Omdia
by informa techtarget

Securing the Software Supply Chain: Strategic Approaches to Scaling Development with AI Adoption

Melinda Marks | *Practice Director, Cybersecurity*

April 2026

This Omdia research and eBook was commissioned by Docker and is distributed under license from Informa TechTarget, Inc.

Research objectives

Modern software development practices prioritize collaboration and speed of delivery, but this commensurately increases the complexity of the software supply chain. Security teams need to address elements that can exacerbate the attack surface, including source code, third-party and open source software (OSS) code and libraries, and developer tools and processes.

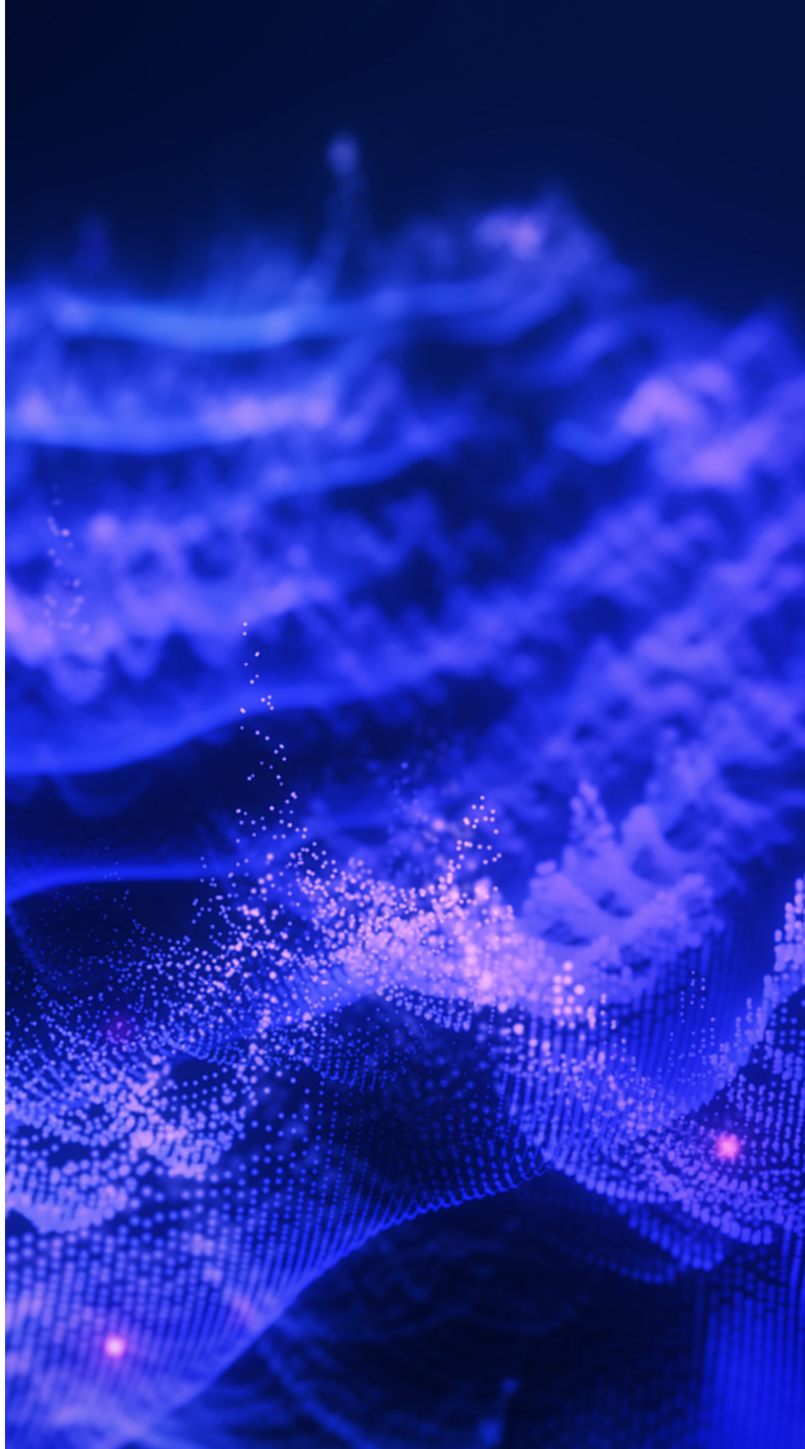
Further, software security is complicated by increasing AI usage, including generative AI assistive tools to build code and agentic AI that can autonomously perform tasks. These dynamics bring up important questions, such as: How do organizations enable developer speed and innovation without increasing vulnerabilities across the software supply chain? What strategies are teams developing to secure the software supply chain while supporting the demands of cloud-native application development?

To understand these trends and the resulting market dynamics, Omdia executed a survey of 400 IT, cybersecurity, and application professionals at organizations in North America responsible for evaluating or purchasing technology products and services to secure their organization's software supply chain.

This study sought to:

- **Assess** usage of third-party software components, including OSS, and its impact on security.
- **Examine** current solutions in place, their effectiveness, and their integration with cloud and application security products.
- **Determine** the impact of attacks and incidents focused on the software supply chain.
- **Validate** key stakeholders and investment plans for software supply chain security.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.



Key findings

Organizations need to address security risk with increasing usage of third-party code and AI adoption

PAGE 4

Security teams face challenges with current software supply chain solutions

PAGE 8

OSS is vital to developers and must be supported

PAGE 11

Effective inventory and software bill of materials tools can help meet security and compliance objectives

PAGE 14

The rapidly evolving threat landscape requires preventative measures and rapid response

