Enterprise Strategy Group by TechTarget

Modernizing Application Security to Scale for Cloud-native Development

Melinda Marks | Practice Director

ENTERPRISE STRATEGY GROUP

AUGUST 2024

Research Objectives

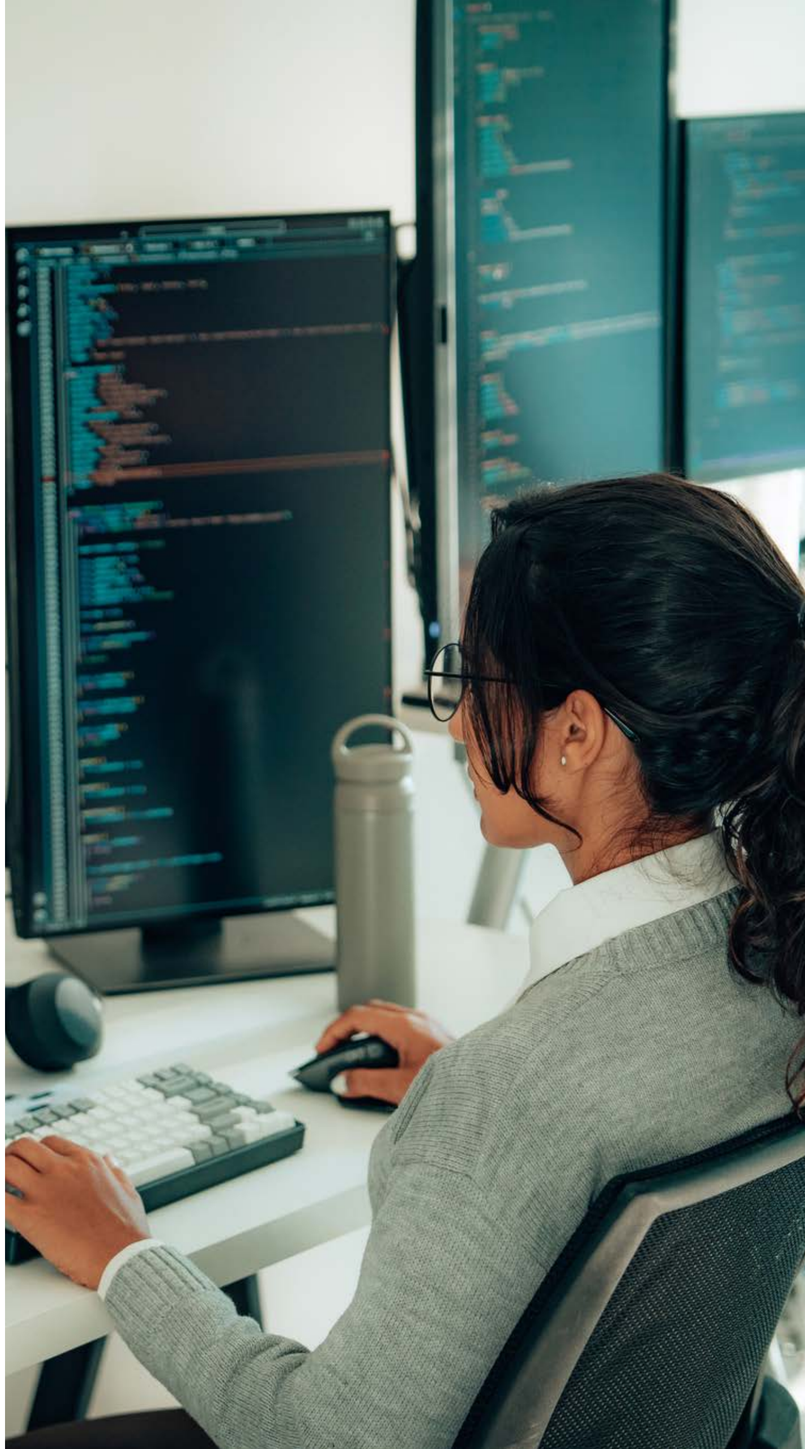
As organizations are under increasing pressure to boost productivity and gain a competitive advantage, they are modernizing application development processes. However, as the adoption of new technologies helps them scale software development for greater speed and volume of releases, security teams need to keep pace to effectively manage risk and protect applications from threats.

Traditional application security methods may be disruptive or even slow down development processes. As development teams scale using cloud-native technologies and modernized processes, the higher chance for mistakes creates software vulnerabilities that leave them susceptible to attack. Security teams need a modernized approach to efficiently incorporate security tools and processes across the software development lifecycle while promoting business growth by supporting development as it scales.

