Enterprise Strategy Group | Getting to the bigger truth.™

WALKING THE LINE:
GitOps and Shift Left Security

Scalable, Developer-centric Supply Chain Security Solutions

Melinda Marks, ESG Senior Analyst

AUGUST 2022

Research Objectives

As organizations adopt modern software development processes, developers are empowered to quickly develop and release their applications by deploying them to the cloud. Security teams are challenged keeping up with the growth and speed of continuous integration/continuous deployment (CI/CD) cycles and their dynamic components.

While the industry has been talking about shifting security left to help security scale with rapid development, organizations have faced challenges putting that into practice. Most cloud-native security incidents are caused by misconfigurations, putting pressure on security teams to find ways to incorporate security into development so coding issues are caught and fixed before deployment. Organizations also need to focus on better ways to work with developers for rapid remediation of any detected security issues.
In order to gain insights into these trends, ESG surveyed 350 IT (30%) and cybersecurity (40%) decision makers, as well as application developers (30%), responsible for evaluating, purchasing, and utilizing developer-focused security products at midmarket (100 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (US and Canada).

THIS STUDY SOUGHT TO:

Determine the extent to which organizations incorporate security into developer workflows.

Understand the challenges organizations face with faster cloud-native development lifecycles.

Gain insights into what types of solutions are most effective at securing software while not slowing down development processes.

Gauge buyer preferences for vendor solutions, how solutions are deployed, and how to reduce work across teams.

Back to Contents

TABLE OF **CONTENTS**

CLICK TO FOLLOW

Modern Development Increases Speed *and* Security Risk

Prevalence of Open Source Software (OSS)

Respondents recognize the growing use of OSS components in application development. Indeed, eight in ten organizations report using open source software in programming cloud-native applications. Developers save time by leveraging existing open source code in their applications so they can spend more time building custom code for the unique functionality of their software; however, it is important to make sure this doesn't introduce security risks. Open source software is available thanks to a strong cloud-native development community and vendors who share and contribute to the code. As a result, it is not surprising to see a high percentage of OSS in software code composition.

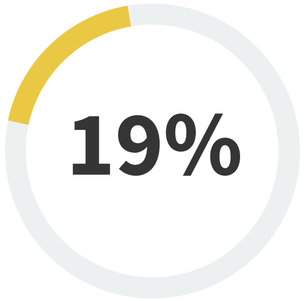
8 IN 10

organizations report using **open source software in programming cloud-native applications.**

» Usage of open source software for cloud-native apps.

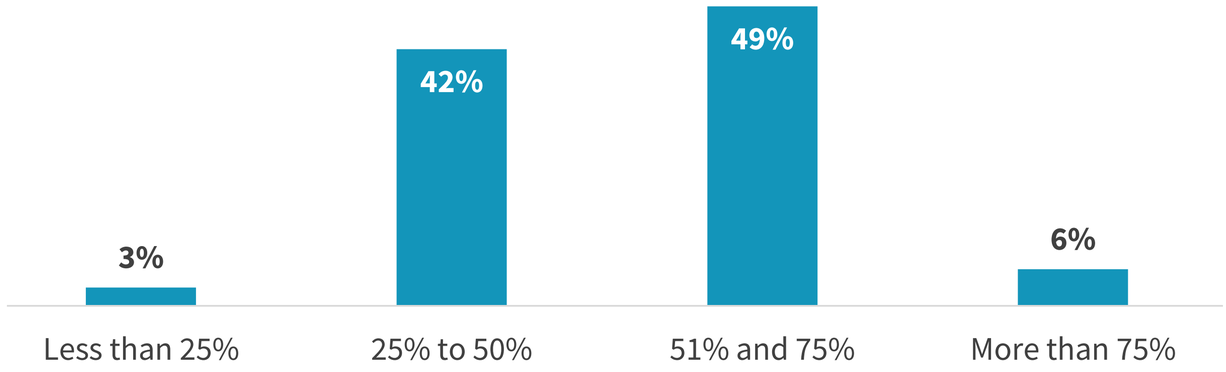
We currently use open source software

We plan to use open source software in the next 12 months



An additional 1% are **interested** in using open source software.

» Percentage of code composition that is OSS.



Back to Contents

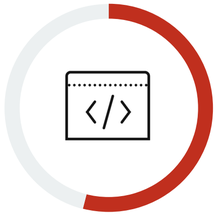
Top Security Concerns with Open Source

While the use of OSS saves developers time, organizations are concerned about security implications. It is attractive for hackers to look for OSS vulnerabilities because if they have a weakness, attackers can target any company using the most popular OSS.

As such, organizations are looking for ways to make sure they fully understand their OSS components and can quickly respond if a vulnerability is found.

> “Organizations are looking for ways to make sure they fully understand their OSS components **and can quickly respond if a vulnerability is found.”**
>
> *- Melinda Marks, ESG Senior Analyst*

» Open source software challenges and concerns.



54%
Having a high percentage of application code that is open source

41%
Being victims of hackers targeting popular/commonly used open source software

40%
Trusting the source of the code

39%
Identifying vulnerabilities in the code

39%
Understanding code composition and producing a software bill of materials

39%
Applying an issued patch quickly once released

38%
Quickly remediating a vulnerability

Back to Contents

Increasing Use of Infrastructure as Code

Infrastructure as code (IaC) enables developers to provision their own infrastructure so they don't have to wait for IT or operations teams to provision it for them. They typically use the code from templates to declaratively script the cloud infrastructure needed, managing resources such as networking, compute services, and storage. More than two-thirds (69%) of organizations currently utilize IaC templates to provision cloud infrastructure, and another 27% plan to do so within the next 12 months. And while the extent of use is more limited today, over the next two years, 61% of organizations expect to use IaC templates for more than half of their cloud-native applications.