PAGE 17

Investment plans prioritizing AI require collaboration across teams

PAGE 20

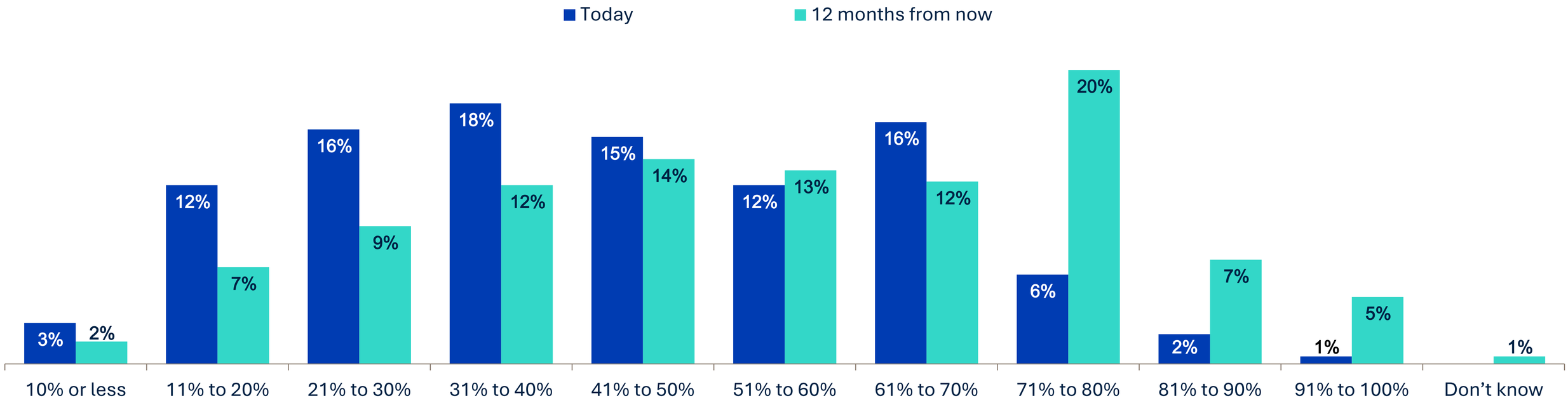
Back to Contents

Organizations need to address security risk with increasing usage of third-party code and AI adoption

Software applications include increasing percentages of third-party code

Utilizing prebuilt third-party software code helps developers who are under pressure to increase productivity and deliver sophisticated software applications, so not surprisingly, these teams are increasingly utilizing third-party code to save time in building their applications. Indeed, 37% of organizations report that more than half of their total software code comes from third-party sources today, which is expected to increase to 57% of organizations over the next 12 months.

Approximate percentage of total software code composition that is third-party code today and in 12 months.



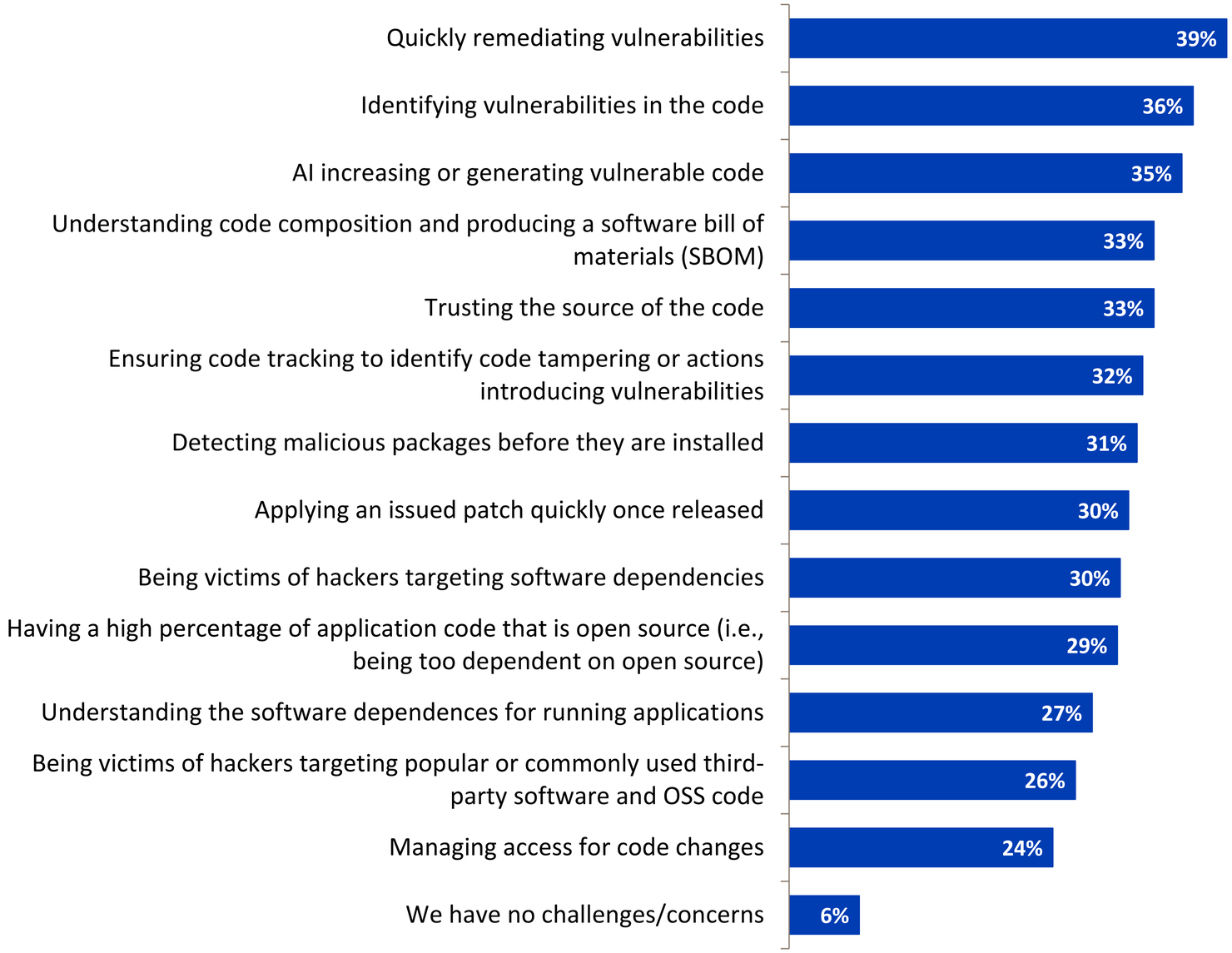
Back to Contents

Organizations report a wide variety of security concerns with using third-party software

The increasing percentages of third-party and open source code components impact security programs and cause many areas of concern. The most common challenges involve vulnerability management, including remediation (39%) and/or identification of vulnerabilities in the code (36%). Additionally, more than a third are worried about AI increasing vulnerable code because AI tools often pull from third-party and OSS code.