To gain insights into these trends, TechTarget's Enterprise Strategy Group surveyed 350 IT, cybersecurity, and application development professionals in North America (US and Canada) responsible for evaluating, purchasing, and utilizing developer-focused security products.

THIS STUDY SOUGHT TO:

- **Identify** development trends driving the need to modernize application security programs.
- **Determine** recommendations and strategies to help application security teams scale to support growth.
- **Evaluate** the top concerns, challenges, and incidents that application security teams have faced with their current tools.
- **Assess** the plans, investment priorities, and team involvement needed to modernize application security.



Key Findings

The Move to Cloud-native Workloads Begets Infrastructure-as-code Adoption and Open Source Software Usage

PAGE 4

Organizations Are Increasing Efforts to Incorporate Security Into Development Processes

PAGE 9

Security Teams Need to Be Equipped to Address Application Security Concerns

PAGE 12

Cloud-native Applications Present Many Cybersecurity Challenges

PAGE 15

Application Security Roles and Responsibilities Dynamics Convey the Need for Cross-team Collaboration

PAGE 19

Organizations Are Investing in Efforts to Modernize Application Security Programs

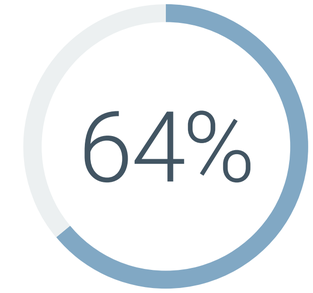
PAGE 23

The Move to Cloud-native Workloads Begets Infrastructure-as-code Adoption and Open Source Software Usage

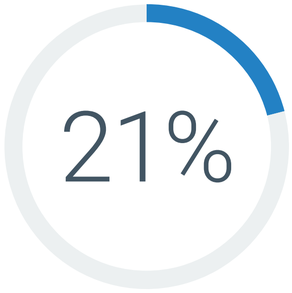
Most Use or Plan to Use Generative AI or Chatbot Tools for Code Development

Nearly all (97%) respondent organizations are currently using, planning to use, or interested in using generative AI (GenAI) or chatbot tools to save time and speed up development. Security teams need to ensure they can support these newer technologies to enable secure usage.

Usage of GenAI as an aid for code development.

