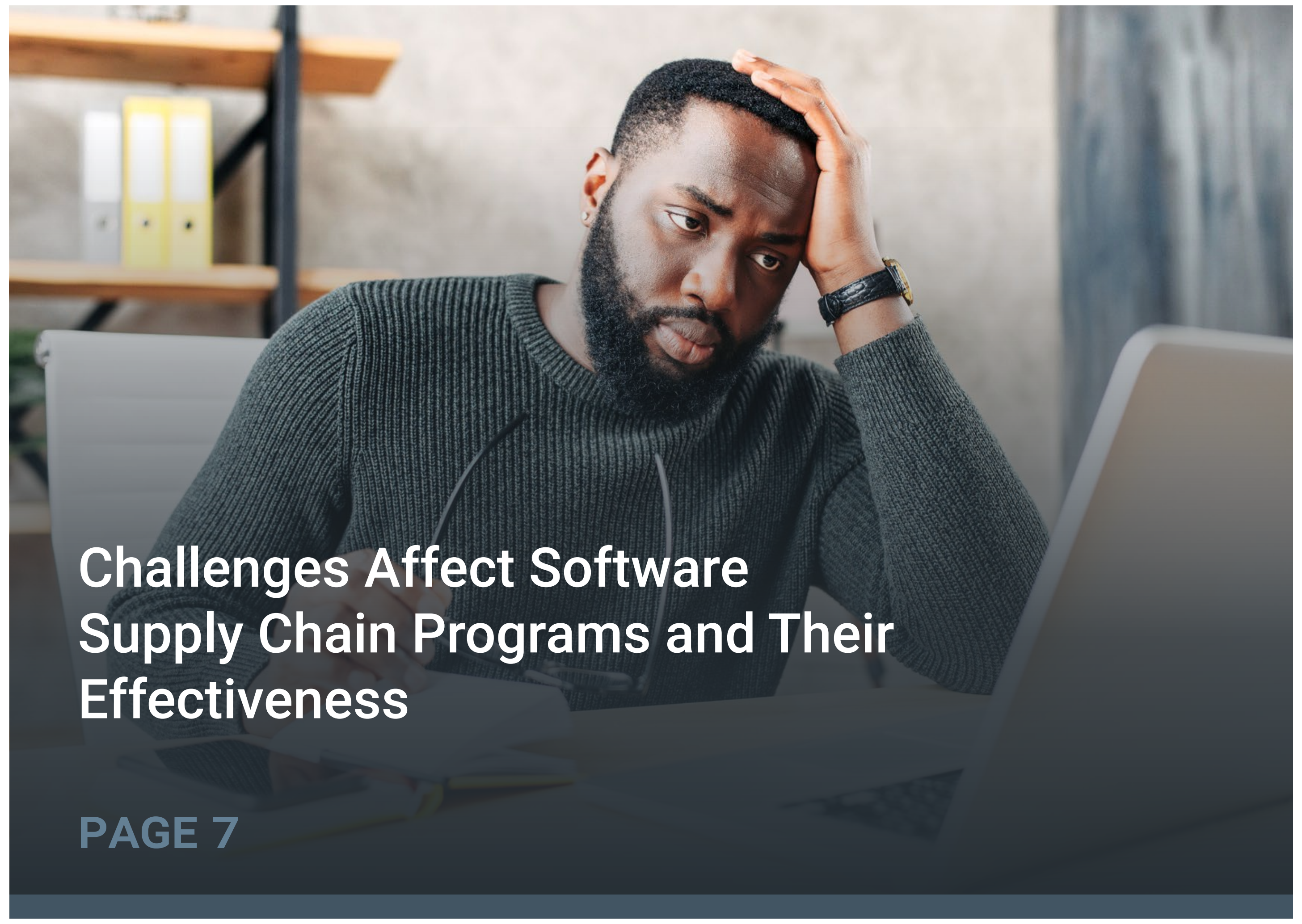
Establish the types of software supply chain security solutions currently in place, their effectiveness, and their integration with other application security tools.

Highlight the key stakeholders involved in selecting and purchasing software supply chain security solutions.

KEY FINDINGS

Software Supply Chain Complexity Rises With Third-party Code Components and Faster Development Cycles

PAGE 4



Challenges Affect Software Supply Chain Programs and Their Effectiveness

PAGE 7

OSS Security and SBOMs Present Obstacles

PAGE 11

Increasing Software Supply Chain Attacks and Threats Are Having Impacts

PAGE 16

Security and Development Teams Need to Collaborate for Software Supply Chain Security

PAGE 20

Investments Increase and Priorities Expand for Software Supply Chain Security

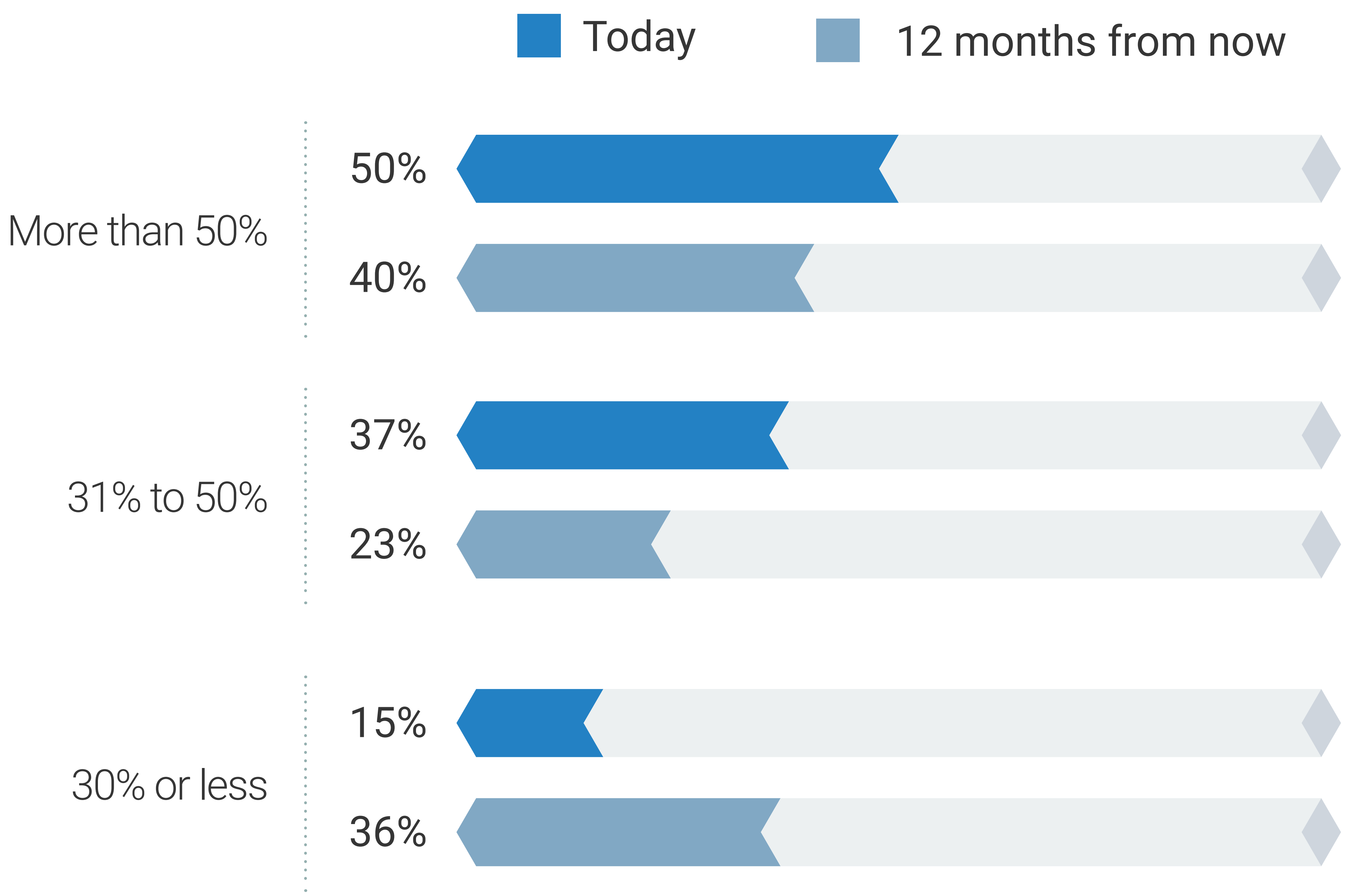
PAGE 23

Software Supply Chain Complexity Rises With Third-party Code Components and Faster Development Cycles

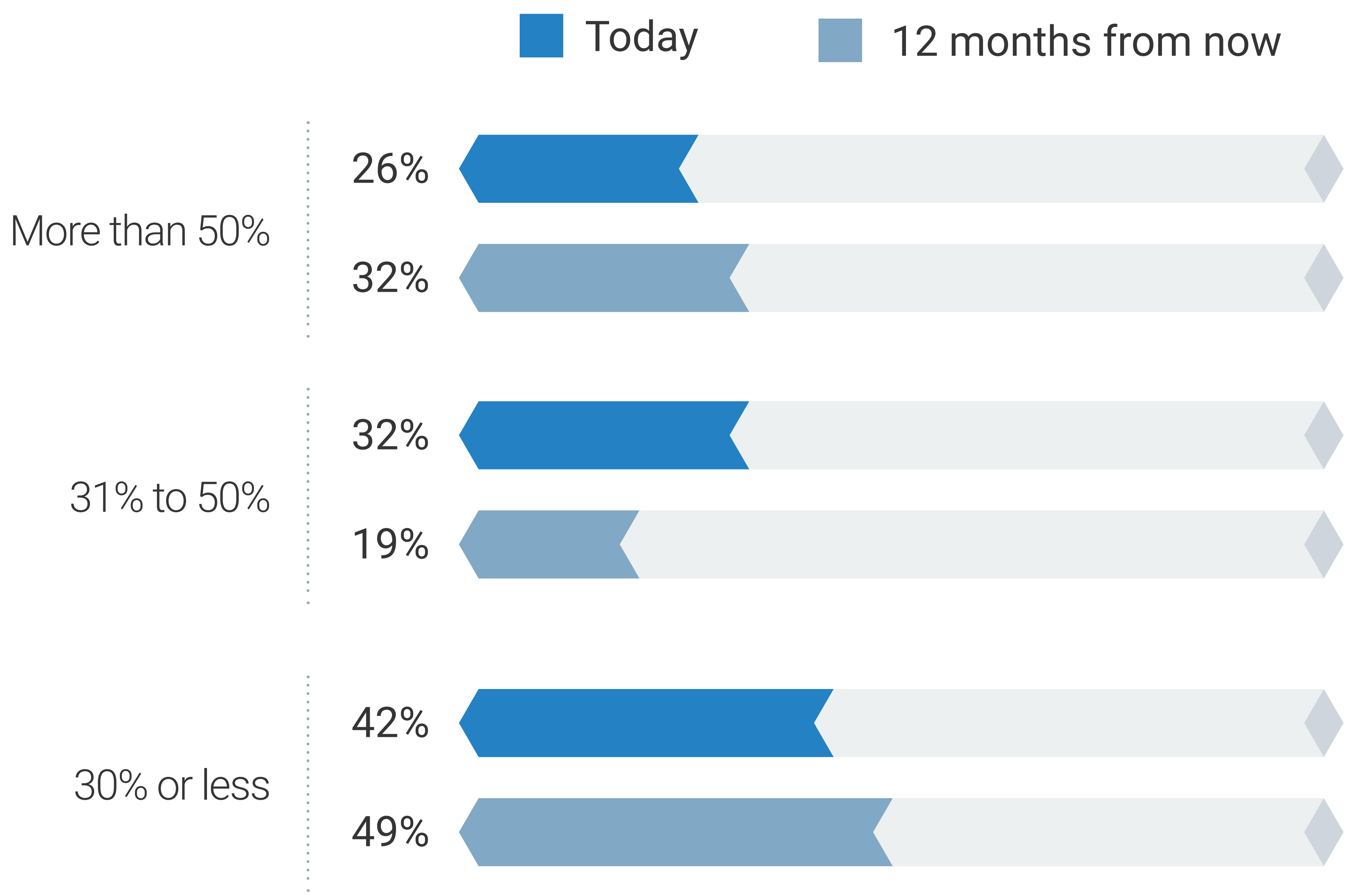
Increasing Third-party Code Composition and OSS Usage

As organizations are under increasing pressure to boost productivity, developers can save time by utilizing existing third-party code, including open source software (OSS), to build their applications. Today, 40% report that more than half of their code is composed of third-party software, compared with 50% of organizations that expect more than half their code to be composed of third-party software 12 months from now. In terms of OSS specifically, 58% of organizations expect that more than 30% of their code will be OSS, compared with only 51% exceeding the 30% threshold today.

Approximate percentage of total software code composition that is third-party code, including OSS.