Other common challenges include understanding code composition and producing a software bill of materials (SBOM) and trusting code sources. Only 6% of organizations cited no challenges or concerns with third-party software.

Challenges or concerns organizations have with using third-party software including OSS.



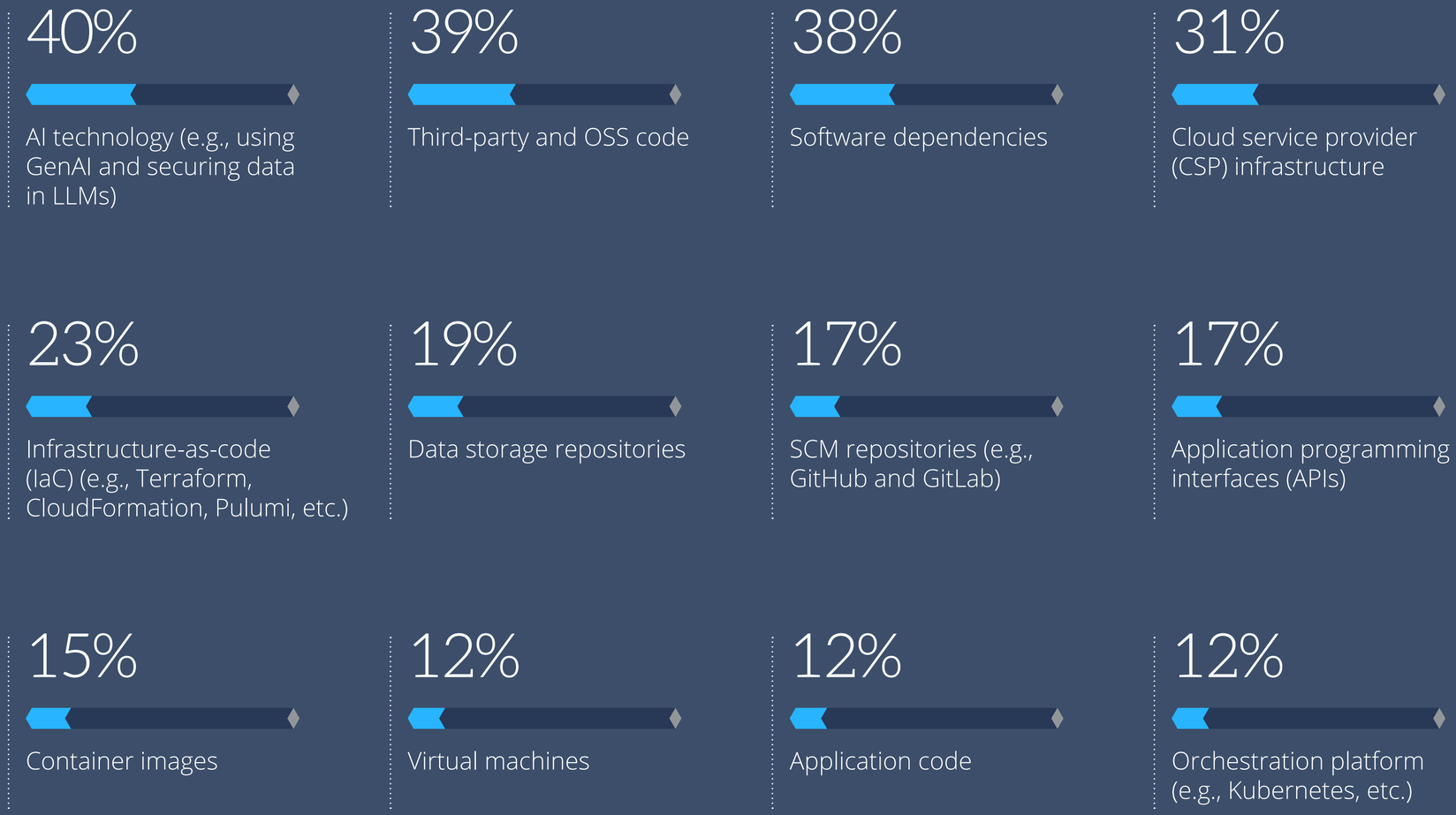
Back to Contents

AI tops elements of concern for software supply chain risk

While increasing percentages of third-party code and OSS introduce complexity in software code composition, several elements contribute to increased security risk in the software supply chain. When asked about top elements of concern, AI topped the list as developers increasingly utilize AI to assist in software development. This was followed closely by third-party and OSS code and software dependencies.

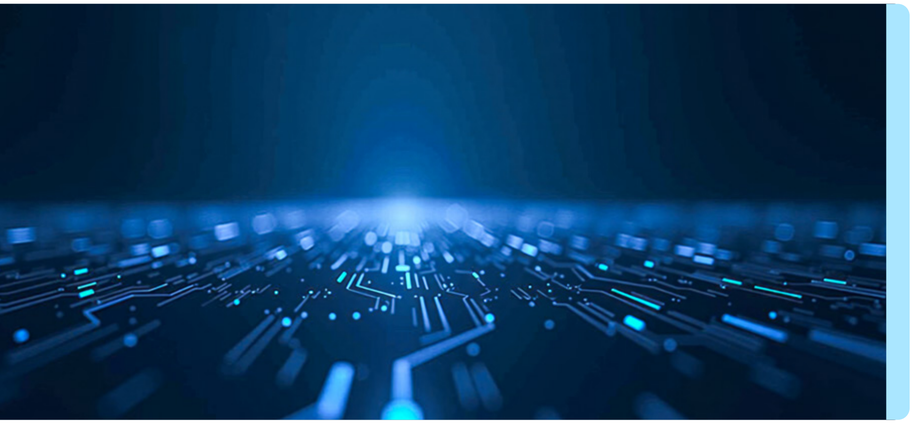
Other elements of concern include CSP infrastructure, infrastructure-as-code (IaC), data storage repositories, SCM repositories, APIs, and container images.

Elements of the cloud-native technology stack that pose the greatest risk to the software supply chain.