OVER THE NEXT TWO YEARS,

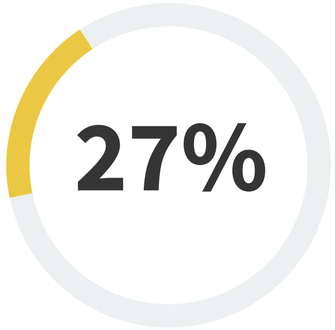
61%

of organizations expect to use IaC templates for **more than half of their cloud-native applications.**

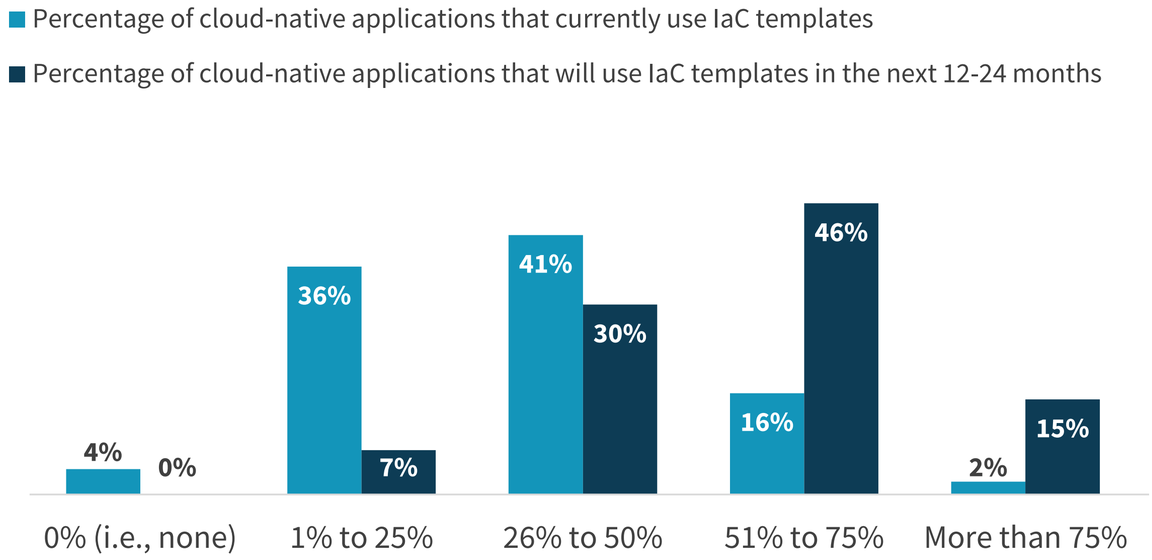
» Usage of IaC templates.

We currently use
IaC templates to provision cloud infrastructure

We plan to use
IaC templates in the next 12 months



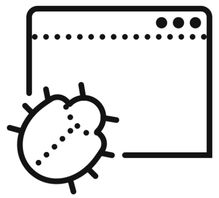
An additional 4% are **interested** in using IaC templates.



Back to Contents

Misconfigurations and Incidents with IaC Usage

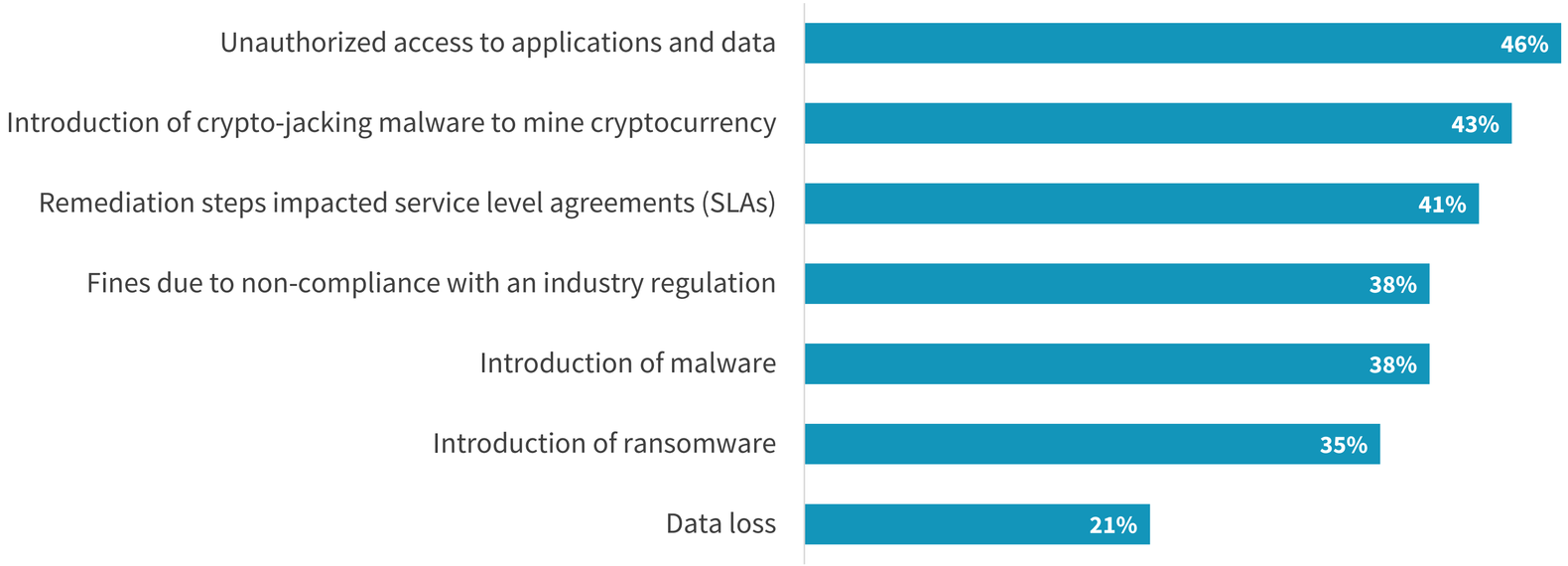
As developers increasingly use IaC, there is a heightened chance of mistakes. The coding issues may be difficult to detect, but because they control access to resources, misconfigurations can have dire consequences. The majority (83%) of respondents reported seeing an increase in misconfigurations with IaC usage. As a result, they have encountered a range of consequences, including unauthorized access to applications and data, introduction of malware, impacted service levels, and data loss.



83%

of respondents say they are experiencing an increase **in IaC template misconfigurations.**

» Impacts of increased IaC template misconfigurations.



Back to Contents

Security Needs to be Incorporated into Development Processes

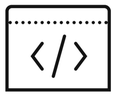
Incorporating Security into Development

Organizations are making efforts to incorporate security processes in development so that the faster release cycles do not expose them to an unmanageable amount of security risk. This includes cybersecurity user stories in agile software development processes, security-as-code (SaC), and GitOps. While 59% say they have implemented security-as-code, respondents believe it will be a highly relevant approach in the next two years. Although most see the utility of adopting SaC, organizations are still determining how to implement it or how to implement it across projects and teams given its maturity and the ongoing cybersecurity skills shortage.

» Security processes currently used to secure cloud-native applications.

The definition of cybersecurity user stories in our agile software development process

63%



Security-as-code

59%

GitOps to revert to prior configurations

55%

» Perceptions on security-as-code.