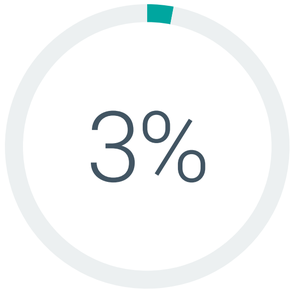


We are currently using it



We plan to use it

We are interested in using it



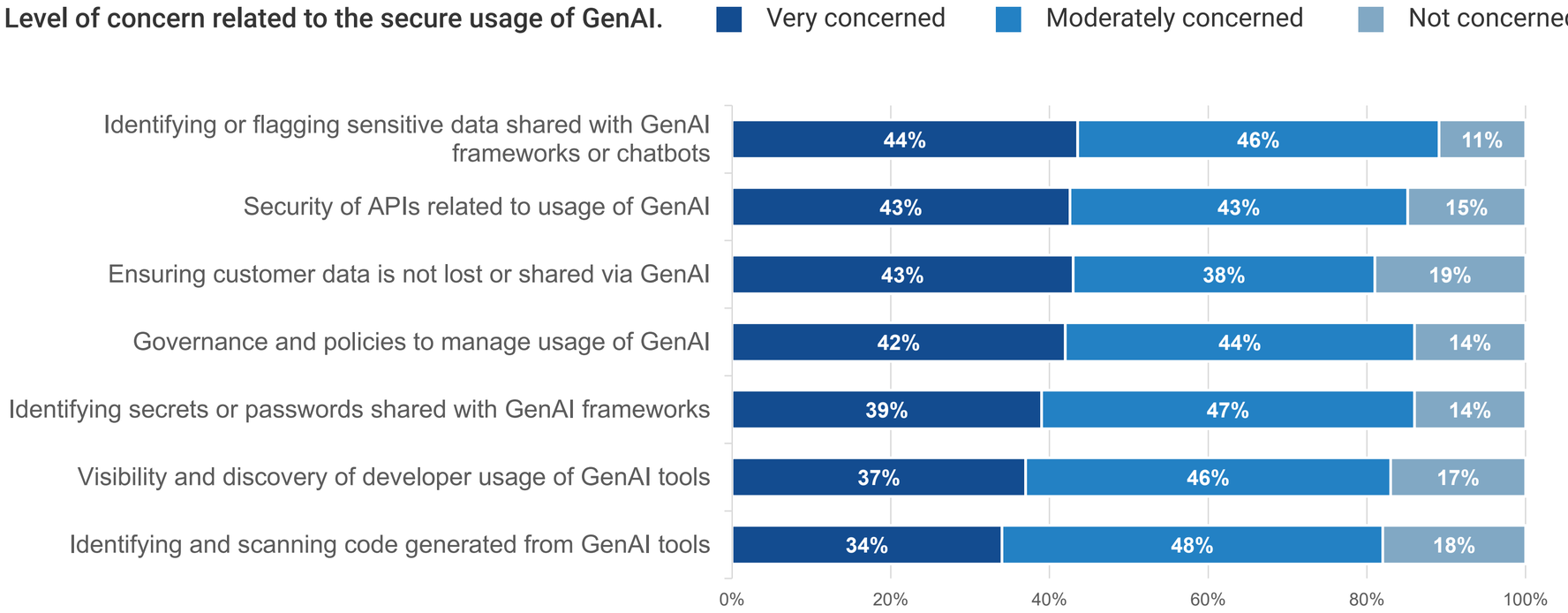
We have no plans to use it

"Nearly all (97%) respondent organizations are currently using, planning to use, or interested in using generative AI (GenAI) or chatbot tools to save time and speed up development."

Level of Concern Around GenAI and Chatbot Usage

When asked about the usage of or plans for GenAI to aid in code development, respondents showed a wide range of concerns. This presents opportunities for security vendors to address these areas, including flagging sensitive data shared outside of organizations, securing APIs, protecting customer data, and addressing governance and polices to manage secure usage.

Level of concern related to the secure usage of GenAI.



"When asked about the usage of or plans for GenAI to aid in code development, respondents showed **a wide range of concerns**."

BACK TO CONTENTS

High Usage of Open Source Code Confirms Importance of Software Supply Chain Security

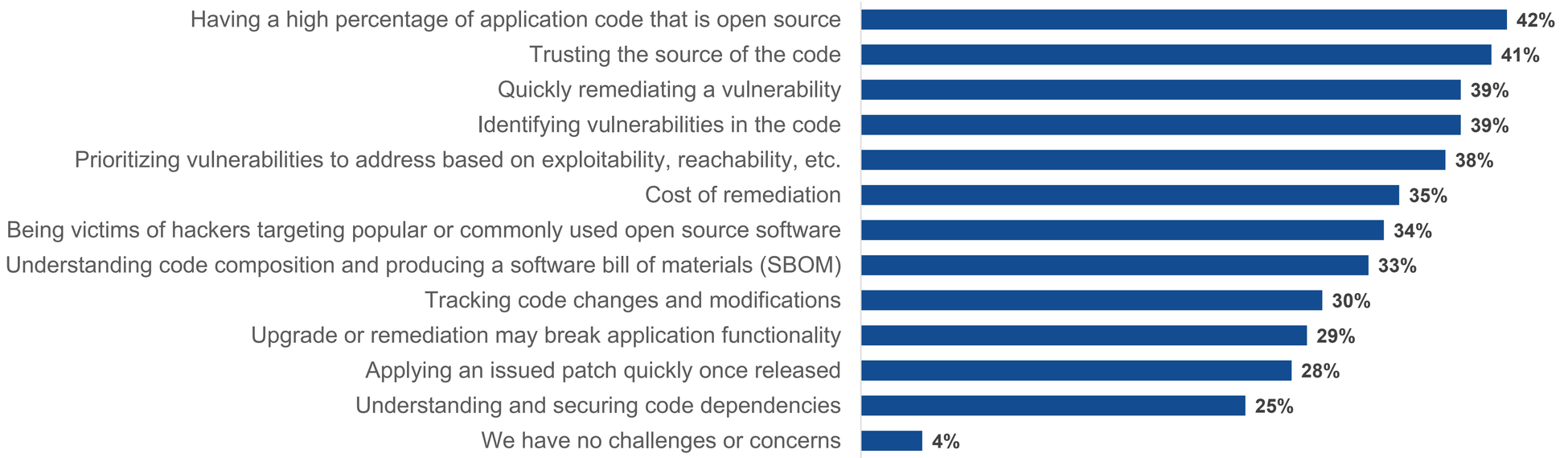
Nearly all organizations are using or planning to use open source software (OSS) in their cloud-native applications. This helps speed development processes because developers can save time by utilizing existing code to build their applications.