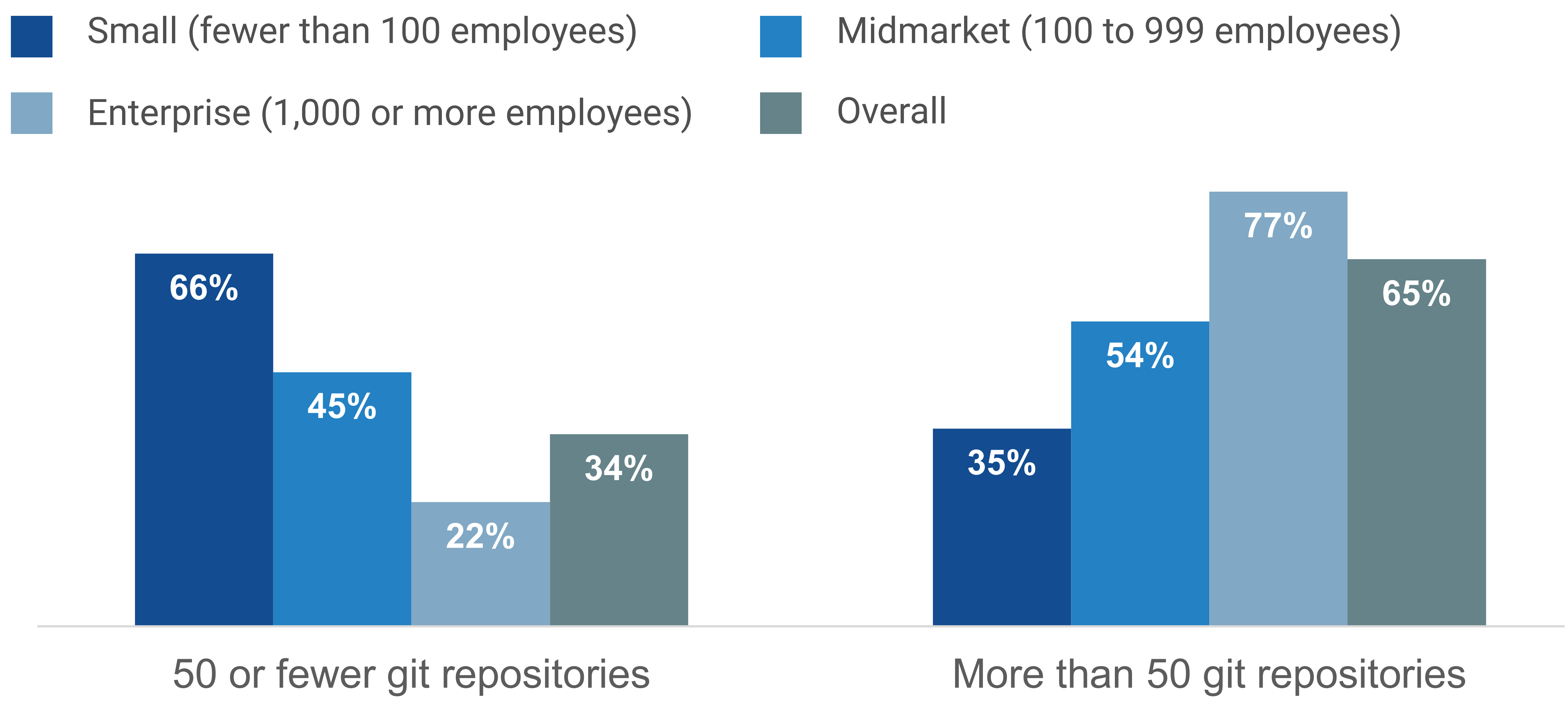
Approximate percentage of total software code composition that is OSS.



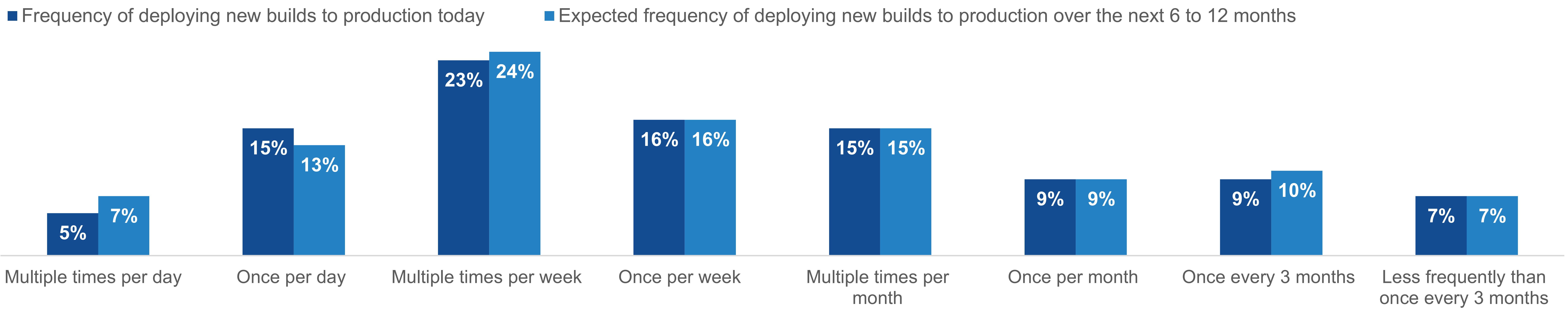
Issues of Scale Stemming From Frequent Releases and Numbers of Code Repositories

Cloud-native application development also enables developers to quickly release and update their applications because it is easy to deploy and update them on demand in the cloud with code pushes. Nearly half release new builds at least multiple times per week, marking a strong contrast to traditional application security with a longer amount of time to provision infrastructure and build an application, plus planned periodic updates. While this helps organizations efficiently deliver products that can be updated with new features and capabilities, it creates demands for security teams that need to ensure that each deployment does not introduce security vulnerabilities in the applications. The data also shows high numbers of code repositories. Even for small organizations (fewer than 100 employees), more than one-third (35%) exceed 50, while the percentage for midmarket (100-999 employees) and enterprise (1,000 or more employees) organizations is 54% and 77% respectively.

Estimated number of git repositories.



Average frequency with which new builds are delivered to production.



BACK TO CONTENTS

Challenges Affect Software Supply Chain Programs and Their Effectiveness

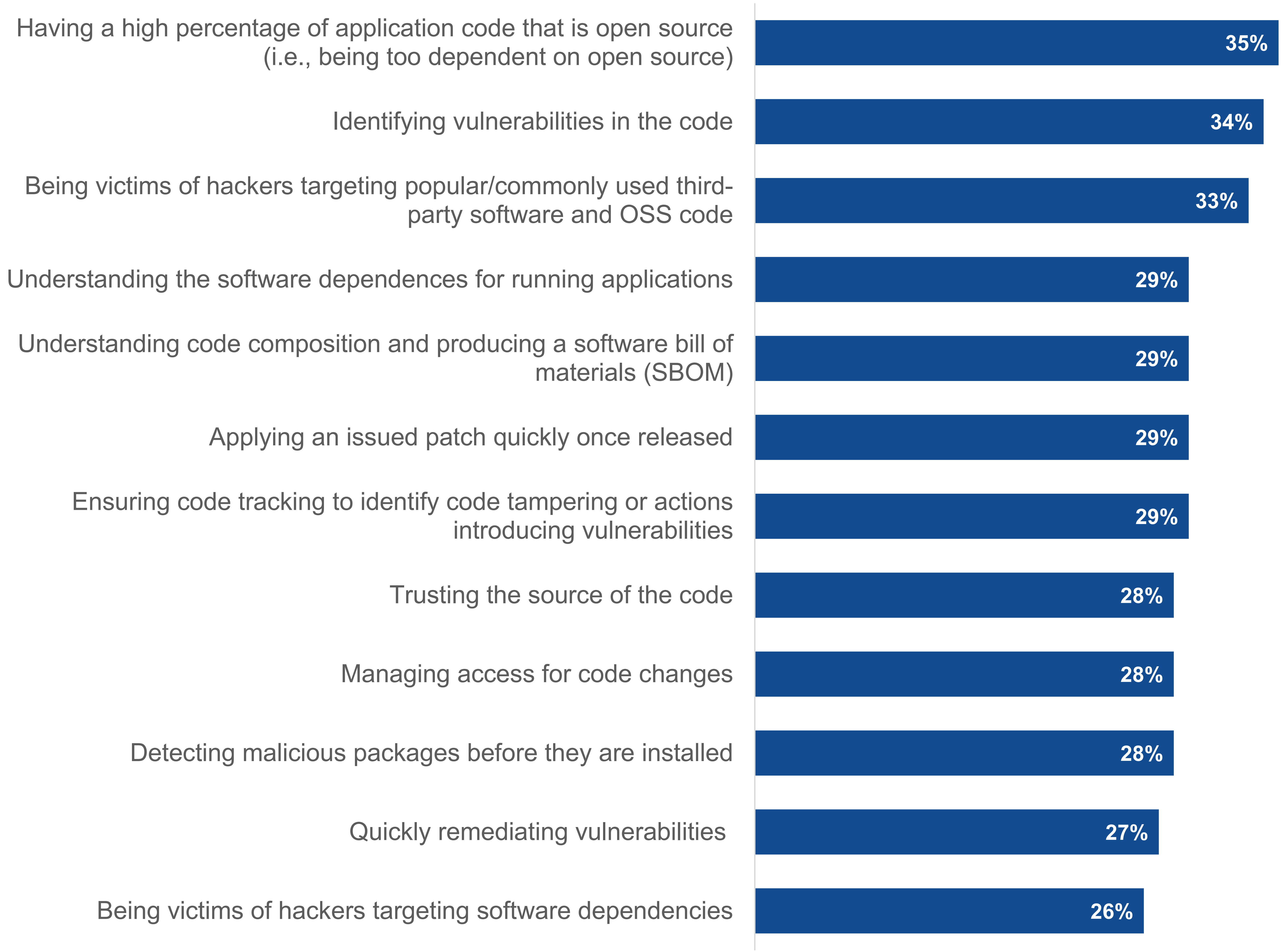
74%

We have a robust program with the **right processes and controls in place** to secure our software supply chain

Most Believe They Have Robust Software Supply Chain Security Capabilities, Though Challenges Persist

Despite nearly three-quarters (74%) of organizations saying they have “robust” software supply chain security capabilities, organizations report multiple challenges/concerns with using third-party software. Specifically, at least one-third of respondents identified being too dependent on open source, struggling to identify vulnerabilities in the OSS code, and/or being victims of hackers that target popular OSS code.

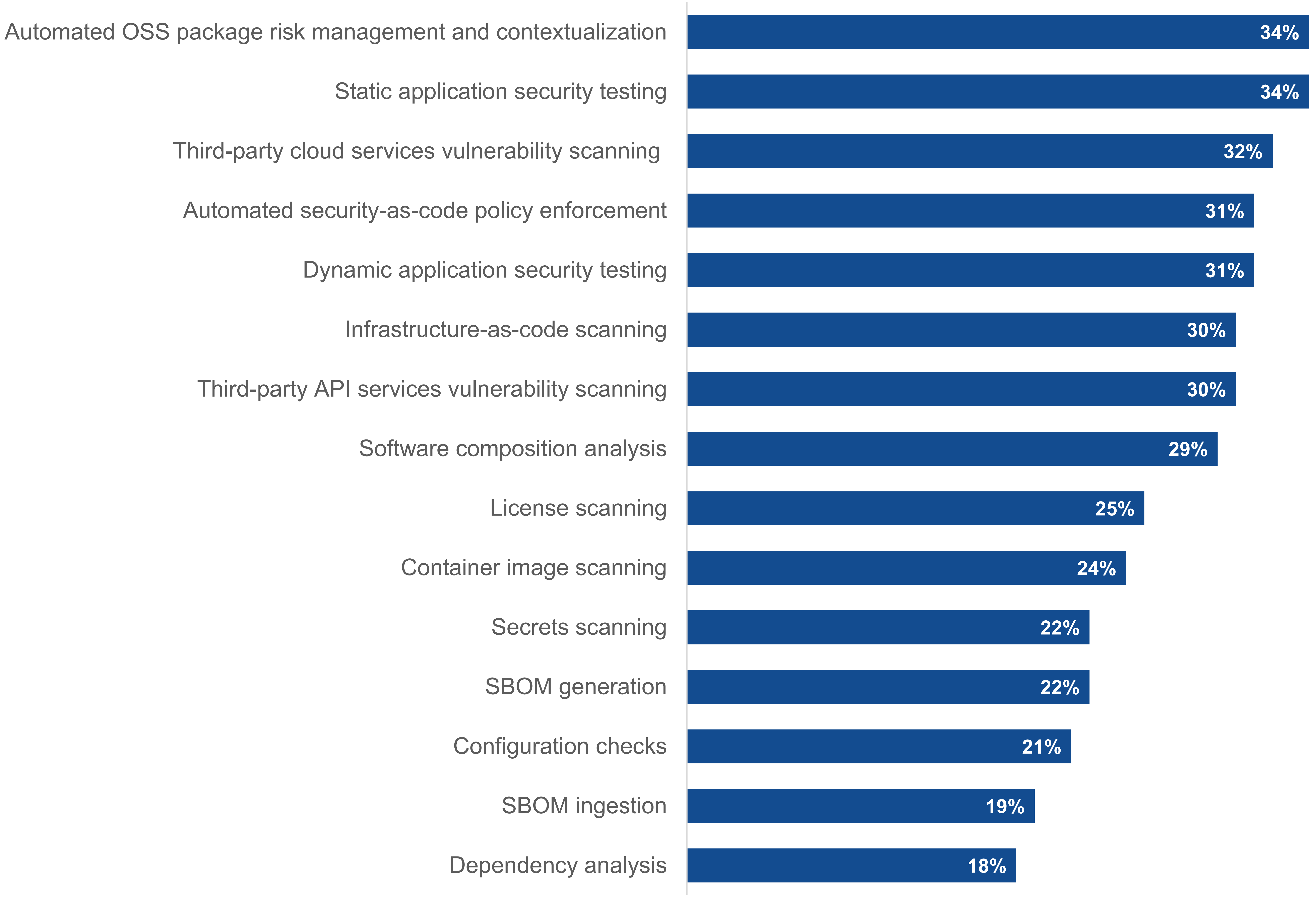
Challenges and concerns with using third-party software, including OSS.