Security-as-code will be a highly relevant cybersecurity approach within the next 24 months

72%

My cybersecurity team lacks critical mass of security analysts equipped to implement security-as-code

56%

Security-as-code is not currently mature enough to incorporate into our cybersecurity program

51%

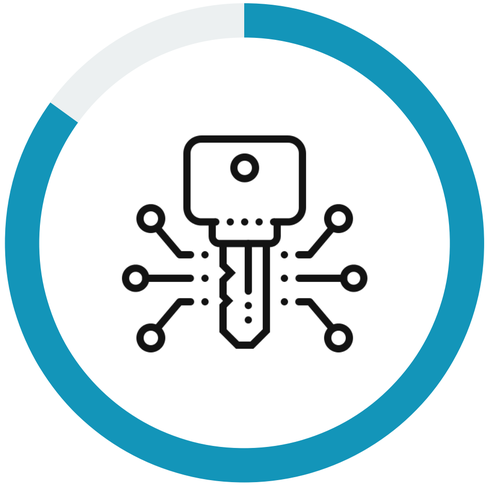
Back to Contents

Secret Scanning in Git Repositories

Developers often hardcode secrets (i.e., credentials including passwords, API keys, and tokens) into their code for ease of use. It follows then that 85% of organizations are scanning git repositories for secrets, and they are finding high numbers of them. Obviously, scanning is a good practice, but it doesn't guarantee protection. The reduction in risk depends on whether security can ensure remediation actions. Indeed, while the majority of organizations scan their git repositories for secrets, nearly one-third (31%) reported that they have had secrets stolen from a source code repository.

31%

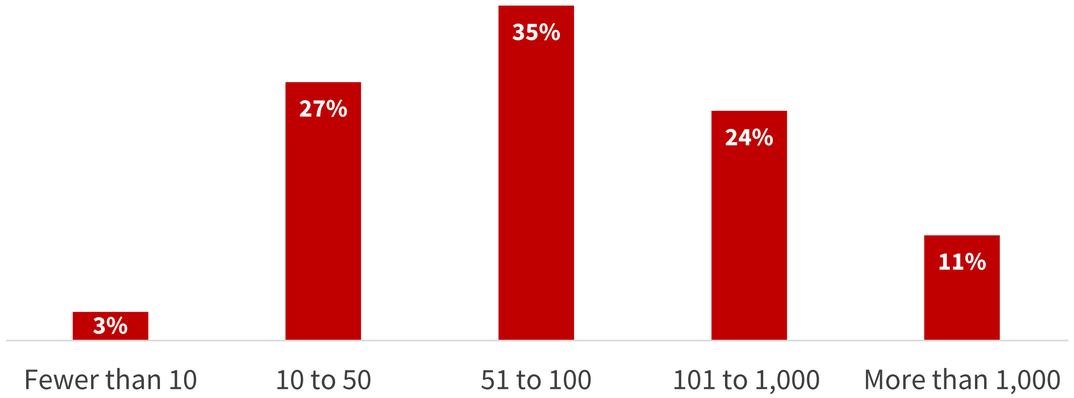
of organizations have had secrets stolen from a source code repository in the last 12 months.



We currently scan our git repositories to uncover risky secrets,

85%

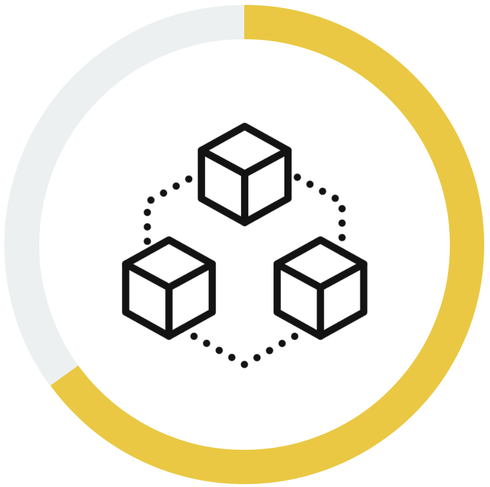
» Estimated secrets from git repository scans.



Back to Contents

Challenges Applying Security Practices While Accounting for Faster Development Cycles

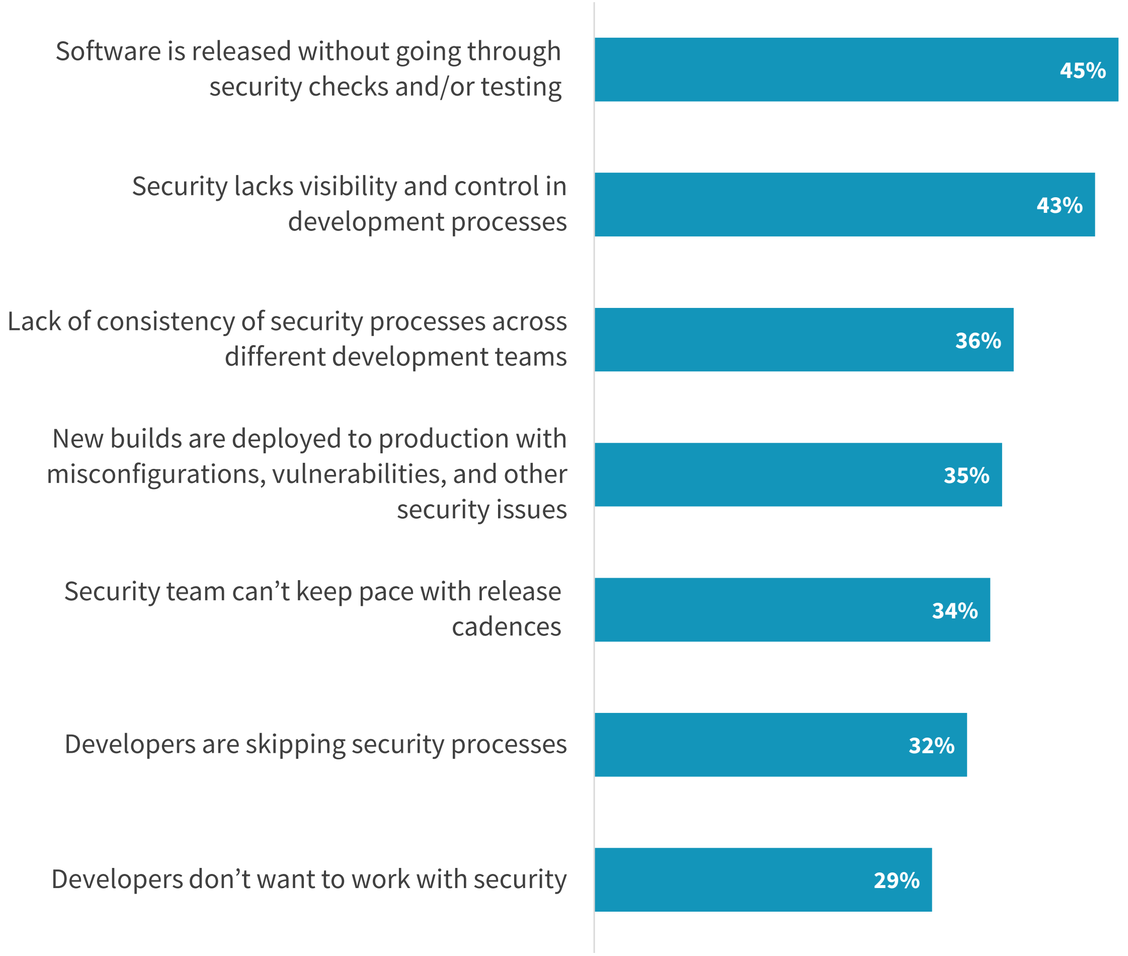
As security teams work to incorporate security into development, they face multiple challenges keeping up with the speed and volume of releases with CI/CD. The most commonly cited are software being released without going through security checks or testing (45%) and the lack of visibility and control security has in development processes (43%). This is further exacerbated by the fact that nearly two-thirds of organizations have more than 50 git repositories.