Composition of cloud-native applications with respect to the use of open source software.

- 70% — We currently use open source software
- 24% — We plan to use open source software in the next 12 months
- 5% — We are interested in using open source software
- 1% — We have no plans to use open source software

The increased OSS usage poses security risks because if hackers find vulnerabilities to exploit in OSS, they have a large number of targets to attack. As a result, nearly all organizations face a wide range of challenges and concerns related to securing their OSS. This underscores the importance of fully understanding all software code components and securing the software supply chain.

Challenges organizations have faced using OSS.



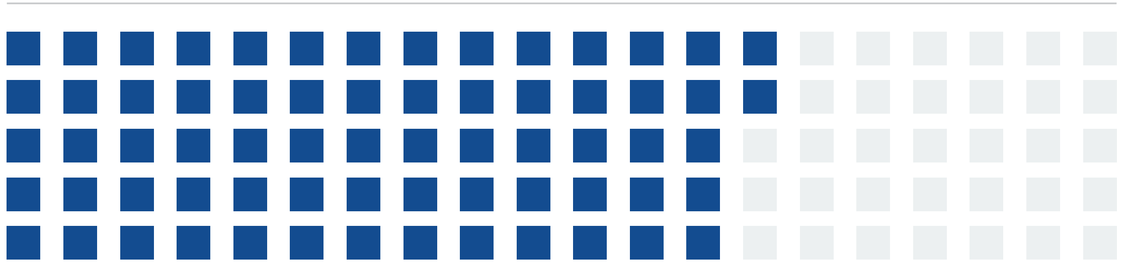
BACK TO CONTENTS

High Usage of Infrastructure-as-code Has Come With Increased Template Misconfigurations

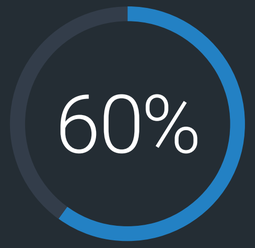
Organizations are increasingly using infrastructure-as-code (IaC) as a useful tool to simplify infrastructure provisioning and easily deploy software applications. Indeed, six in ten organizations currently use IaC, with an additional 27% planning to use these templates in the next 12 months. The technology enables developers to provision their own infrastructure so they don't have to wait for IT or operations teams to perform these functions. They typically use the code from templates to declaratively script the cloud infrastructure needed, managing resources such as networking, compute services, and storage.

However, with increased IaC adoption, misconfigurations can be magnified because any flaws are easily proliferated if not addressed. This represents another key area for modern application security to address.

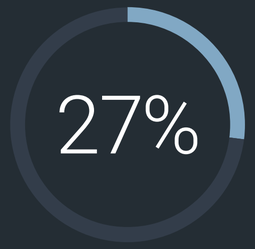
67%
are experiencing an **increase** in IaC misconfigurations



Usage of IaC templates.

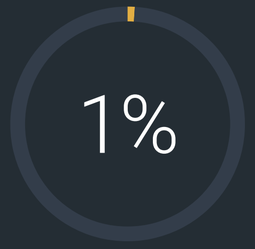


We currently use IaC templates to provision cloud infrastructure



We plan to use IaC templates in the next 12 months

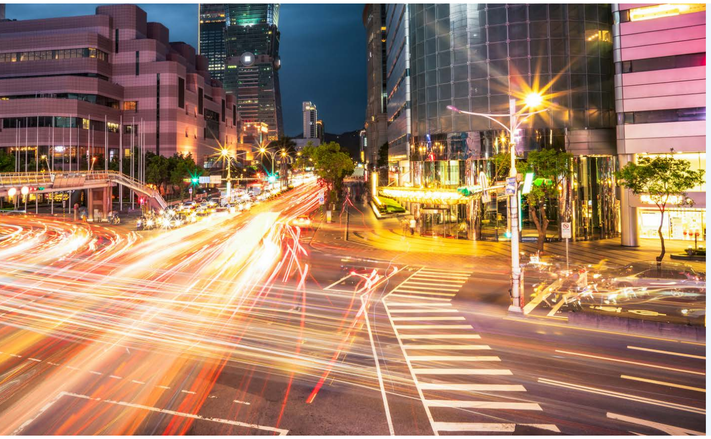
We are interested in using IaC templates



We have no plans to use IaC templates

BACK TO CONTENTS

Organizations Are Increasing Efforts to Incorporate Security Into Development Processes