Software Supply Chain Security Tools in Place

Organizations are using a wide variety of tools to address software supply chain security. While these are all important tools, the most commonly used are automated OSS package risk management, static application security testing, and vulnerability scanning for third-party cloud services. Currently, software bill of materials (SBOM) generation and ingestion, configuration checks, and dependency analysis are less frequently used, even though these are still important components of a comprehensive software supply chain program.

Tools used for software supply chain security.



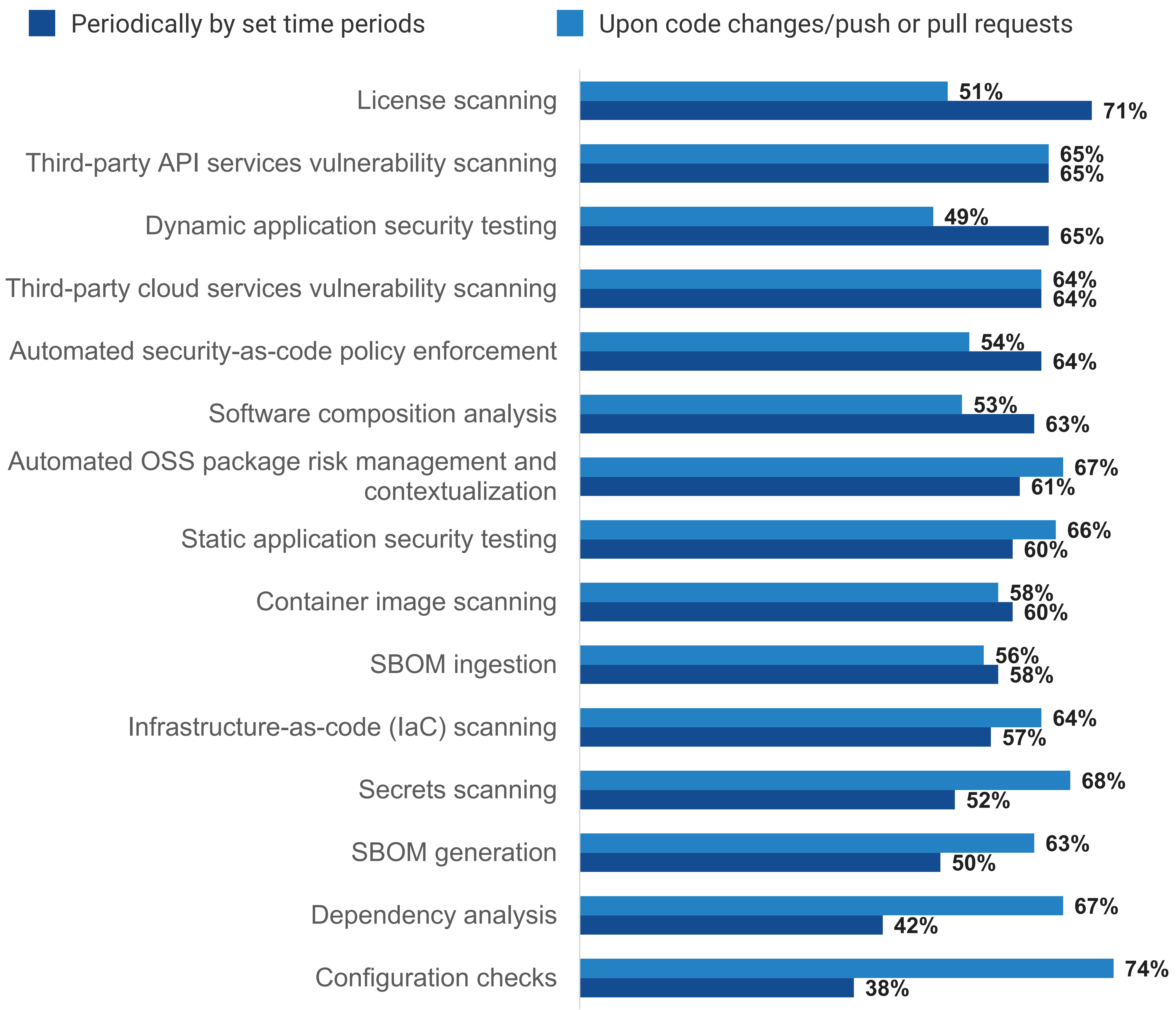
The Need to Optimize Efficiency of Security Processes in Development

Organizations need to look for ways to optimize efficiency as they incorporate security into their development processes to secure their software supply chain. Currently, organizations use tools both periodically by set time periods and upon code changes.

License scanning, dynamic application security testing, security-as-code policy enforcement, and software composition analysis are most commonly used upon code changes.

Secrets scanning, SBOM generation, dependency analysis, and configuration checks, on the other hand, are more often used periodically.

When tools for software supply chain security are used.



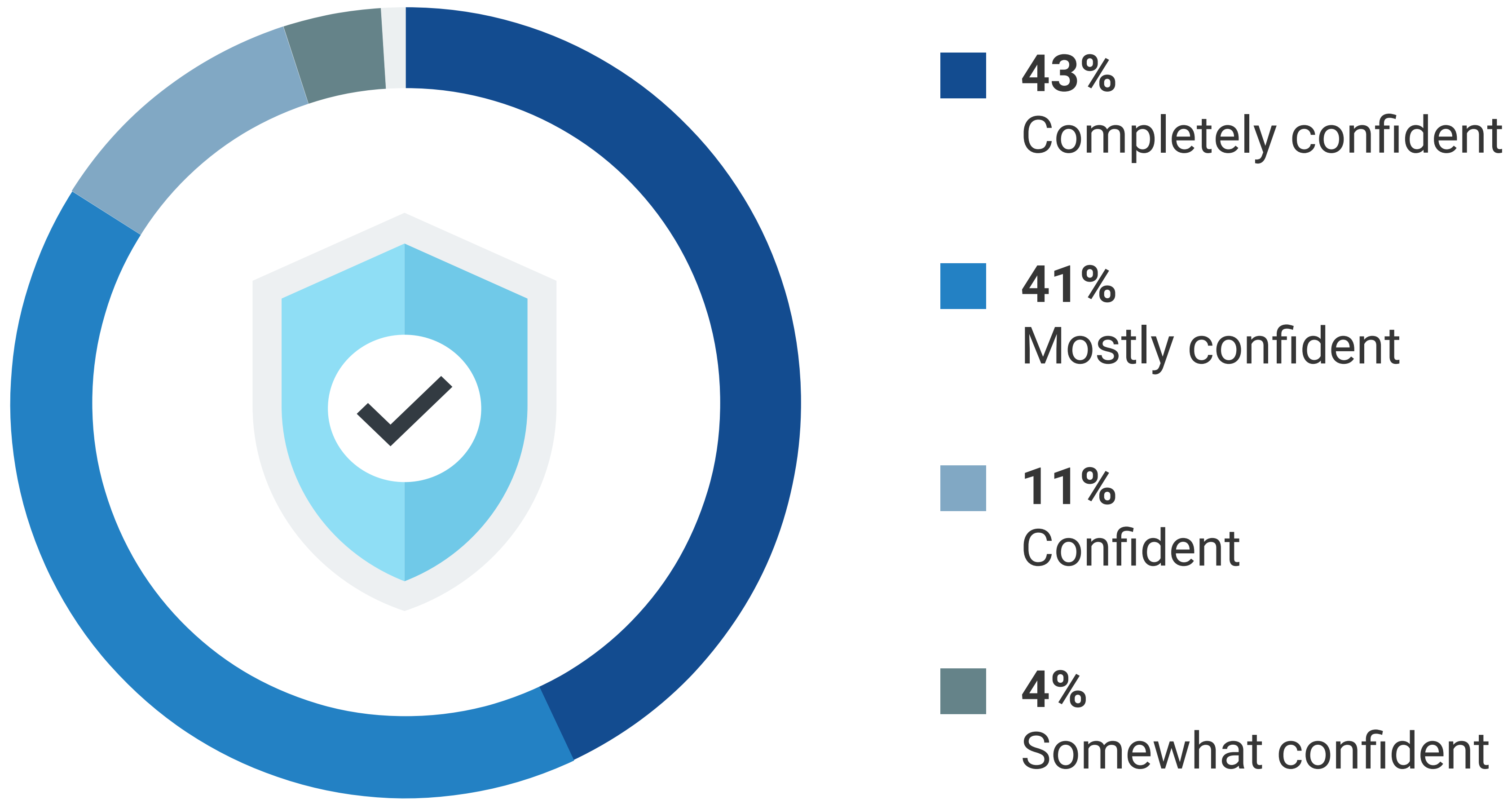
OSS Security and SBOMs Present Obstacles

OSS Security Assurances and Confidence

Given the pervasive usage of open source software, organizations are using multiple assurance processes/factors to determine the security of their OSS. The most commonly used among these include automated and manual governance processes, code signing, assurance frameworks, and the reliability of the code's source. Community efforts in this area help developers use code that they know is secure.

However, despite all these measures, only 43% of organizations report that they are *completely confident* that their developers are only using secure OSS, so there is much room for improvement.

Level of confidence that developers are only using secure OSS.



Factors or assurance processes used to determine the security of OSS.

44%	Governance process with automated analysis and policy enforcement
41%	Governance process with manual analysis
38%	Code signing for attribution and provenance
36%	Assurance frameworks
36%	The reliability of the vendor or source
32%	Frequency of releases/commits
32%	Whether the project has a responsible disclosure policy
30%	Vendor tools/ratings
29%	Information in the registry or package manager
29%	The security scorecard
28%	Whether the project has an active community
25%	Repository ratings

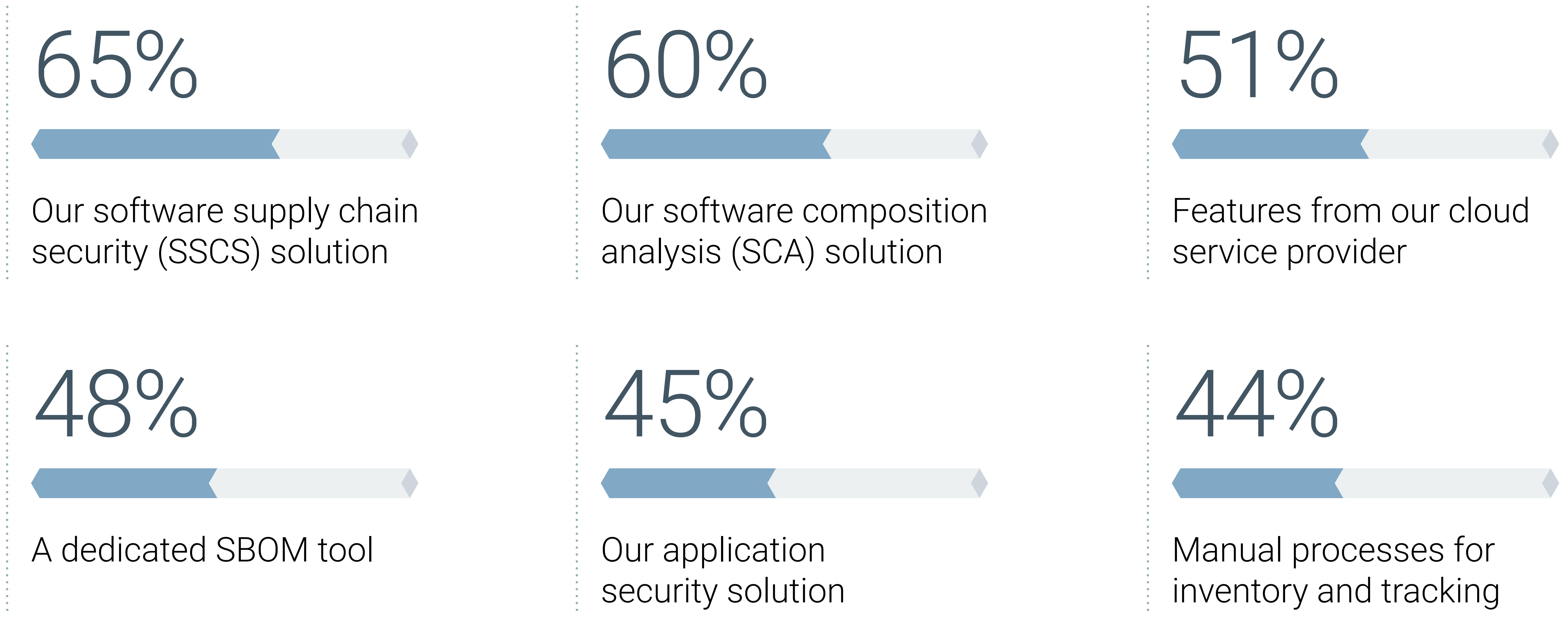
BACK TO CONTENTS

Few Are Using Tools to Generate SBOMs

Regulations increasingly call for software bills of materials to ensure software supply chain security. However, organizations are struggling to build accurate inventories of their software code composition. Indeed, as seen previously, only 22% of organizations are using an SBOM generation tool. Of those, only 48% currently generate an SBOM as a part of the application development process for all applications, while 49% do so on a case-by-case basis.