65%

of organizations have **more than 50 git repositories.**

» Security challenges caused by faster CI/CD development cycles.



Back to Contents

The Cloud-native Cybersecurity Threat Landscape Is Intensifying

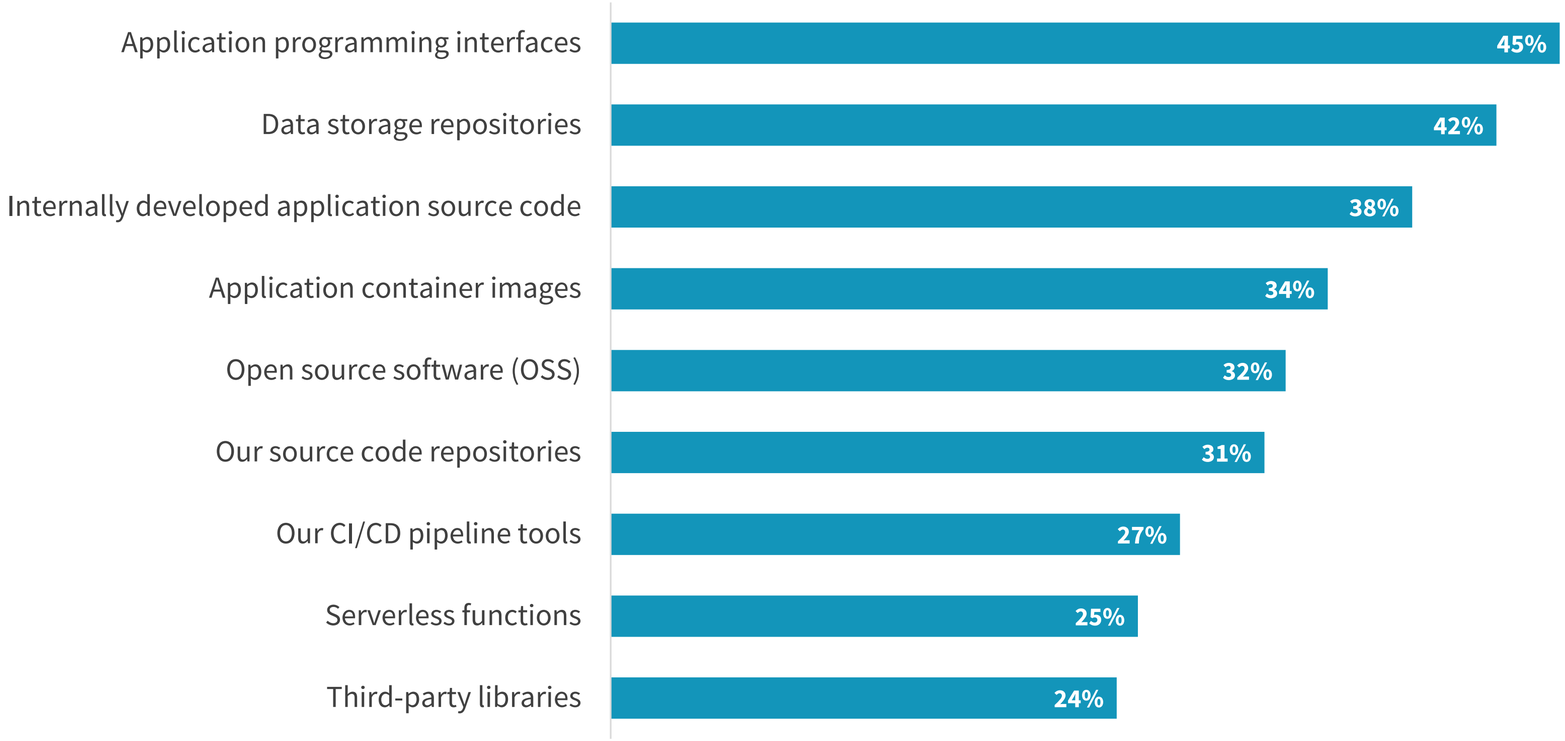
Cloud-native Elements Most Susceptible to Attack Align with Recent Incidents

Organizations rated the elements across the software stack and tool chain that they felt were most susceptible to attack. APIs were the most commonly identified element, followed by data storage repositories and internally developed application source code.

The vast majority of respondents indicate their organizations have faced a variety of security incidents and related consequences tied to their internally developed cloud-native applications. The three most commonly cited incident types involved insecure use of APIs, code vulnerabilities, and compromised account credentials, which happens to align with two of the most susceptible software stack elements.

> **“APIs were the most commonly identified element,** followed by data storage repositories and internally developed application source code.”

» Elements of the cloud-native application stack believed to be most susceptible to compromise.

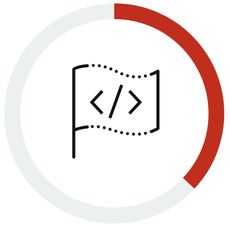


Back to Contents

» Cybersecurity incidents experienced as a result of cloud-native applications.

Attacks that resulted in the loss of data due to the insecure use of APIs,

38%



Exploit(s) that took advantage of known vulnerabilities in internally developed code,

37%

Compromised services account credentials,

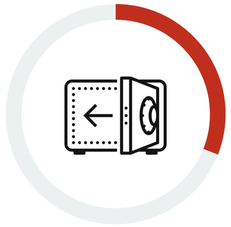
35%

Exploit(s) that took advantage of known vulnerabilities in open source software,

34%

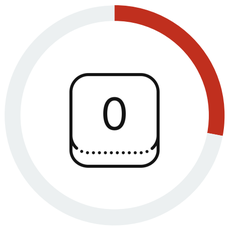
Exploit of a misconfigured cloud service,

33%



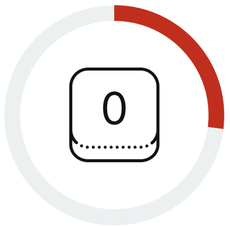
Secrets stolen from a source code repository,

31%



“Zero day” exploit(s) that took advantage of new and previously unknown vulnerabilities in open source software,

28%



“Zero day” exploit(s) that took advantage of new and previously unknown vulnerabilities in internally developed code,

27%

Compromised privileged user credentials,

26%

Back to Contents

Increased Efforts to Secure the Software Supply Chain Following Highly Publicized Attacks

Between concerns about and actual incidents tied to cloud-native applications, organizations would be well-served to take preemptive measures to mitigate these issues. Indeed, nearly three-quarters (73%) have significantly increased their efforts to secure open source software, container images, and third-party software components as a result of recent software supply chain attacks. Organizations are taking a wide range of actions to reduce their risk in light of these attacks.