Back to Contents

Security teams face challenges with current software supply chain solutions

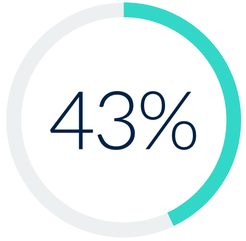


Nearly half do not feel they have robust software supply chain security

Organizations need a comprehensive program to secure their software supply chain, especially in light of increasing percentages of third-party code and usage of AI technologies in development. However, only 55% feel they have robust programs with the right processes and controls in place to secure their software supply chains. This is causing security teams to evaluate their current tool sets and look for ways to improve their programs to address the increasing complexity of mitigating risk across the software supply chain.

Assessment of current software supply chain security capabilities.

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



We have some processes and controls in place for software supply chain security

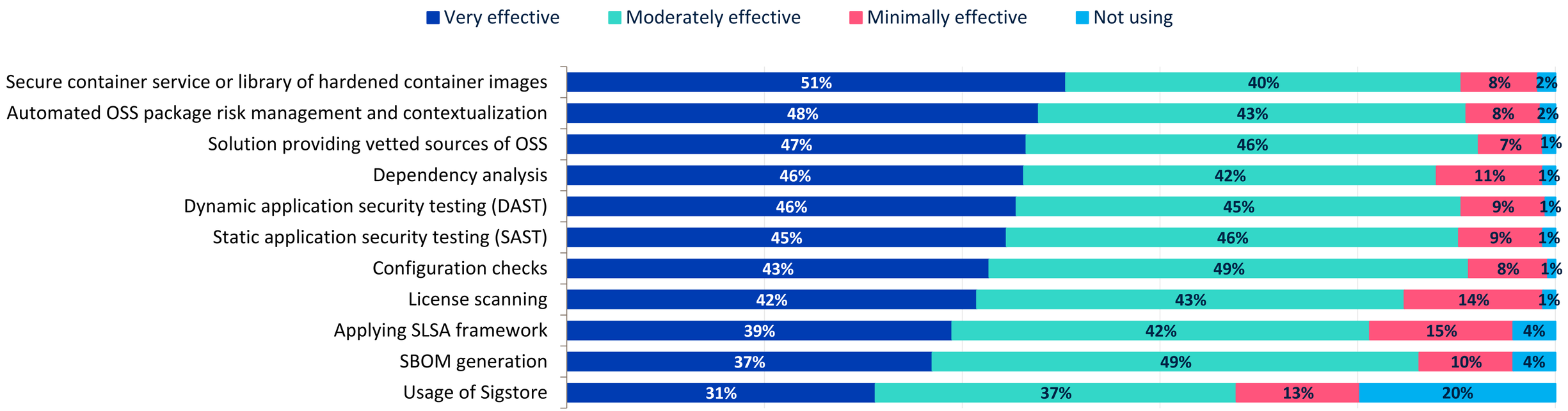
We have minimal policies, processes, and controls in place for software supply chain security and rely too much on individual efforts and manual measures

Back to Contents

Teams need effective security tools to secure third-party and OSS code

Secure container services or libraries of hardened container images were the only security tools for third-party and OSS code components that more than half of organizations identified as very effective. In general, organizations need more effective tools and confidence in capabilities to manage security and risk for third-party and OSS code components.

Effectiveness of security tools when it comes to third-party and OSS code components.



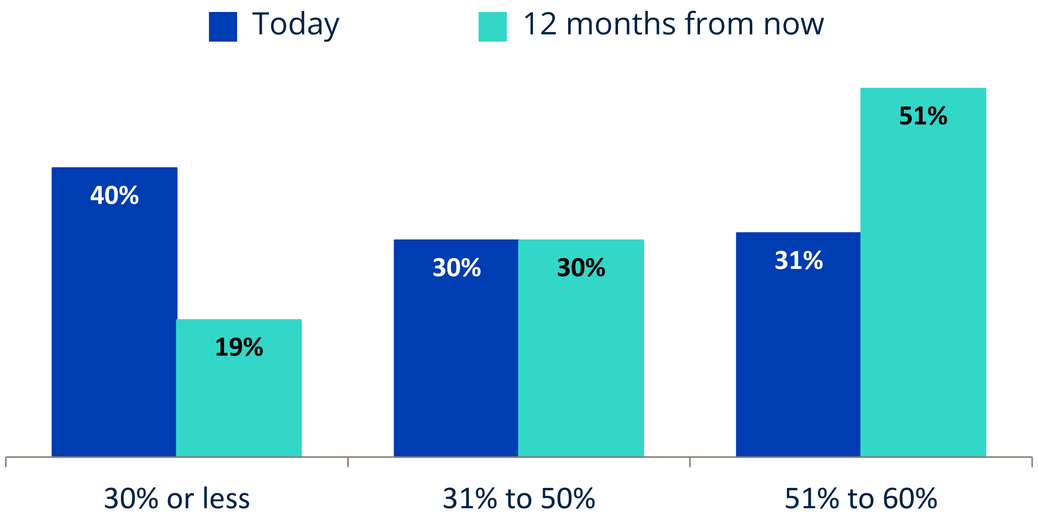
Back to Contents

OSS is vital to developers and must be supported

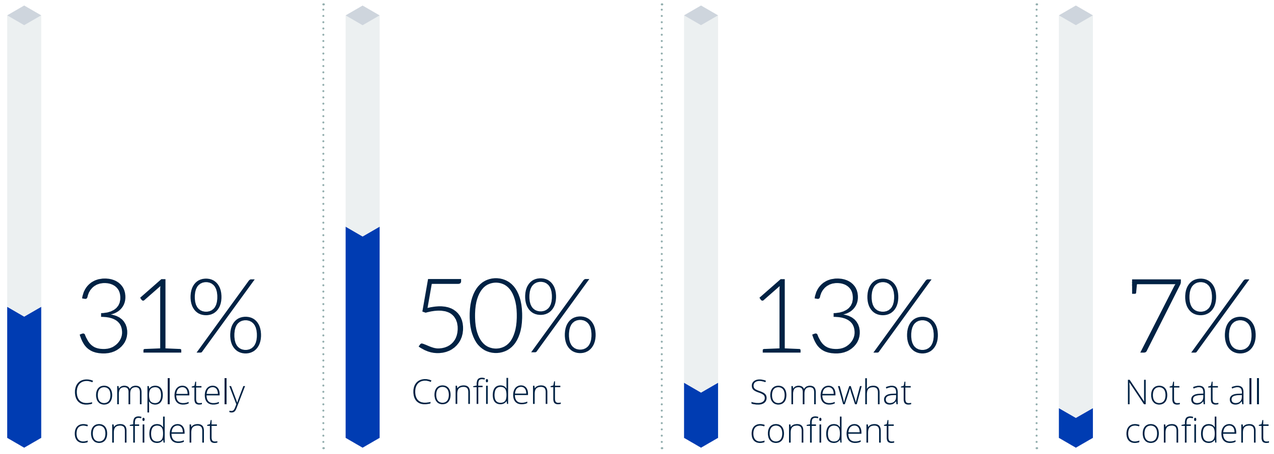
Organizations have high levels of confidence in secure OSS usage