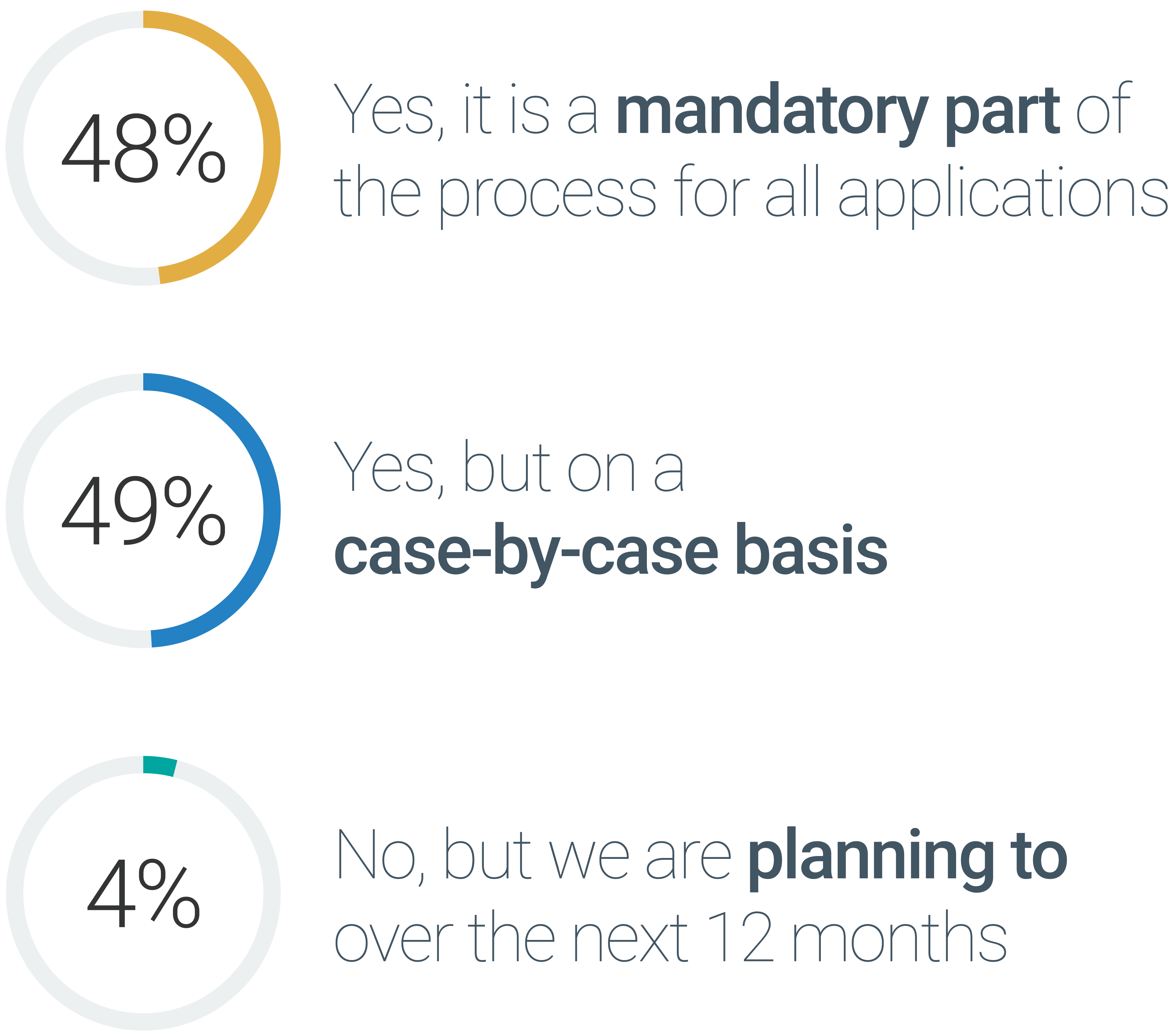
There are many options for organizations when it comes to SBOM generation. Indeed, the tools organizations are using may be from a software supply chain security solution, their software composition analysis solution, their cloud service provider, or their application security solution, or they could be dedicated SBOM tools. However, a staggering 44% use manual processes for inventory and tracking.

Tools or processes used to generate an SBOM.



> "**Only 22%** of organizations are currently using an SBOM generation tool."

Do organizations using an SBOM generation tool generate an SBOM as part of their application development processes?



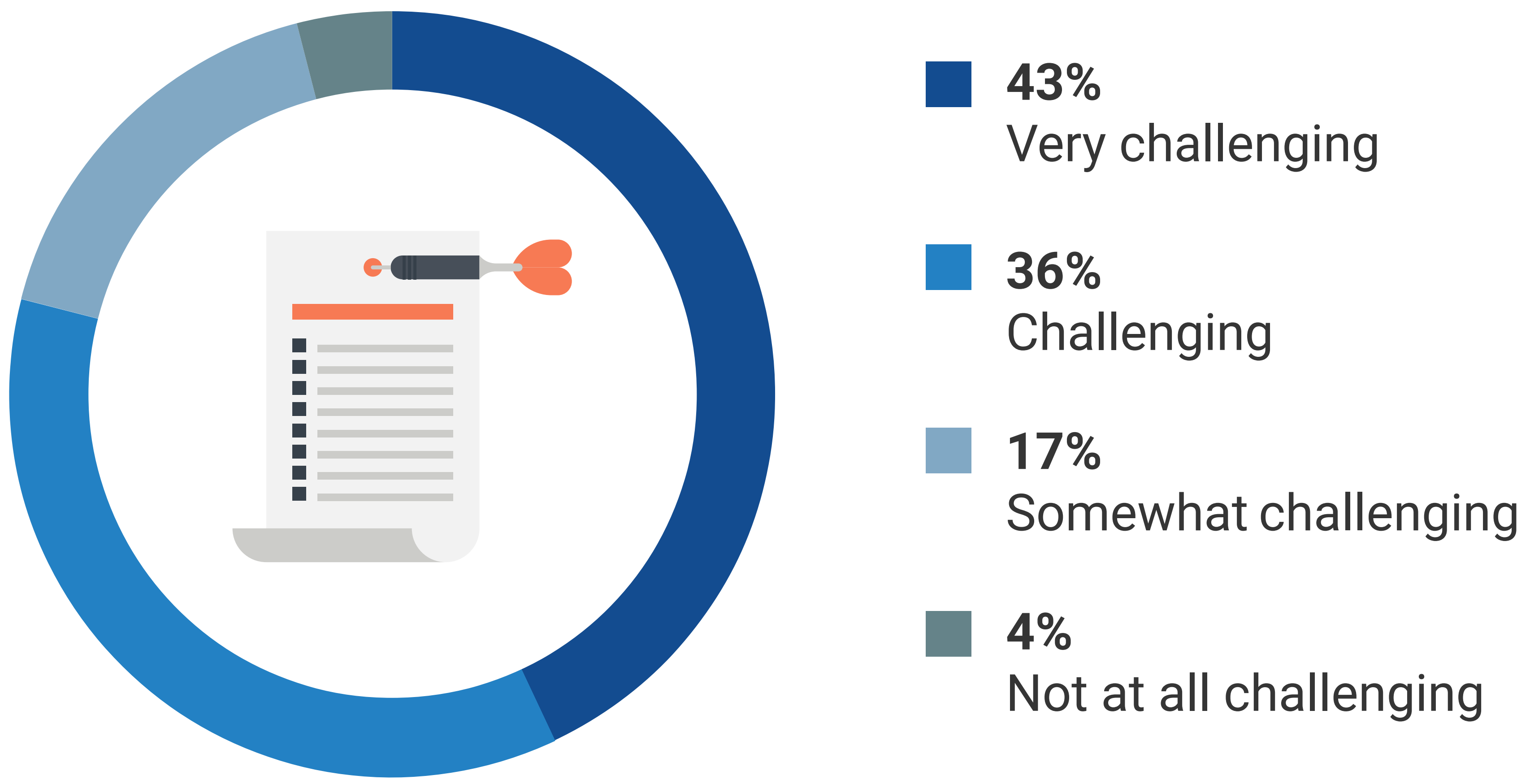
BACK TO CONTENTS

SBOMs Are Vital for Software Supply Chain Security, but They're Still Seen as Difficult to Generate

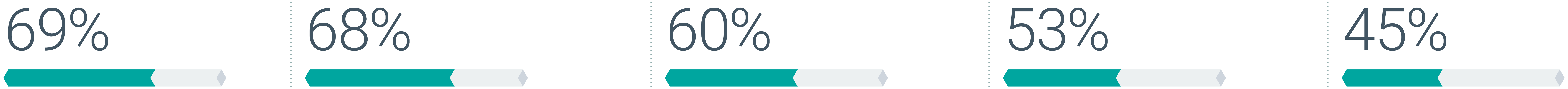
Those organizations generating SBOMs find it useful for managing software supply chain risk. From enabling the implementation of security controls to mitigate risk, through providing a comprehensive view of all potential issues across the supply chain, to helping to ensure compliance, the majority of organizations have realized multiple benefits from SBOMs.

Unfortunately, more than three-quarters of the organizations using tools to generate SBOMs find the process challenging (36%) or very challenging (43%). Organizations need to find better ways to incorporate SBOM generation into their application security programs.

Level of difficulty generating an SBOM.



How the use of SBOMs has affected the ability to manage software supply chain risk.



69% Enables us to implement security controls and processes to mitigate risk

68% Helps our customers understand the composition of our applications and prove that their security requirements have been met

60% Provides a comprehensive view of all the components and dependencies across the supply chain

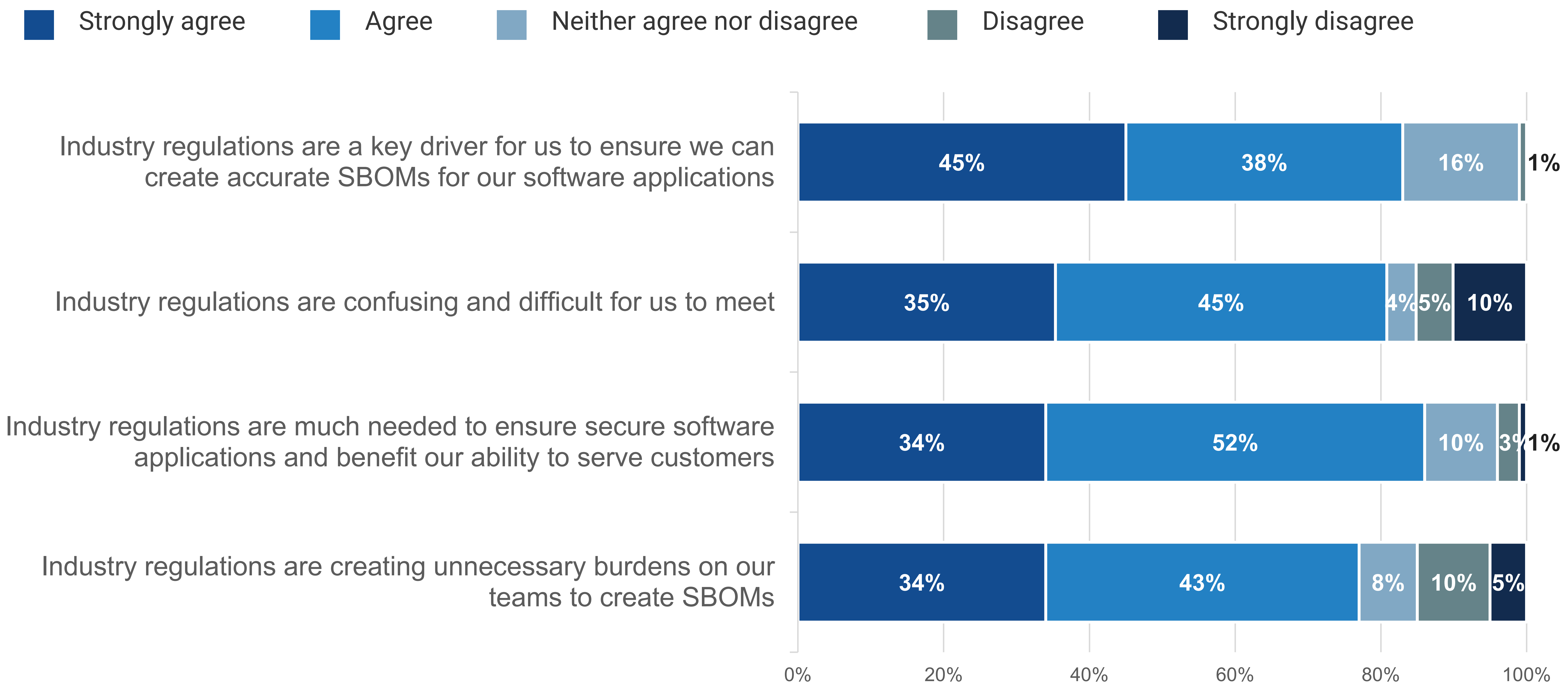
53% Enables more efficient vulnerability mitigation

45% Helps us meet compliance regulations

Industry Regulations Are Needed but Create Challenges

The research shows that governance and regulations are key drivers for software supply chain security programs, and SBOMs are often a key component. While organizations understand the need for industry regulations, they can nonetheless be confusing and difficult for organizations to meet while adding unnecessary burdens for security teams. This is why it is important for organizations to find the right tools to more easily generate SBOMs as part of the software development process.