73%

of organizations said they have significantly increased their efforts to secure open source software, container images, and third-party software components as a result of recent software supply chain attacks.

» Top ten actions taken because of recent software supply chain attacks.

Back to Contents

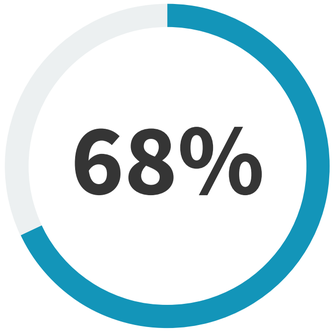
Security Must be Inserted into Development Processes without Disruption

Organizations Shifting Left to Scale

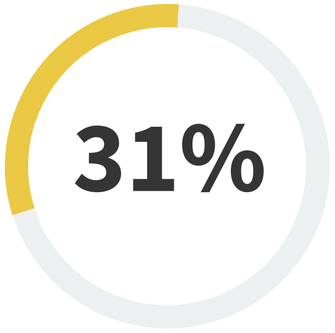
Most organizations are prioritizing developer-focused security solutions and even shifting some security responsibilities to developers because it's the only way they can scale. Indeed, nearly all respondents said this is important, and more than two-thirds (68%) identified it as a high priority. Although 36% said they are *completely* comfortable shifting security responsibilities to development, the majority of organizations reported being either mostly (49%) or slightly (15%) comfortable.

» Priority level for adopting a developer-focused security strategy.

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

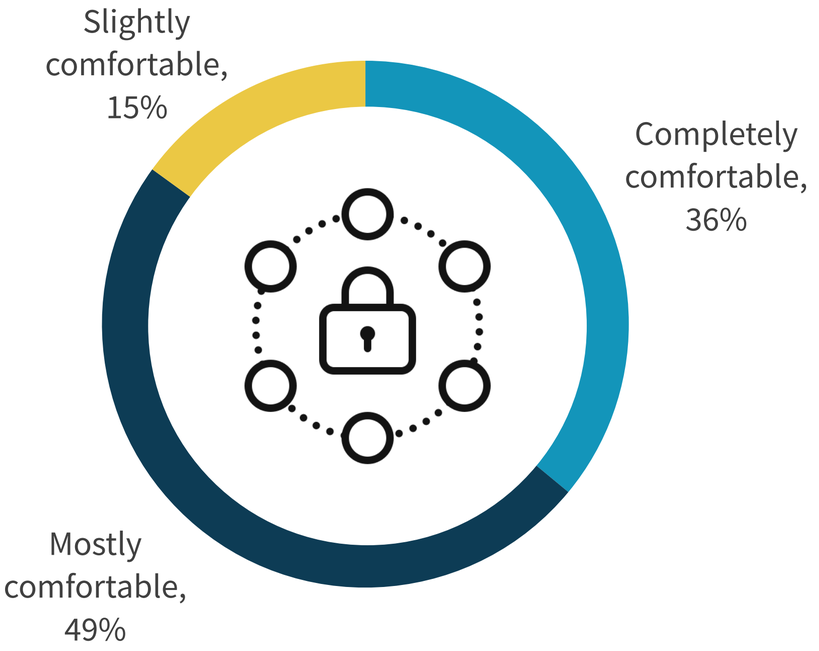


It's important, but not a high priority (i.e., we have higher security and/or AppDev priorities)



An additional 1% say **it's not a priority at all**
(i.e., security is doing fine without shifting responsibilities to developers)

» Security teams' comfort level adopting a developer-focused security strategy.