Total code composition increasingly includes open source software. Today, 31% of organizations report that more than half of their code is composed of OSS, and this number is expected to jump to 51% over the next 12 months. With that in mind, it is encouraging that the majority of organizations are either confident (50%) or completely confident (31%) that their developers are only using secure OSS, though ideally confidence levels will continue to improve as more developers incorporate security into their responsibilities.

Approximate percentage of total software code composition that is OSS today and in 12 months.



Confidence level that developers are only using secure OSS.



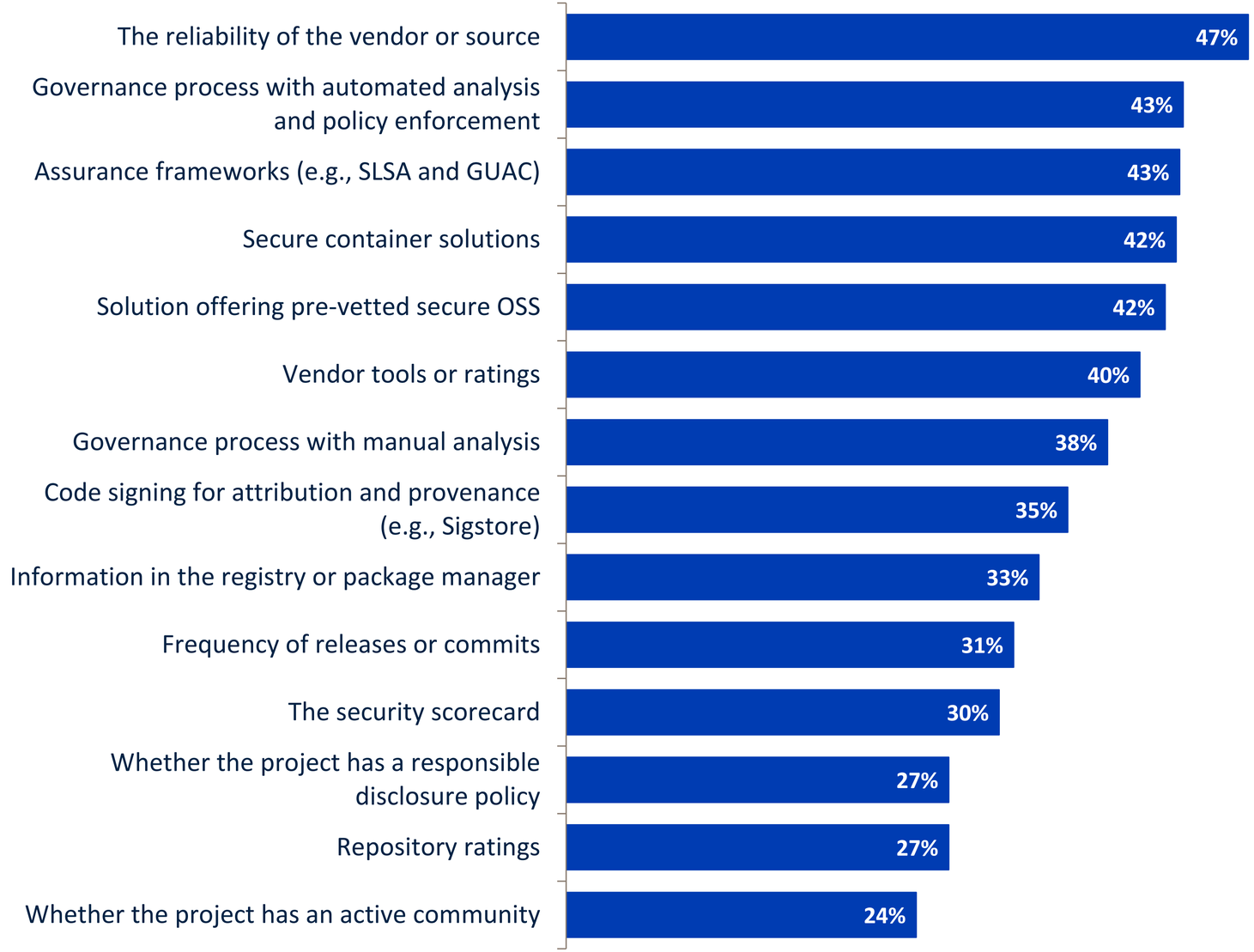
Back to Contents

Reliability of the source tops assurance factors for secure OSS

Organizations look at a variety of factors to determine secure OSS. The biggest factor is the reliability of the vendor or source, but organizations are also looking to governance processes, assurance frameworks, and solutions offering vetted OSS.

Lower on the list of factors are project disclosure policies, repository ratings, and whether the project has an active community. It is important for vendors, the cybersecurity industry, and the OSS community to educate teams on ways to ensure secure OSS.

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



Back to Contents

Effective inventory and software bill of materials tools can help meet security and compliance objectives

Incorporating SBOM generation in the application development process has helped mitigate risk

For those generating SBOMs, just more than half said they are generated on a case-by-case basis, and for 42%, it is a mandatory part of the process for all applications. SBOM generation should be automated and incorporated into development processes for software supply chain security and compliance. It is not surprising that having an inventory of software components contributes to risk management via more efficient vulnerability mitigation, the ability to set controls and processes to mitigate risk, and the ability to help meet compliance regulations, among others.

Do organizations currently generate an SBOM as part of their application development processes?