Level of agreement with general statements about industry regulations requiring SBOMs to help address software supply chain risk.



> "While organizations understand the need for industry regulations, **they can nonetheless be confusing and difficult for organizations to meet** while adding unnecessary burdens for security teams."

Melinda Marks | Practice Director, Cybersecurity
ENTERPRISE STRATEGY GROUP

BACK TO CONTENTS

Increasing Software Supply Chain Attacks and Threats Are Having Impacts

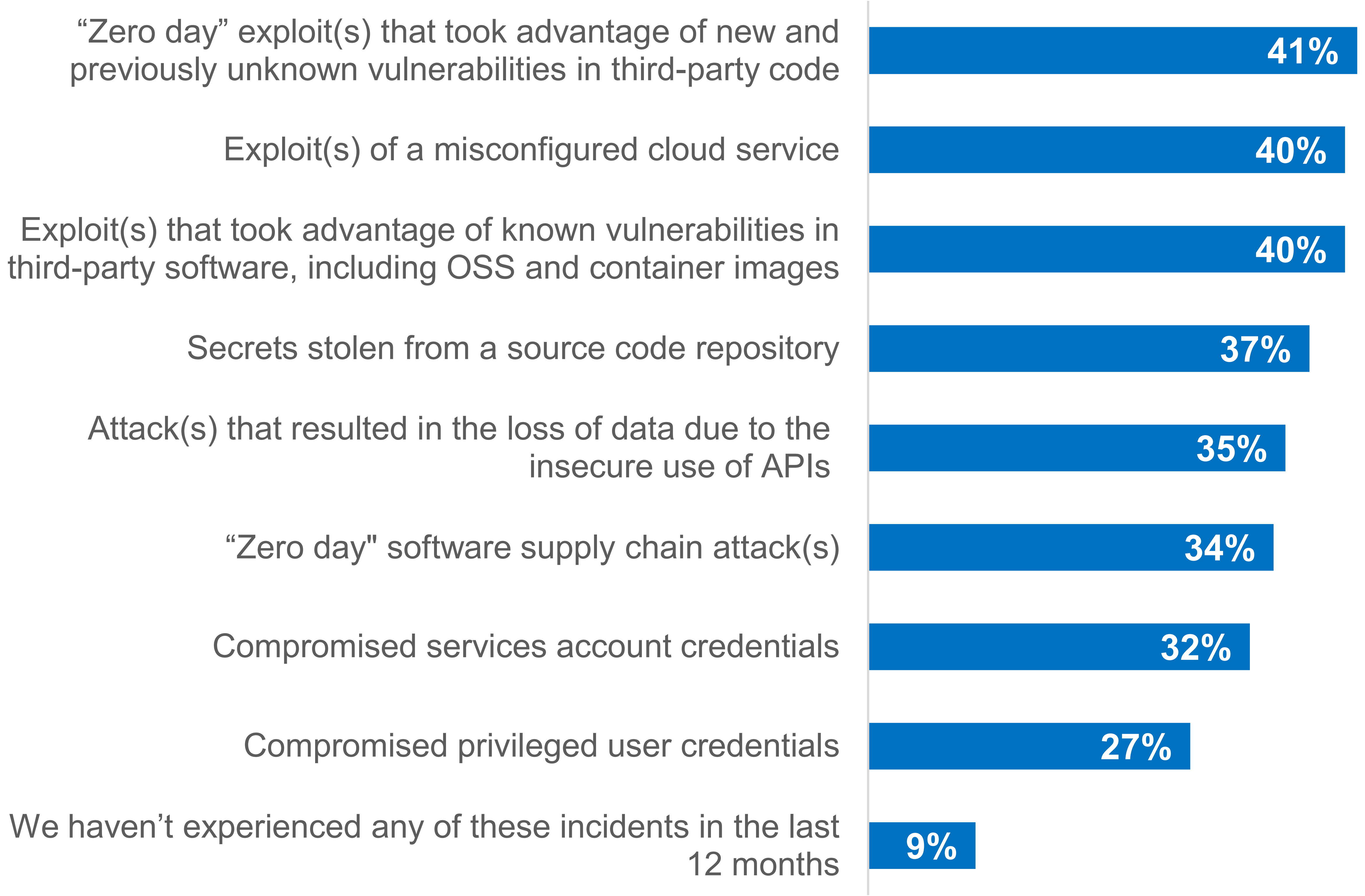
Software Supply Chain Incidents and the Subsequent Effects

The majority of organizations (91%) reported facing software supply incidents within the last year. At least four in ten pointed to exploitations of vulnerabilities in third-party code and/or misconfigured cloud services. Other incidents included stolen secrets from source code repositories, insecure use of APIs, and compromised user credentials.

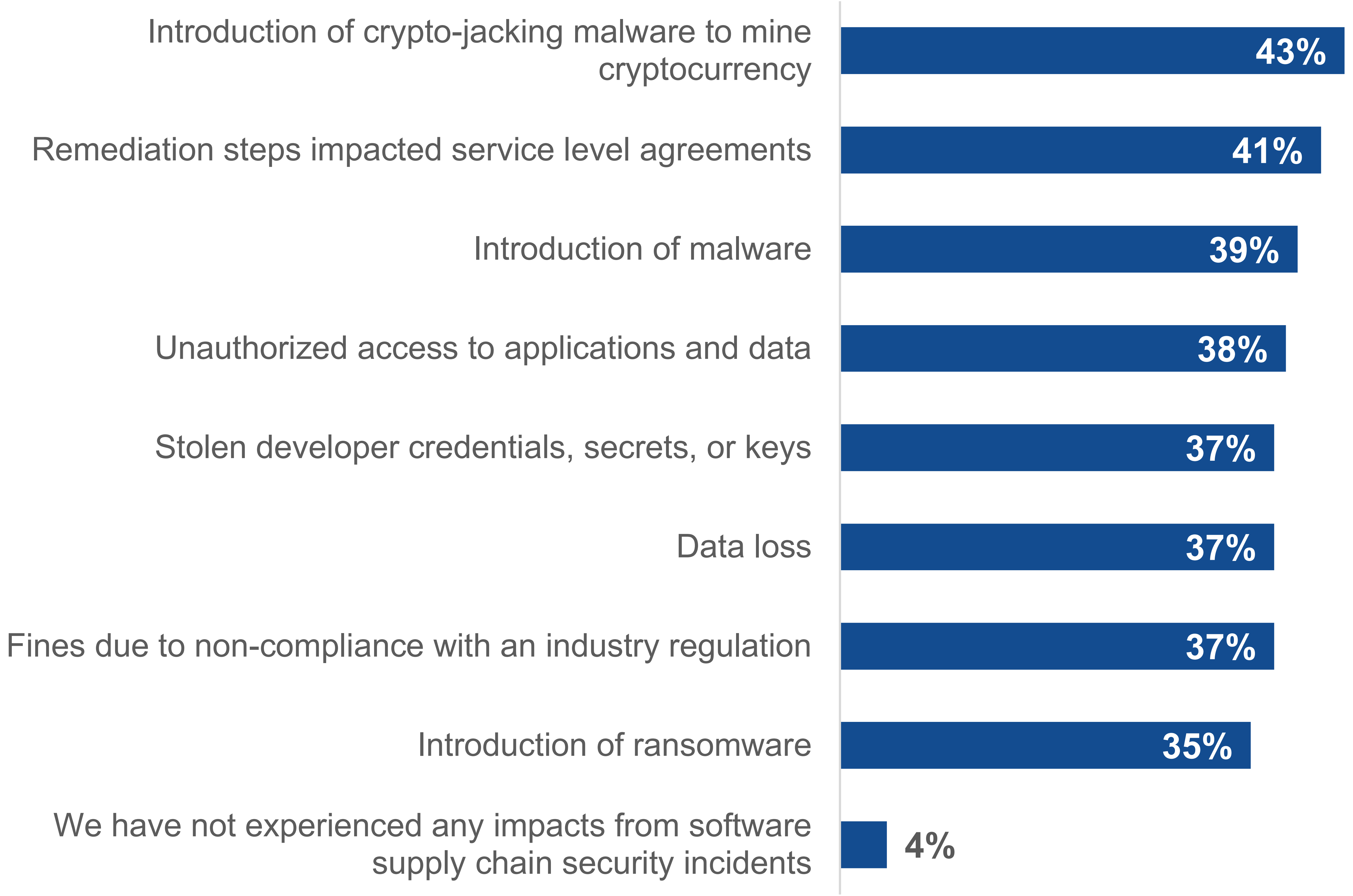
The range of these incidents shows the importance of efficiently detecting and remediating issues to minimize their potential impact.

Among those organizations that have experienced software supply chain incidents in the last 12 months, 96% suffered some kind of impact. The most commonly experienced effects included the introduction of crypto-jacking malware (43%) and SLAs being impacted by remediation steps (41%).

Types of software supply chain incidents experienced in the last 12 months.



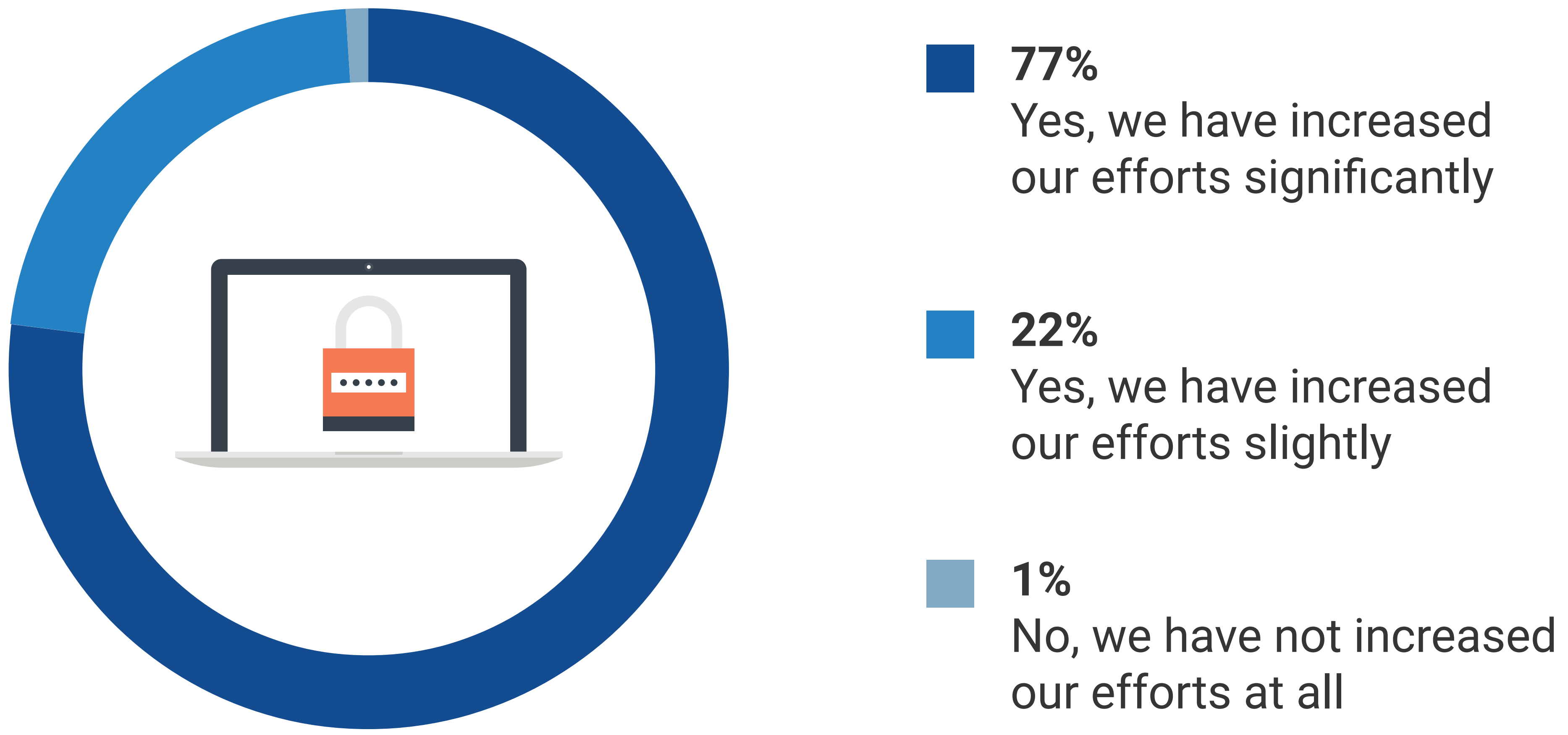
Impacts experienced from software supply chain security incidents.