Organizations Pervasively Use or Plan to Use DevOps

Organizations are moving to DevOps methodologies leveraging cloud-native tools to automate continuous integration and continuous deployment (CI/CD) and drive efficiency in software development processes. Development teams can more easily collaborate using CI/CD pipeline tools, checking code out to work on it and checking it back in when finished. Application deployment is also simpler, and when updates are needed, developers can check out their code, make changes, and update their applications. This speeds up software development and enables continuous updates to optimize innovation and deliver feature-rich applications. The research shows 55% of organizations employing DevOps, with an additional 15% planning to use it, and another 27% interested in DevOps. Only 3% did not have plans to use DevOps methodologies.

Status of DevOps to automate CI/CD for code and application infrastructure.

31%	24%	15%	27%	3%
We employ DevOps extensively	We employ DevOps in a limited fashion	We plan to employ DevOps in the next 12-24 months	We are interested in DevOps	We do not employ DevOps and have no plans to do so

BACK TO CONTENTS

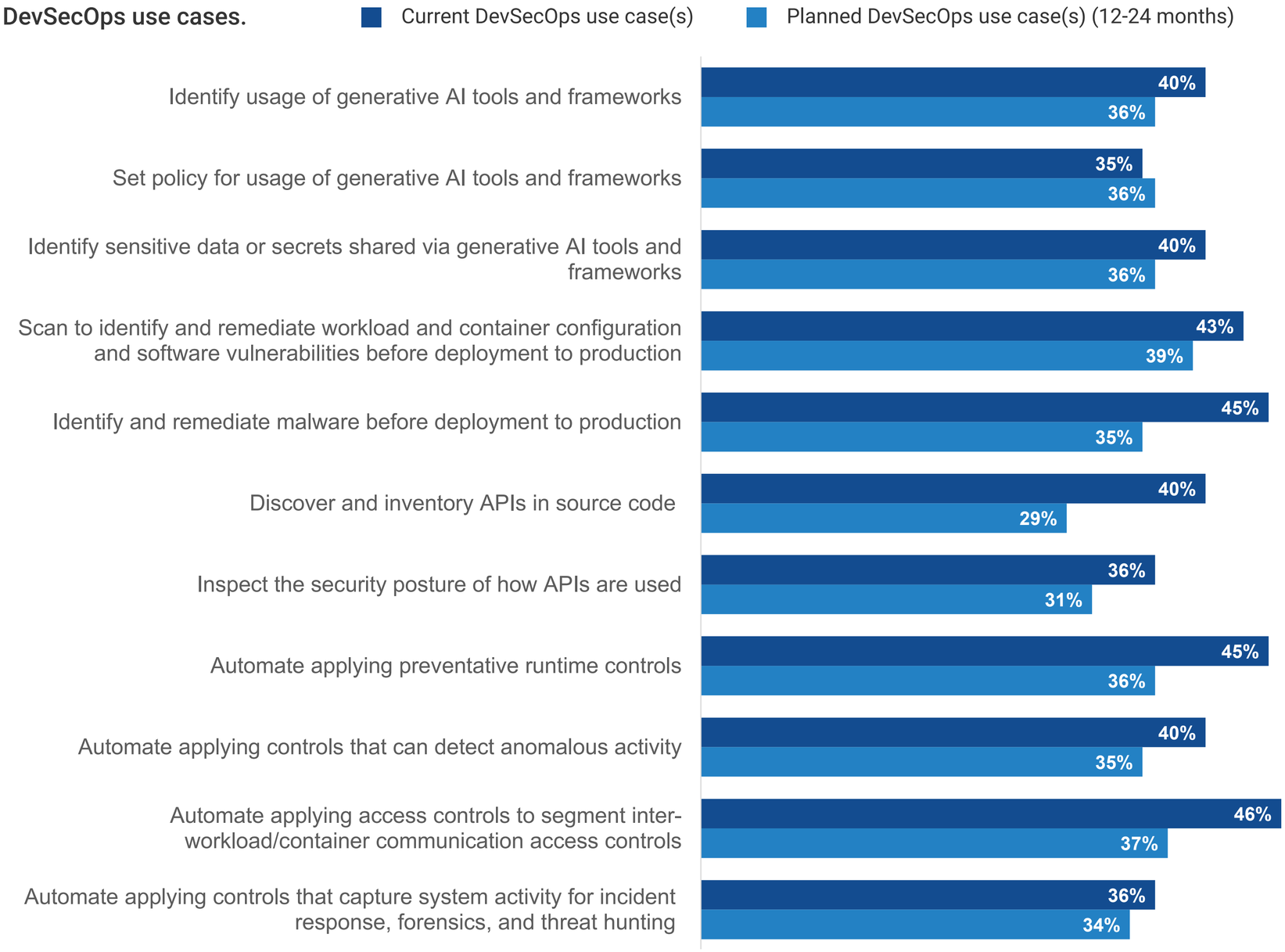
Incorporating Security From Build Time to Runtime