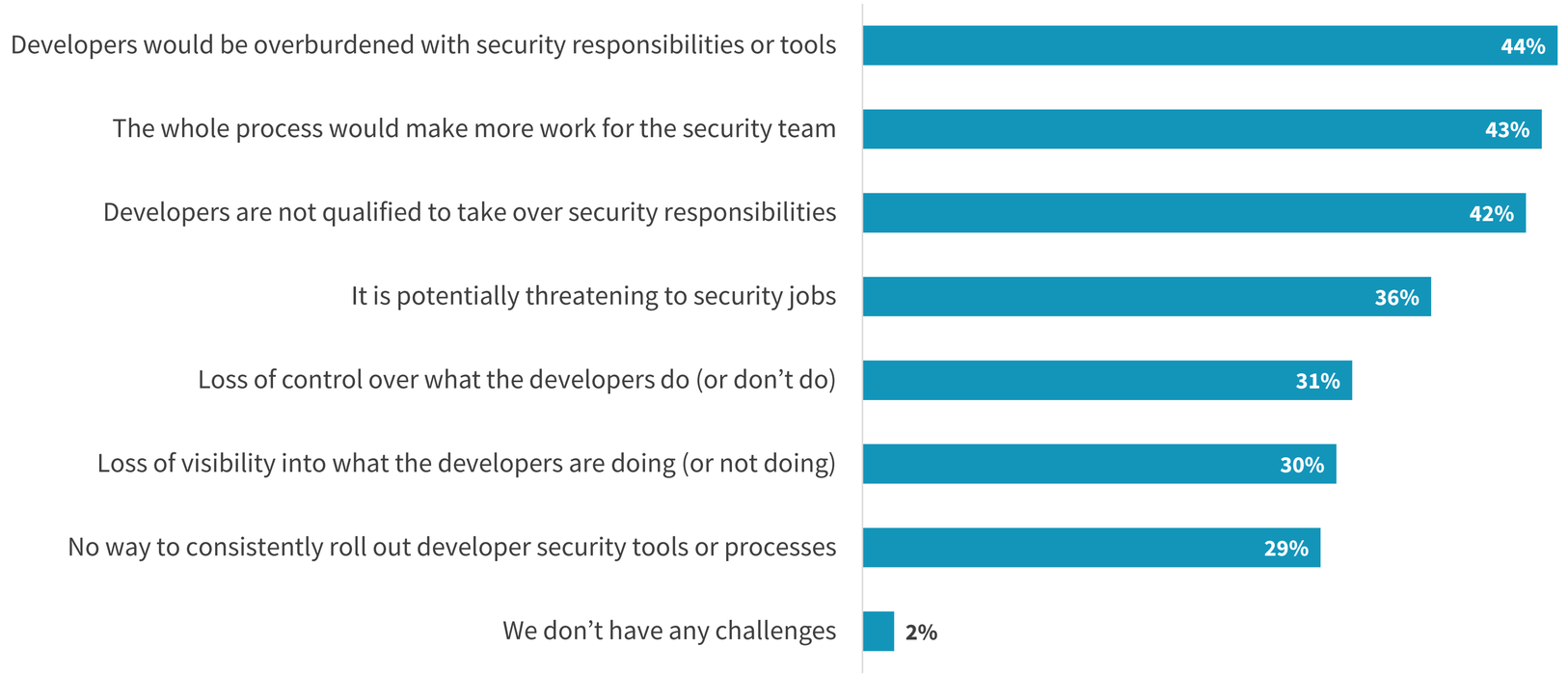
Back to Contents

Challenges Shifting Security to Development

While there are obvious benefits of developers being more involved in security activities and processes, there are also obstacles to overcome. The most commonly cited challenges related to developers assuming more security tasks include the notion that developers will either be overburdened by (44%) or underqualified to take over (42%) security responsibilities, along with the related notion that these efforts would ultimately end up making more work for cybersecurity teams (43%).

“While there are obvious benefits... **there are also obstacles to overcome.**”

» Challenges having developers take on more security responsibilities.

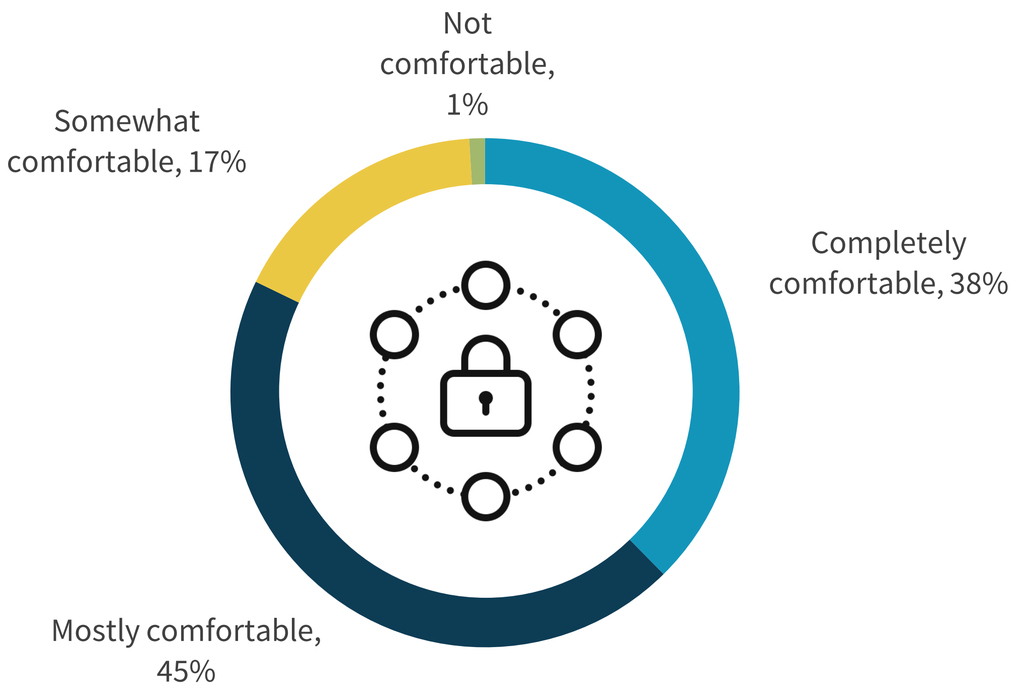


Back to Contents

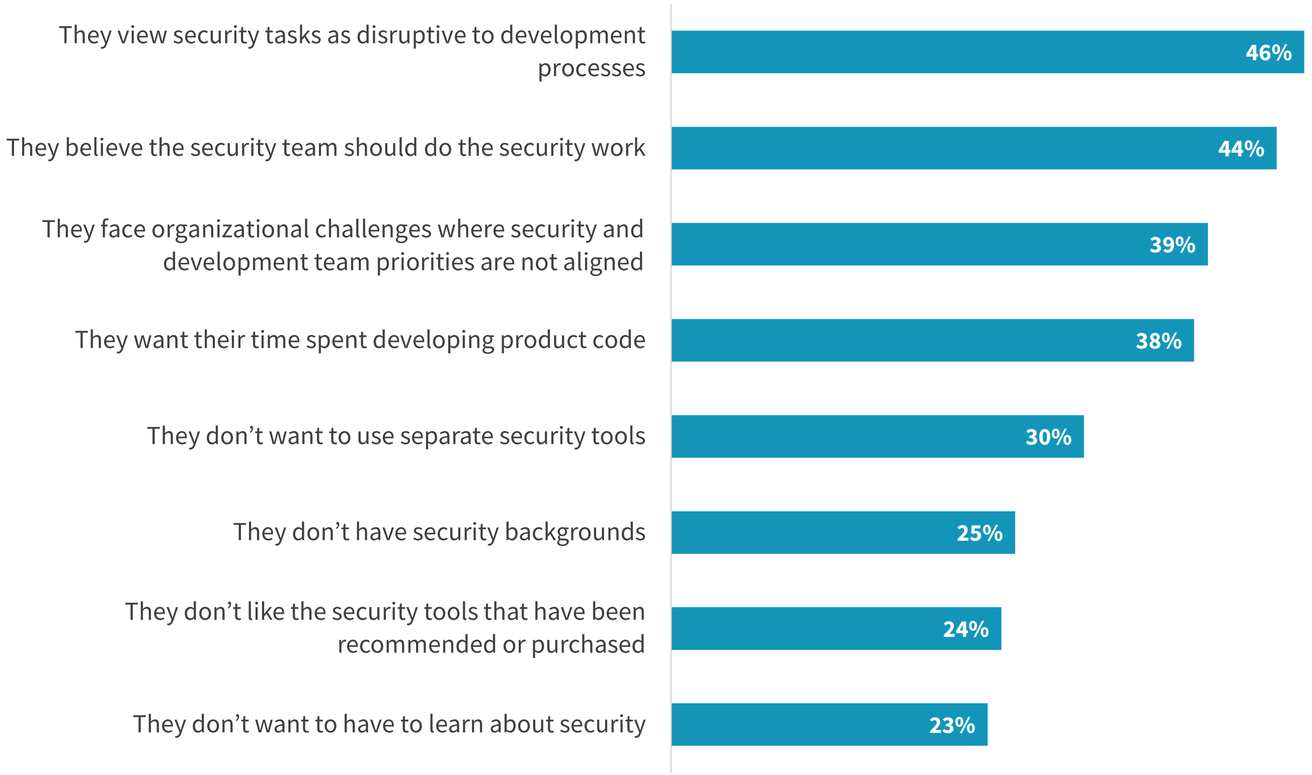
Developer Challenges

From the developer perspective, the majority are either completely (38%) or mostly (45%) comfortable taking on more security responsibilities. For developers not completely comfortable with this shift-left strategy, the most common objections include the beliefs that security tasks are disruptive to development processes and that security teams should maintain full autonomy over the security ecosystem.