Organizations Increase Efforts Following Attacks

Organizations report significantly increasing their efforts to secure third-party software components as a result of software supply chain attacks, especially when they are highly publicized attacks due to wide usage of vulnerable code. However, there is a range of measures taken, including adding detection rules, adopting authentication technology to catch access issues, implementing risk analysis, increasing monitoring, and performing security control assessments. Organizations need to optimize incorporating security processes throughout the software development lifecycle to efficiently address these issues and utilize blocking methods when attacks are detected.

Have organizations increased efforts to secure third-party software components, OSS, or container images as a result of software supply chain attacks?



Top five actions taken because of recent software supply chain attacks.

33%

Added new detection rules to security controls and/or security analytics systems

33%

Adopted some form of strong authentication technology like multifactor authentication for access to development environments and source code repositories

30%

Implemented preinstallation risk analysis of OSS packages

30%

Increased monitoring of runtime applications

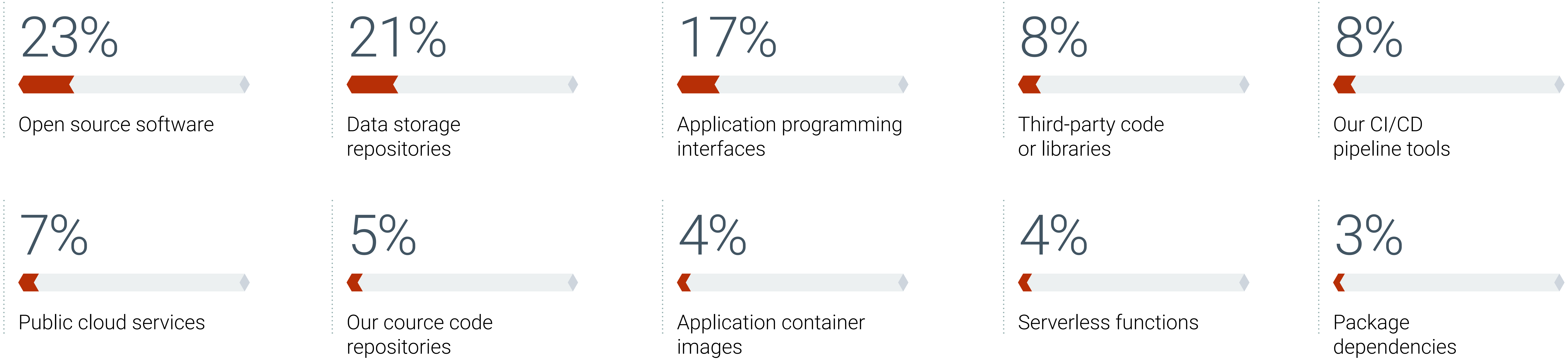
30%

Performed an assessment of current security controls to determine if they would prevent/ detect a similar type of attack

Software Supply Chain Elements Most Susceptible to Compromise

Organizations feel that a wide range of elements are susceptible to compromise, underscoring the complexity of finding an effective software supply chain security strategy. Among the most common perceived culprits are open source software, data storage repositories, and APIs.

Elements of the software supply chain most susceptible to compromise.



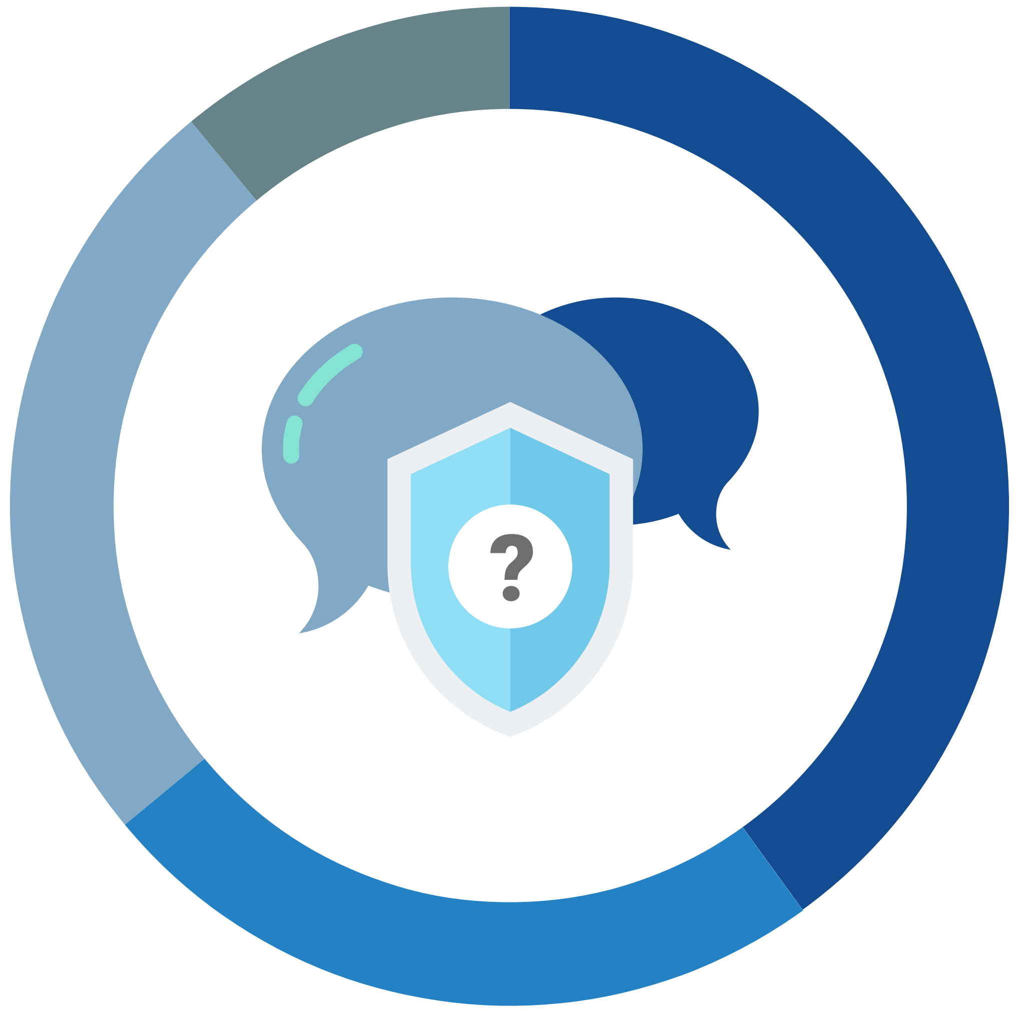
23%	Open source software
21%	Data storage repositories
17%	Application programming interfaces
8%	Third-party code or libraries
8%	Our CI/CD pipeline tools
7%	Public cloud services
5%	Our cource code repositories
4%	Application container images
4%	Serverless functions
3%	Package dependencies

Security and Development Teams Need to Collaborate for Software Supply Chain Security

Scaling Security by Enabling Developers to Fix Their Code

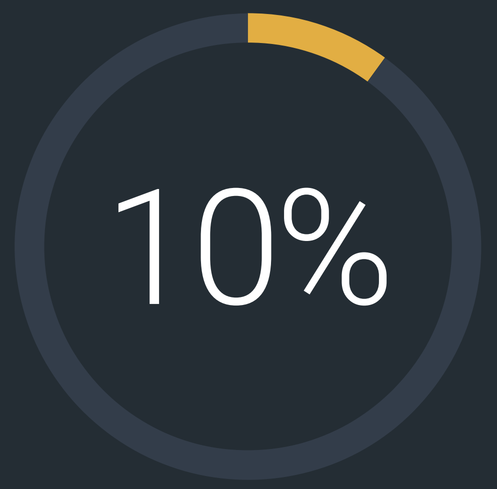
Security organizations realize the need to empower developers to efficiently fix code issues to mitigate application vulnerabilities. Indeed, most organizations are prioritizing this effort to “shift security left” to developers, with more than nine in ten identifying it as a high (39%) or top (52%) priority. The good news is that a majority of developers are completely (40%) or mostly (24%) comfortable taking on security responsibilities, with only 11% not comfortable taking on security responsibilities. And while the developers can be empowered to fix their own code, a majority of organizations report that security teams maintain significant influence over the security products and processes for developers. This enables security to have the control and visibility they need to drive efficient processes to mitigate risk and respond quickly to threats and attacks.

Developer sentiment toward taking on security responsibilities.

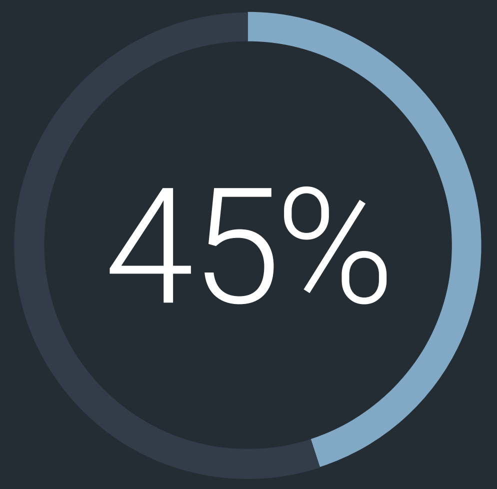


- ■ **40%** Completely comfortable with taking on security responsibilities
- ■ **24%** Mostly comfortable with taking on security responsibilities
- ■ **25%** Somewhat comfortable with taking on security responsibilities
- ■ **11%** Not at all comfortable with taking on security responsibilities

Priority level for developers securing their own code.

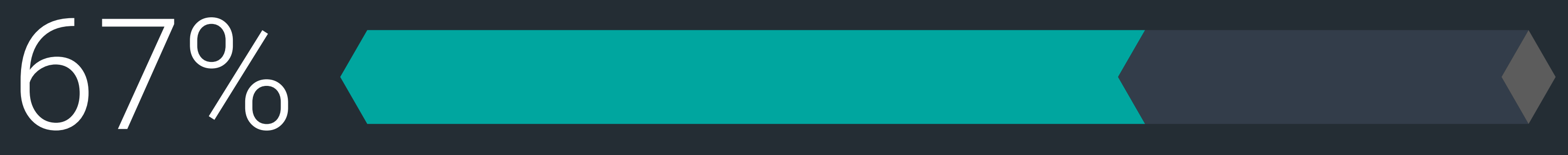


It’s our **top application security priority**



It’s a **high priority** (i.e., it will have a significant impact on our application security program)

Do security teams have influence over developer security products and processes?



Yes, security teams have **significant influence** over security products and processes for developers

BACK TO CONTENTS

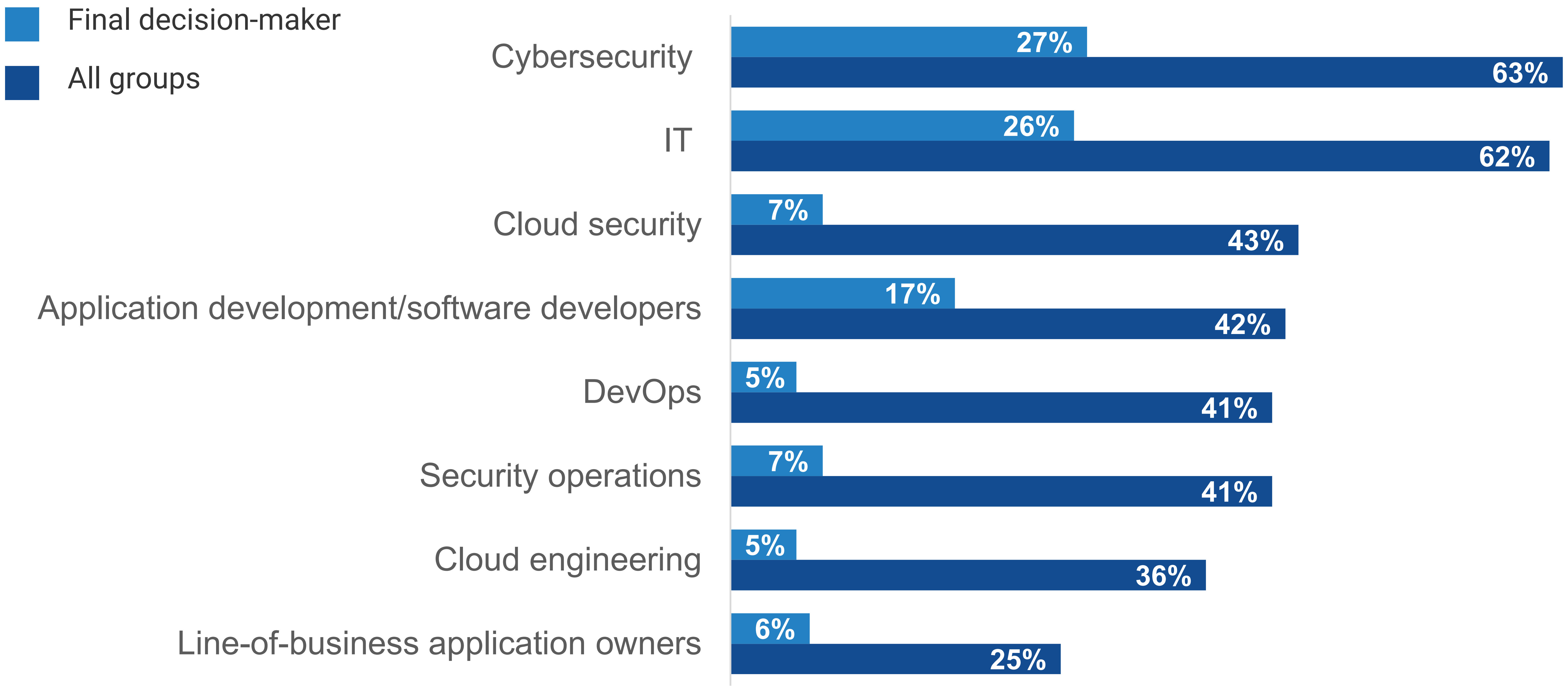
The Need for Collaboration Across Teams

The complexity of software supply chain security, including issues around third-party code, development processes, access, and authentication, requires coordination and alignment of objectives across teams.