- 42% — Yes, it is a mandatory part of the process for all applications
- 55% — Yes, but on a case-by-case basis
- 3% — No, but we are planning to over the next 12 months

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

- 73% — Enables more efficient vulnerability mitigation
- 72% — Enables us to implement security controls and processes to mitigate risk
- 68% — Helps us meet compliance regulations
- 57% — Provides a comprehensive view of all the components and dependencies across the supply chain
- 53% — Helps our customers understand the composition of our applications and prove that their security requirements have been met

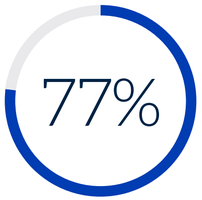
Back to Contents

Teams generate SBOMs from a variety of tools

Respondents often generate their SBOMs from multiple tools. Most often, it is from a software composition analysis solution, but high percentages generate them with a software supply chain security solution, CSP capabilities, an SBOM tool, and application security solutions.

While using manual processes is least commonly cited, it is shocking to see that more than a third are generating them manually. This shows the opportunity for security vendors to address these needs with easier-to-use SBOM tools that can be tied to application development processes.

Tools or processes organizations use to generate an SBOM.



Our software composition analysis (SCA) solution

Features from our cloud service provider

Our application security solution

Our software supply chain security (SSCS) solution

A dedicated SBOM tool

Manual processes for inventory and tracking

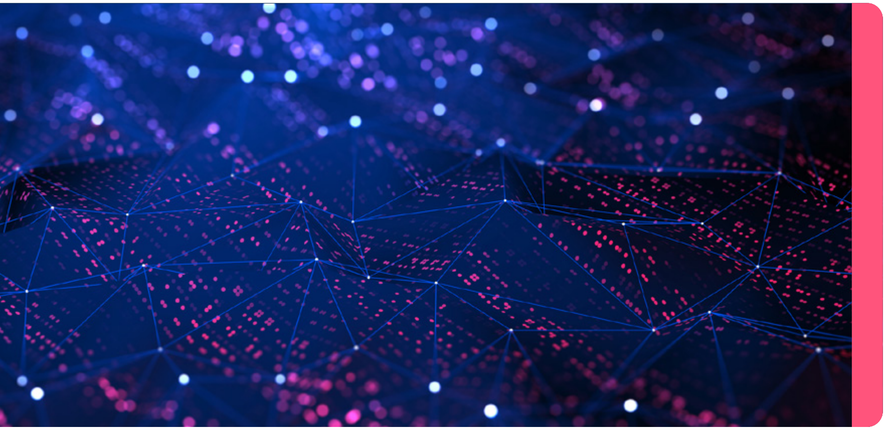
Back to Contents

The rapidly evolving threat landscape requires preventative measures and rapid response

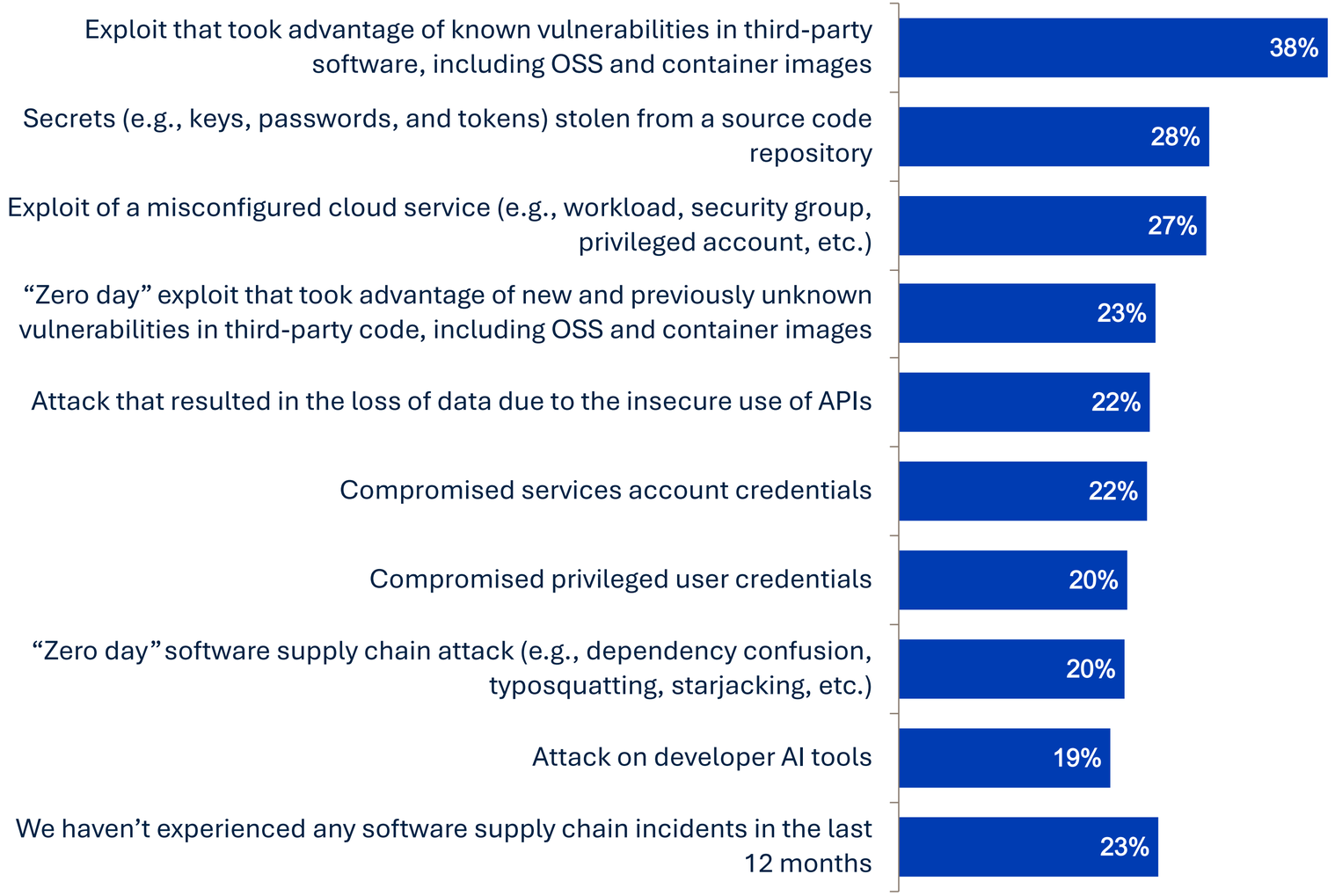
Software supply chain incidents

A majority (77%) of organizations experienced a software supply chain incident in the last year. This includes 23% from zero day exploits, 20% from zero day software supply chain attacks, and 19% facing attacks on developer AI tools.