» Developers' comfort level with increased security involvement.



» Reasons developers aren't completely comfortable with taking on security responsibilities.



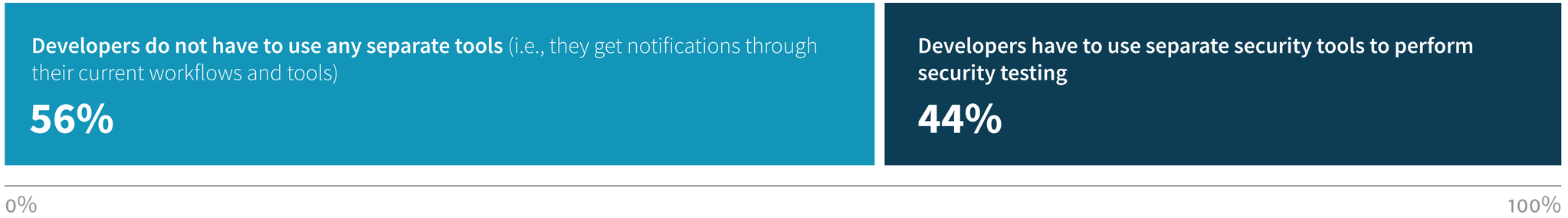
Back to Contents

Organizations Are Incorporating Monitoring and Security Testing into Development to Reduce Risk

Security Tools Outside of Developer Workflows

More than half (56%) of organizations are using tools that work within developer tools, though 44% still rely on separate security tools to perform testing. For wider acceptance among developers, organizations should look for security tools that work within developer workflows so there is no context switching needed to remediate coding issues.

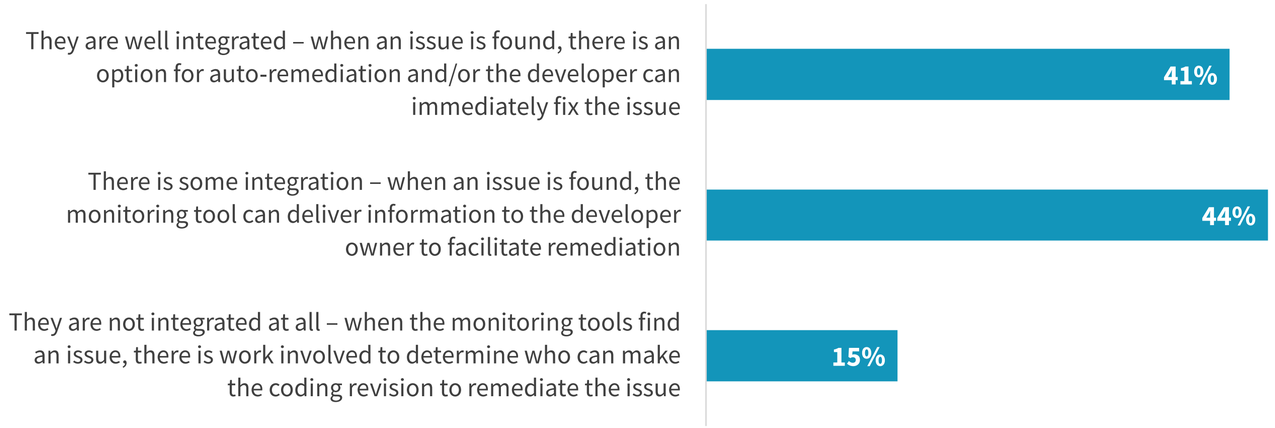
» Manner in which security tools work within developer tools and workflows.



Security Monitoring Tools Integration with Development Processes

Organizations are integrating their monitoring solutions with developer-focused security tools to speed remediation. This is a good practice to ensure that if a security issue is found in runtime, it can be efficiently remediated without requiring as much time from both security and development teams. When successfully integrated, the developer can efficiently remediate the issue without needing help from the security team.

» Level of integration between cloud security monitoring solutions and development processes.



Back to Contents

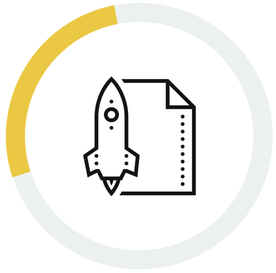
Top Challenges for Security Testing in Development

Organizations are adopting various tools as part of their burgeoning developer-focused security strategies, including the use of third-party penetration testing tools or consulting services to help ensure that their applications are secure. While security teams are trying to shift security testing left to developers, they face many challenges, mainly around gaining the visibility and control they need to make sure that the testing has been done and developers can make needed changes without disrupting processes.

» Usage of third-party penetration testing solutions or consulting services to ensure cloud-native application security.

Yes, for all applications,

71%



Yes, but only for business-critical applications

27%

An additional 1% said they **don't** use these services.

» Challenges with security testing for development team(s).

Back to Contents

Organizations Are Investing in Securing Development Processes

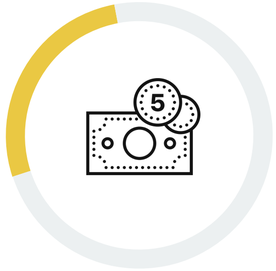
Organizations Are Investing in Securing Development Processes

Looking ahead, more than two-thirds (69%) of organizations are planning to make significant investments in security solutions that can be integrated into their cloud-native software development processes. In terms of where these investments are being directed, more than one-third (34%) identified improving application security testing, while 31% said detecting secrets stored in source code repositories and/or applying runtime API security controls.

» Plans to invest in security solutions that can be integrated into cloud-native software development processes.