Cybersecurity and IT are most often involved and are the final decision-makers for more than half of organizations.

But other teams are often involved in the evaluation processes, which is important to ensure that security can be efficiently incorporated into development processes without impacting productivity.

Groups involved with the evaluation processes and purchasing decisions for software supply chain security products or services.



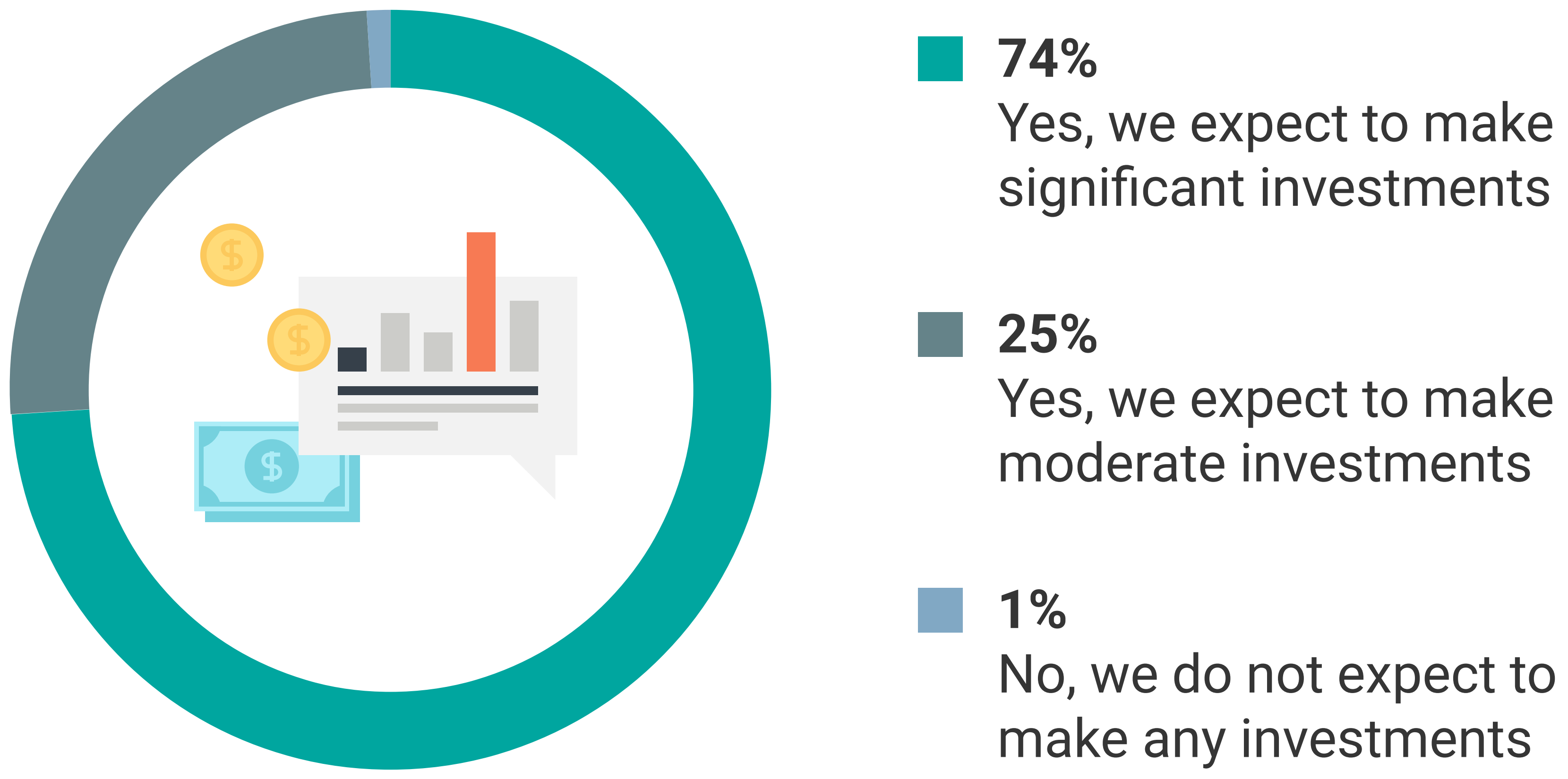
> “Cybersecurity and IT are **most often involved and are the final decision-makers** for more than half of organizations.”

Investments Increase and Priorities Expand for Software Supply Chain Security

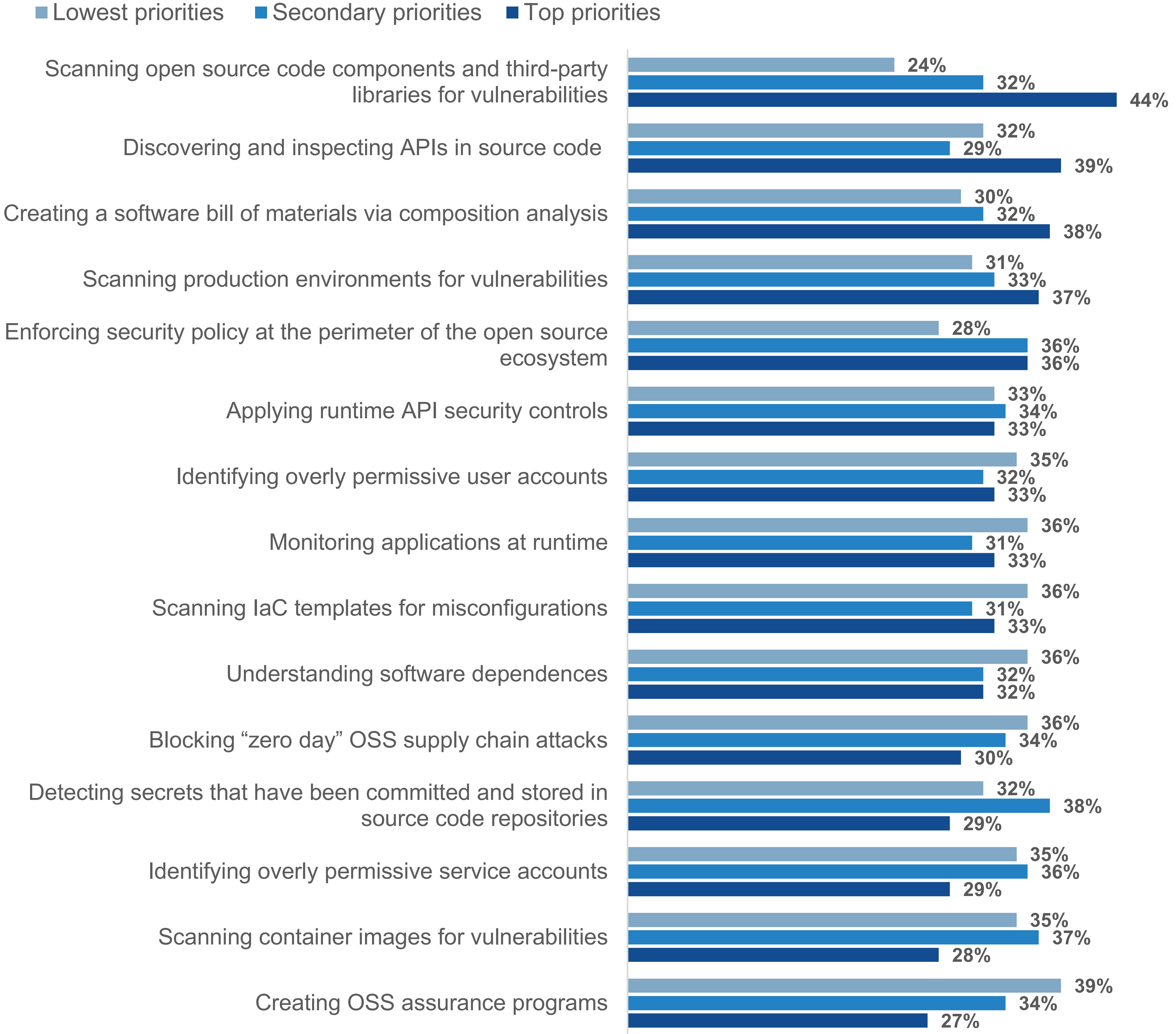
Significant Investments in Software Supply Chain Security

A majority of organizations (74%) are making significant investments in software supply chain security, with an additional 25% making moderate investments. However, due to its complexity, the spending priorities sprawl across a range of requirements, indicating a potential need for tools offering multiple capabilities. In terms of priorities, tools for testing and scanning, API discovery and inspection, and SBOMs are most commonly on spending radars for the next 12-18 months.

Do organizations plan on investing in software supply chain security?



Prioritization of software supply chain security investment areas over the next 12 to 18 months.



BACK TO CONTENTS

Goals for and Expected Benefits of Software Supply Chain Security

Organizations are also looking for a variety of benefits to justify their investments. These are common application security goals that should also align with software development goals of driving process efficiency, application availability and uptime, staff support, and cost savings. Organizations should look for solutions that drive efficiency across teams in the software development lifecycle (from pre-deployment to runtime), plus ways to rapidly respond in the case of threats or attacks.

Desired benefits from investing in software supply chain security solutions.

58%	Ability to fix code issues before applications are deployed into production
53%	Improved application uptime/availability
52%	Reduction in/avoidance of security incidents
52%	Fewer security issues detected in runtime
51%	Time savings for the security team
47%	Time savings for developers
46%	More actionable data to inform remediations
38%	Cost savings

> "Organizations should look for solutions **that drive efficiency across teams in the software development lifecycle** (from pre-deployment to runtime), plus ways to rapidly respond in the case of threats or attacks."

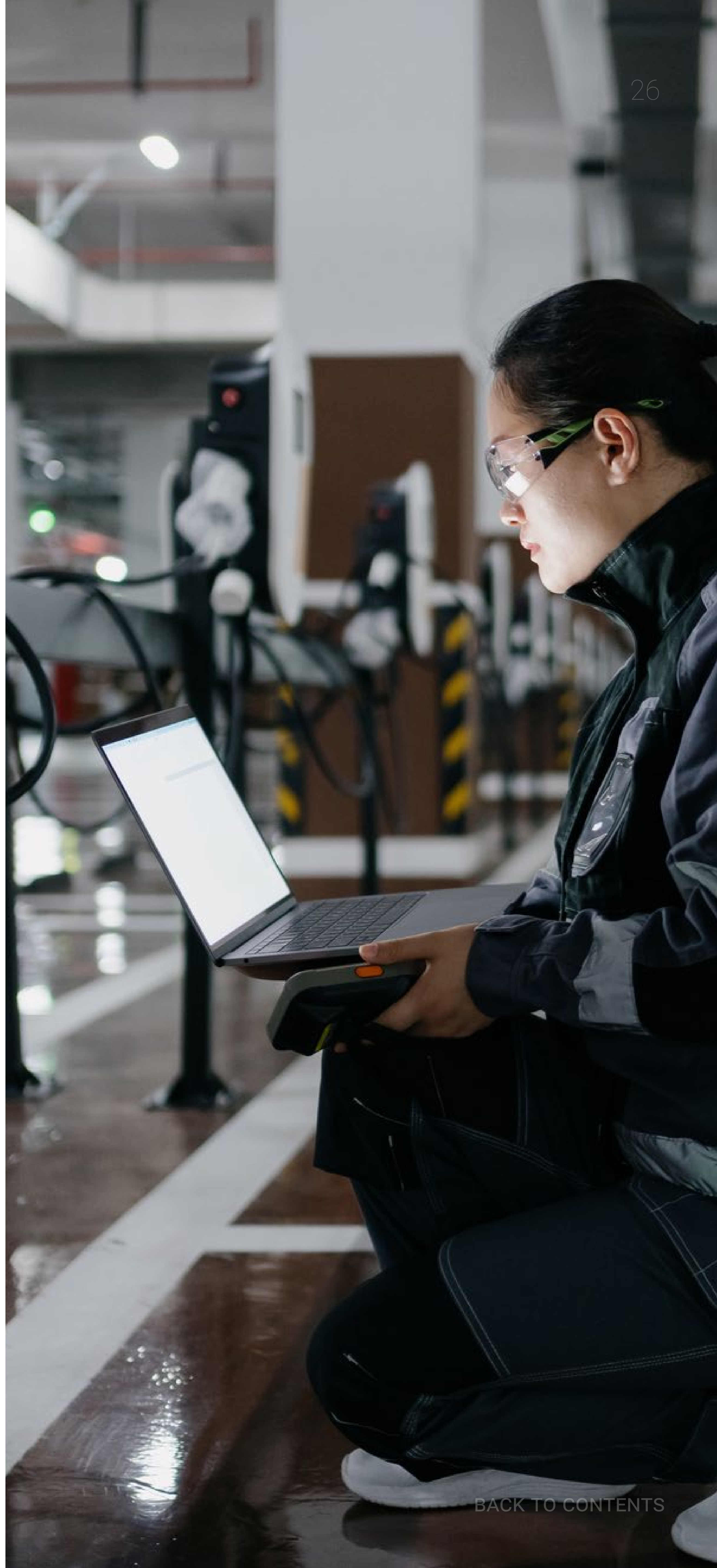
BACK TO CONTENTS

Phylum

ABOUT

Phylum is on a mission to secure the universe of code. Its platform automates software supply chain security to contextualize risks, block attacks and allow users to only use open-source code that they trust. The company is built by a team of career security researchers and developers with decades of experience in U.S. Intelligence Community and commercial sectors. Phylum is the winner of the Black Hat 2022 Innovation Spotlight Competition and was named a Top Infosec Innovator by Cyber Defense Magazine.