Many of these were preventable. Indeed, the most common incident cited involved an exploit that took advantage of known vulnerabilities in third-party software, including OSS and container images. Other incidents stemmed from secrets stolen from a source code repository and the exploit of a misconfigured cloud service. These underscore the importance of efforts to mitigate risk, starting as early as possible in the development lifecycle, and ideally catching and remediating issues before the applications are deployed.



Software supply chain incidents organizations have experienced in the last 12 months.



Back to Contents

Impacts of software supply chain security incidents

Organizations have suffered serious impacts from software supply chain incidents. Nearly half (46%) faced unauthorized access to applications and data, while more than one-third had SLAs impacted by remediation steps (37%) and/or experienced stolen developer credentials, secrets, or keys (35%). Organizations also suffered loss of data, introduction of malware and ransomware, and fines for noncompliance.

This illustrates the importance of mitigating security risk as well as the criticality of quickly detecting and responding to attacks to minimize possible impacts.

Impacts organizations experienced from software supply chain security incidents.

46%

Unauthorized access to applications and data

37%

Remediation steps impacted service level agreements (SLAs)

35%

Stolen developer credentials, secrets, or keys

32%

Introduction of malware

31%

Data loss

25%

Introduction of ransomware

25%

Introduction of crypto-jacking malware to mine cryptocurrency

24%

Fines due to non-compliance with an industry regulation

8%

We have not experienced any impacts from software supply chain security incidents

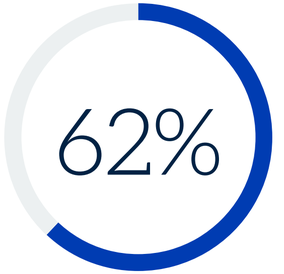
Back to Contents

Investment plans prioritizing AI require collaboration across teams

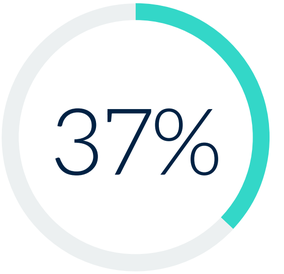
Software supply chain security investments are set for a variety of plans

When asked about spending plans, nearly two-thirds (62%) of organizations said they expect to make significant investments in software supply chain security, while 37% anticipate making more modest investments. Organizations aspire to gain multiple benefits from their investments in software supply chain security, including avoiding incidents, being able to fix issues before applications are deployed, achieving cost savings, and having fewer security issues detected in runtime. These responses reflect the need to strengthen the overall program to optimize efficiency for groups (developers and security) across the software development lifecycle.

Do organizations plan to invest in software supply chain security?



We expect to make significant investments



We expect to make moderate investments

Benefits organizations hope to achieve by investing in software supply chain security solutions.

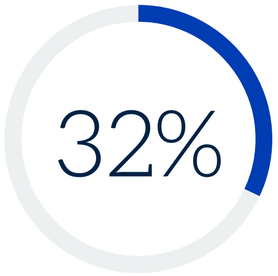
50%	Reduction in or avoidance of security incidents	49%	Ability to fix code issues before applications are deployed into production	47%	Cost savings	47%	Fewer security issues detected in runtime
46%	Improved application uptime or availability	44%	Time savings for the security team	42%	More actionable data to inform remediations	41%	Time savings for developers

Back to Contents

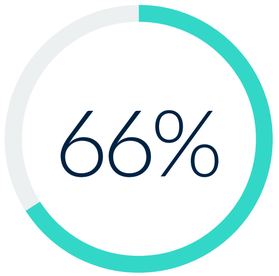
Enabling developers to secure their code is a high priority

Enabling developers to secure their code removes the security team from being a bottleneck for remediating security issues. As a result, the majority prioritize enabling developers to secure their own code; for nearly one-third, it's their top application security priority. At the same time, however, nearly half (45%) of security teams have only moderate or less influence over security products and processes for developers. In order for organizations to secure the growing complexity of the software supply chain with increased productivity and growth, security teams will need to have full visibility and control to effectively mitigate risk, especially as developers become more involved in security processes.

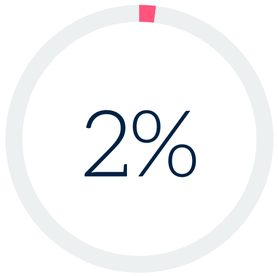
Priority level for enabling developers to secure their code.



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)



It's important but not a high priority (i.e., we have higher application security and/or application development priorities)

Can security teams influence and/or roll out security products and processes for developers to use for software supply chain security?

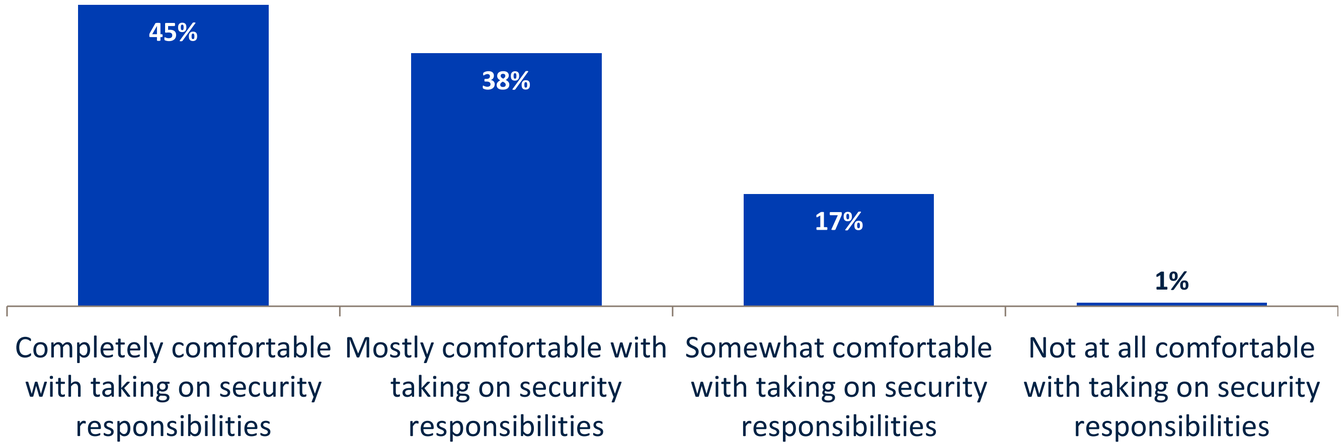
55%	Yes, security teams have significant influence over security products and processes for developers
38%	Yes, security teams have moderate influence over security products and processes for developers
7%	Yes, security teams have limited influence over security products and processes for developers
1%	No, security teams have no influence over security products and processes for developers