We expect to make **significant investments,**

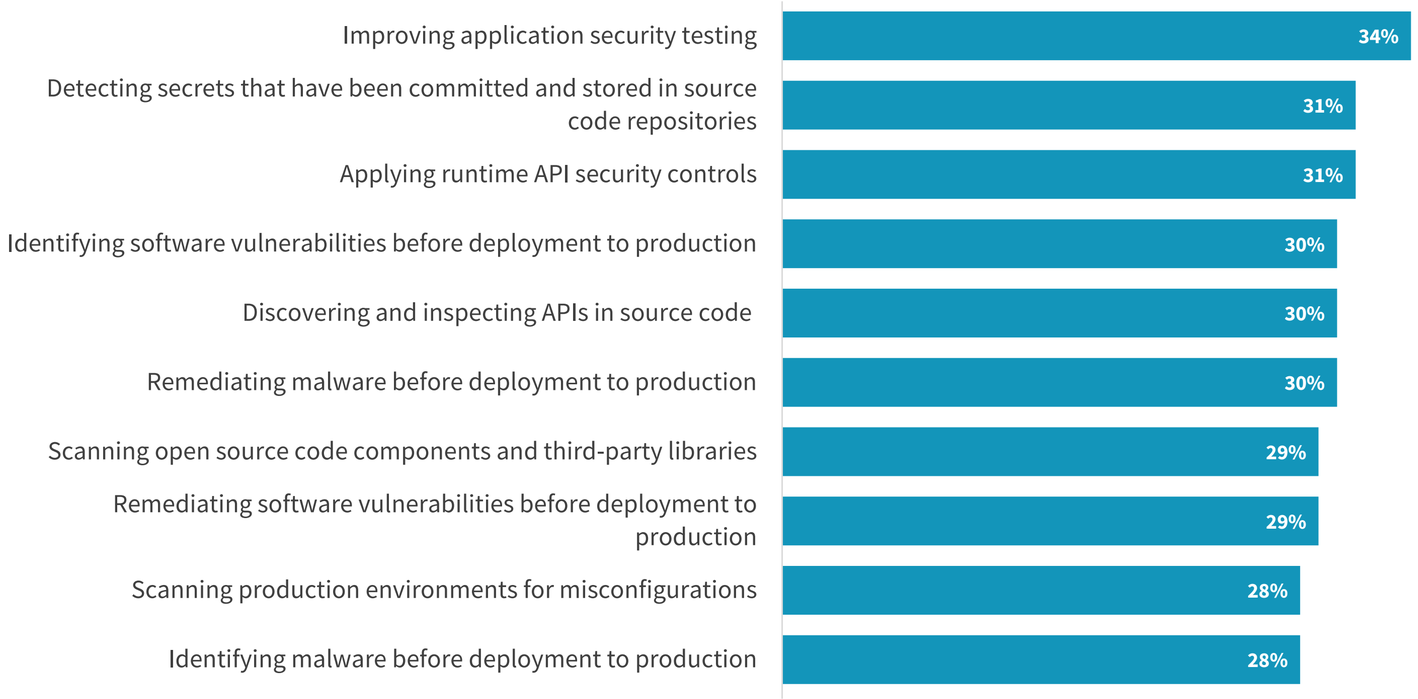
69%



We expect to make **moderate investments,**

31%

» Top ten priorities for securing cloud-native software development processes.



Back to Contents

SYNOPSYS®

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

LEARN MORE

ABOUT ESG

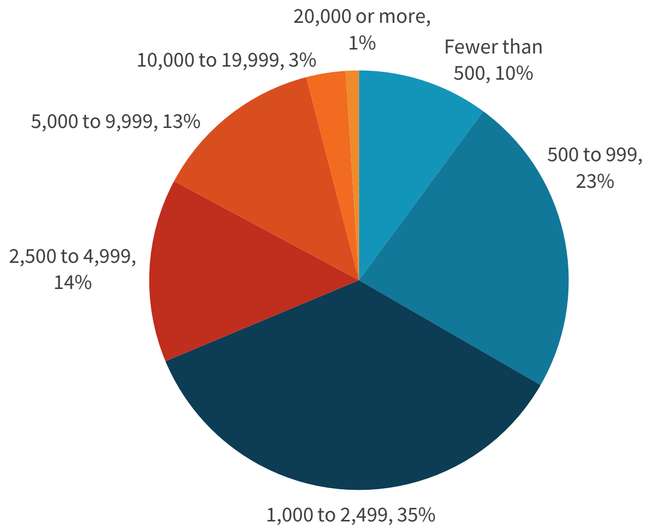
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology

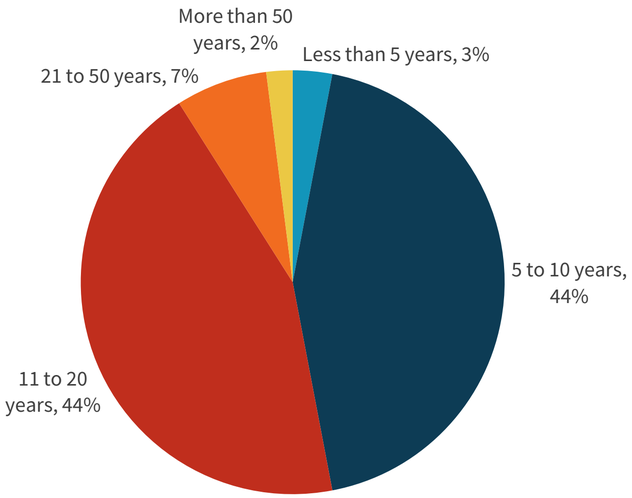
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals, as well as application developers, from private- and public-sector organizations in North America between May 18, 2022 and June 10, 2022. To qualify for this survey, respondents were required 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 350 IT, cybersecurity, and application development professionals.

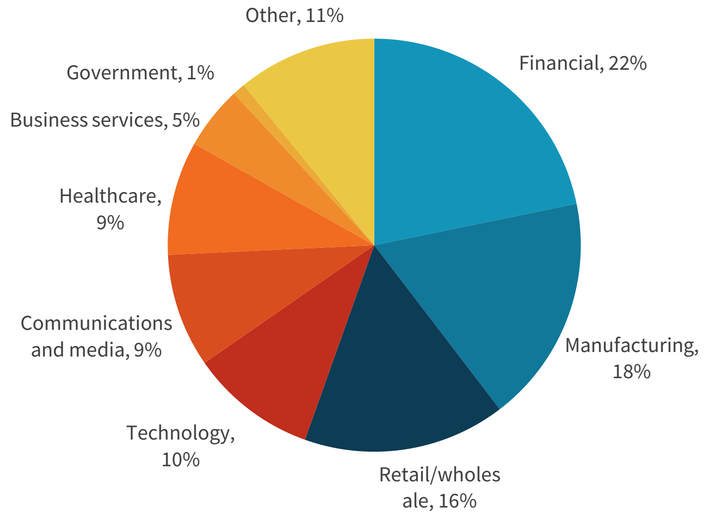
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



Back to Contents

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.