The Phylum Research Blog

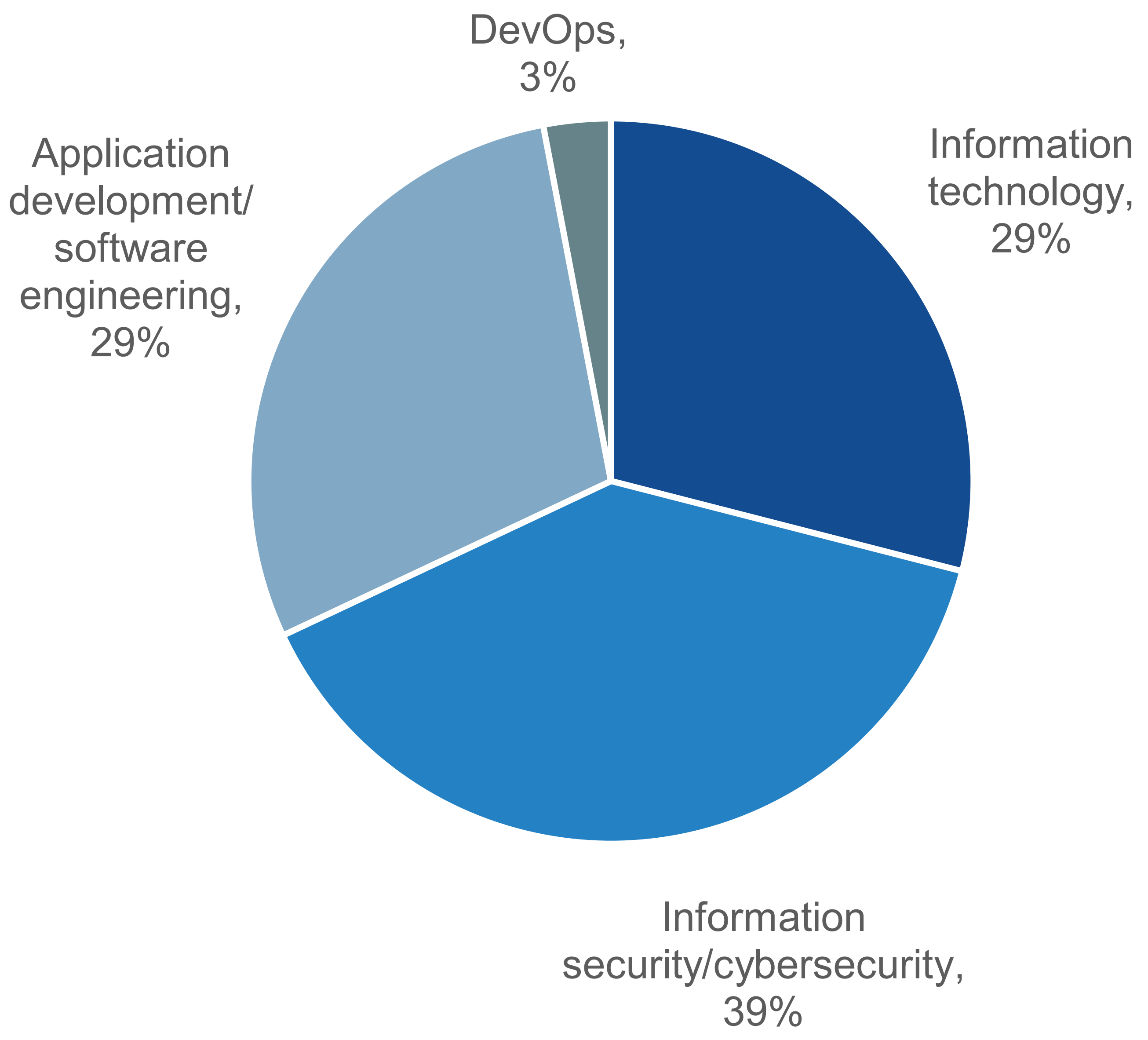


RESEARCH METHODOLOGY AND DEMOGRAPHICS

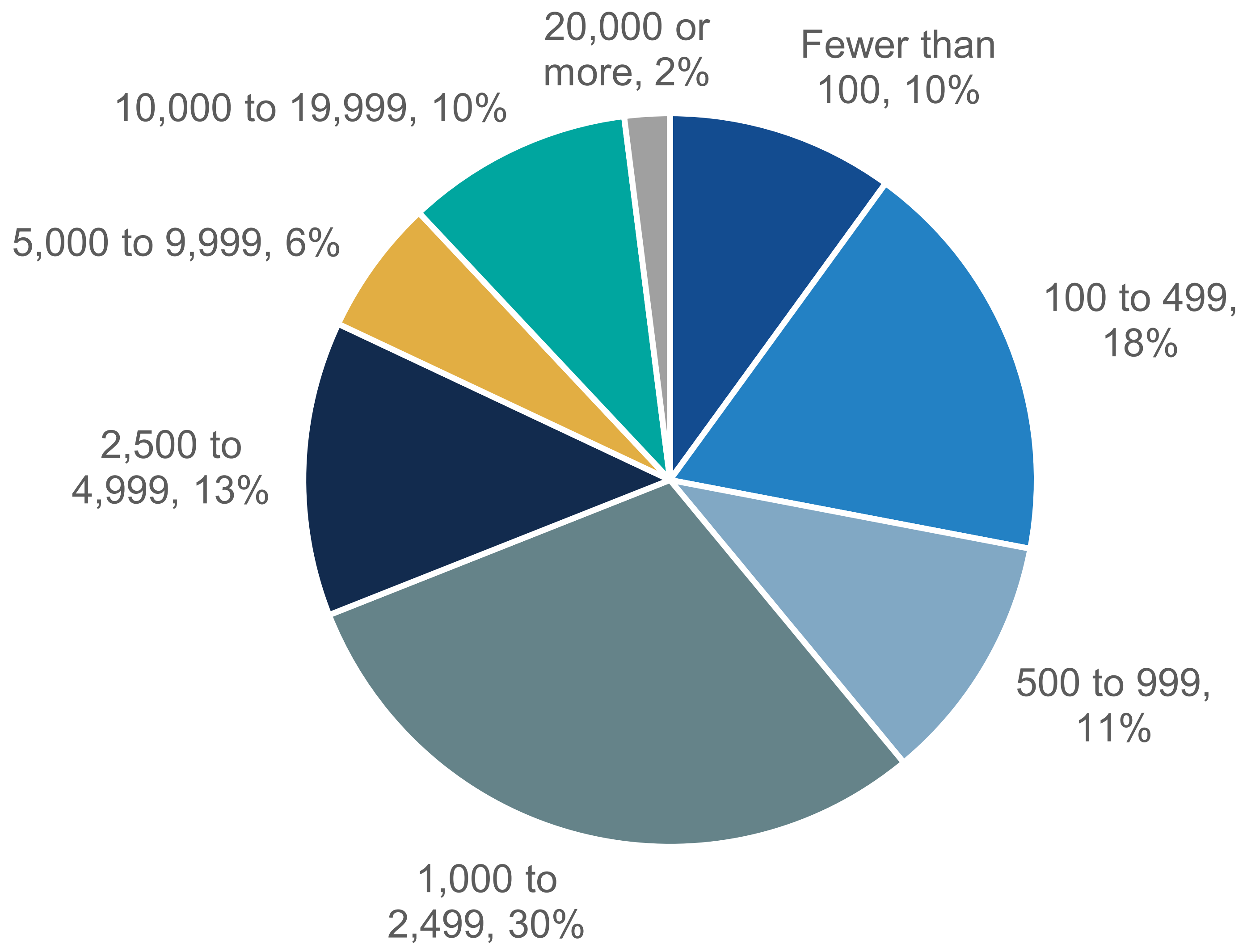
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America between November 15, 2023 and December 5, 2023. To qualify for this survey, respondents were required to be responsible for evaluating, purchasing, and utilizing developer-focused security products. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 368 IT, cybersecurity, and application development professionals.

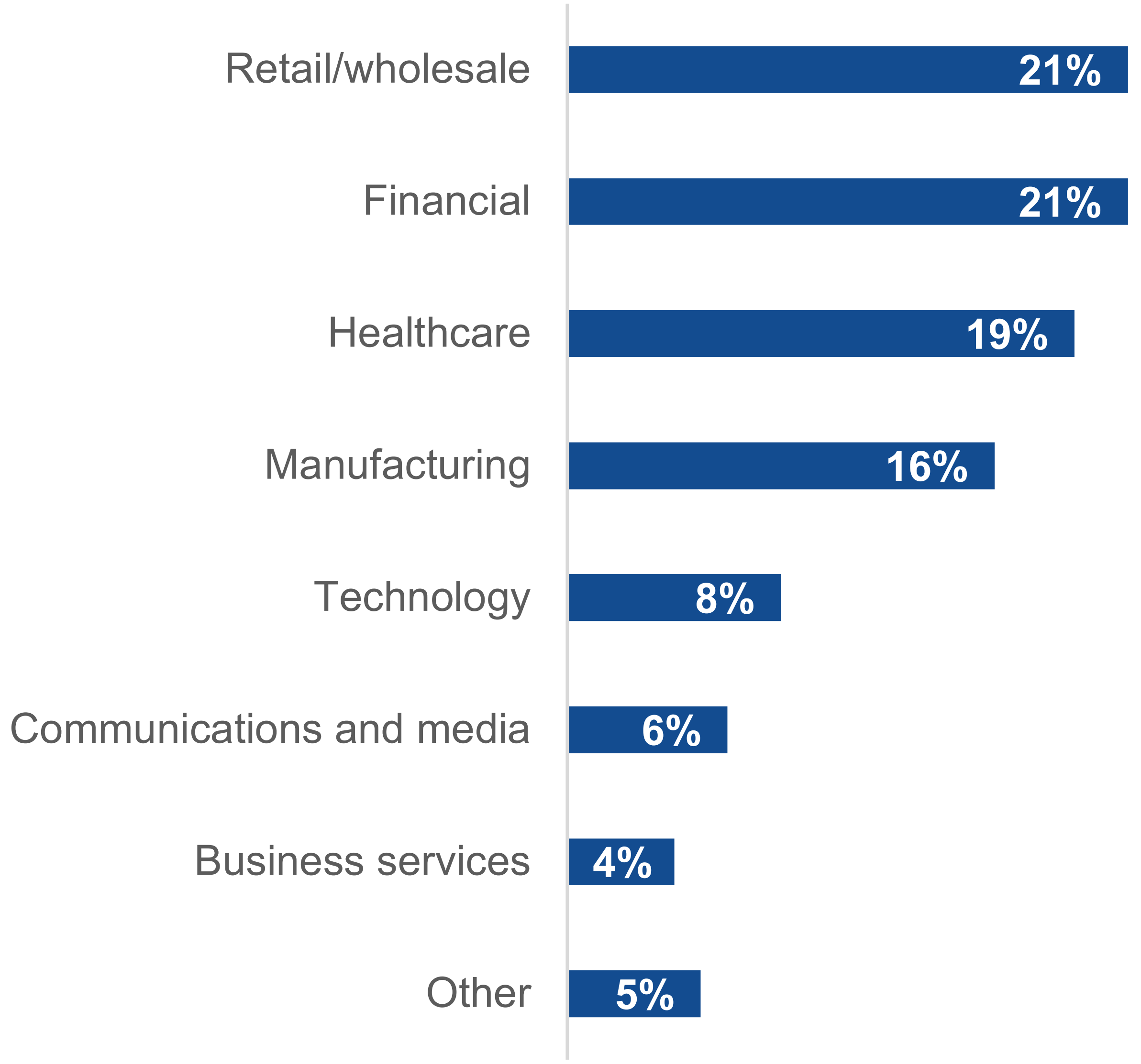
Respondents by job function.



Respondents by number of employees.



Respondents by industry.



BACK TO CONTENTS

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.