Back to Contents

Supporting development is a critical need

As shifting security left to developers frees up security teams, they need to make sure that they make it as easy as possible for developers to secure their own code. The good news is that the majority of respondents believe their developers are mostly (38%) or completely (45%) comfortable taking on security responsibilities. Those organizations whose developers are only somewhat comfortable or not comfortable need to ensure that security tasks are not disruptive to development processes. Security teams need to find tools that they can roll out consistently across development teams, working within development workflows to make it easy for developers to increase the quality and security of their code.

Perceived comfort level of developers with taking on security responsibilities.



Why developers are uncomfortable with taking on security responsibilities.

46% They view security tasks as disruptive to development processes

46% They want to spend their time developing product code

32% They face organizational challenges where security and development team priorities are not aligned

30% Security controls are not embedded into default tools or base components

30% They don't have security backgrounds

29% They believe the security team should do the security work

23% They don't like the security tools that have been recommended or purchased

19% They don't want to use separate security tools

14% They don't want to learn about security

Back to Contents

About

Docker drives modern software development by making it easy to adopt container technology to radically boost productivity, security, testing, and collaboration at every step of the developer experience, including emerging AI workflows. Embraced by over 20 million developers worldwide, Docker's unmatched flexibility and choice make it the preferred tool for developers seeking efficiency and innovation for creating modern applications. Learn more about Docker at www.docker.com.

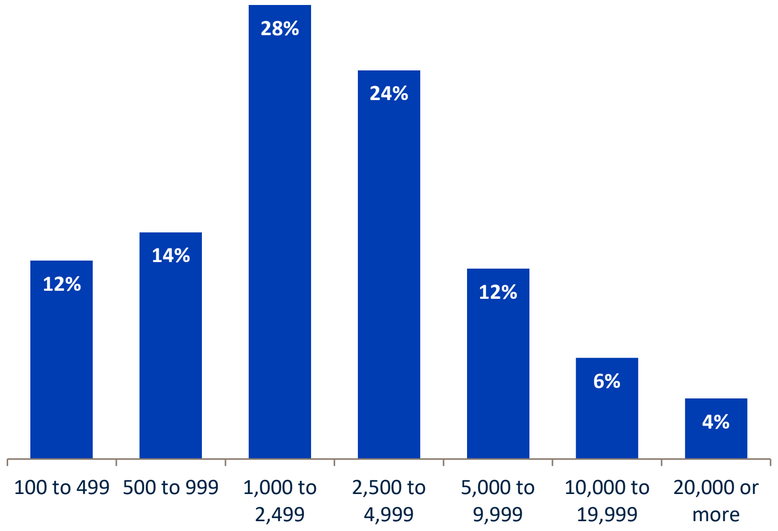
Learn more

Research methodology and demographics

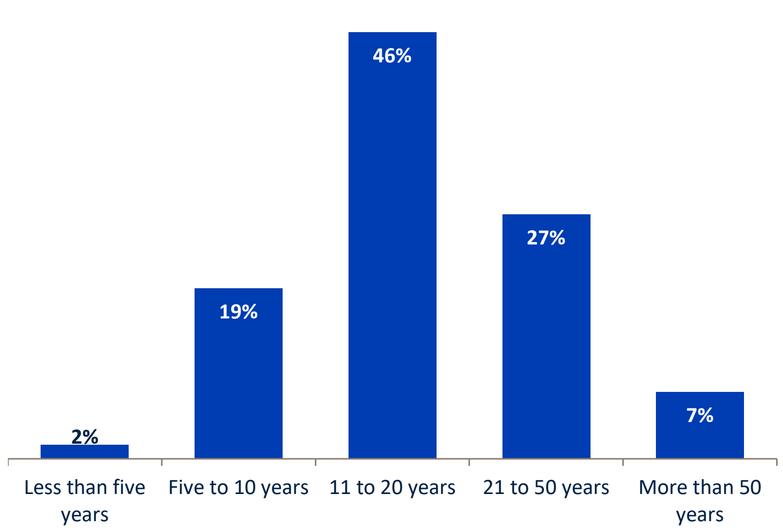
To gather data for this report, Omdia conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America between February 12, 2026, and February 25, 2026. To qualify for this survey, respondents were required to be responsible for evaluating or purchasing technology products and services to secure their organization's software supply chain. 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 several criteria) for data integrity, we were left with a final total sample of 400 of IT, cybersecurity, and application development professionals.

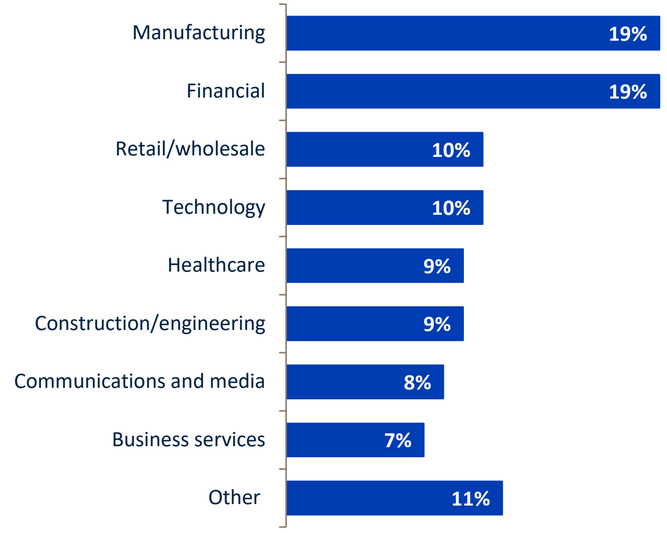
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



Back to Contents

Omdia provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.