Organizations are making efforts to incorporate security processes into DevOps processes (DevSecOps) so that the faster release cycles and updates do not expose them to an unmanageable amount of security risk. A wide range of security practices is used in DevOps processes throughout the software development lifecycle, spanning from early development to runtime.

Practices incorporated earlier in development can mitigate risk by catching and remediating issues before the application is deployed.

In runtime, security practices are important to identify and mitigate vulnerabilities as quickly as possible to protect running applications.

DevSecOps use cases.



BACK TO CONTENTS

Security Teams Need to Be Equipped to Address Application Security Concerns

Top Challenges for Application Security Teams

Application teams face a number of challenges, showing the need for them to modernize their approach.

These challenges include understanding and managing risk for GenAI, improving program effectiveness, understanding developer environments and assets, keeping up with the speed and volume of releases, and prioritizing remediation.

These challenges also emphasize the need to align with development and DevOps teams so they can better collaborate.

Biggest challenges for application security teams supporting cloud-native development processes.

45%

Understanding and managing risk related to usage of generative AI (GenAI)

42%

Measuring and improving application security program effectiveness

41%

Understanding developer environments and assets to effectively manage security

40%

Keeping up with speed and volume of releases

39%

Prioritizing remediation actions needed to have the highest impact on mitigating risk

38%

Securing the multiple elements of the software supply chain

38%

Gaining visibility of the attack surface from code development to production

35%

Getting information needed for compliance with security regulations

32%

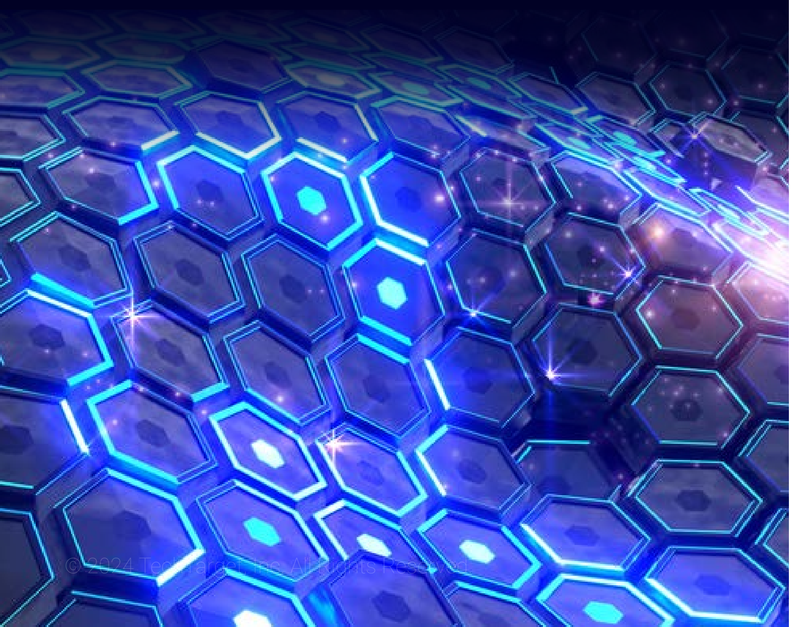
Making sense of and correlating testing results from multiple tools

BACK TO CONTENTS

Remediation Challenges in Runtime

The research shows that nearly all organizations face challenges fixing vulnerabilities after applications are deployed. This underscores the importance of incorporating security processes and tools in build processes to remediate issues before applications are deployed.

When the applications are running, security teams need help prioritizing what to fix, and they need to ways to work efficiently to remediate vulnerabilities to protect their applications from exposure to attacks.



Challenges fixing a security vulnerability after an application is deployed.

47%

Prioritizing and justifying application rework or security tasks during a development sprint or cycle

47%

Finding the origin of the vulnerability in the source code

39%

Finding the developer or owner who can remediate the code

35%

Too time consuming to test for regressions after a code fix

34%

Too many alerts that are likely false positives or unexploitable vulnerabilities

26%

Lack of remediation guidance

BACK TO CONTENTS

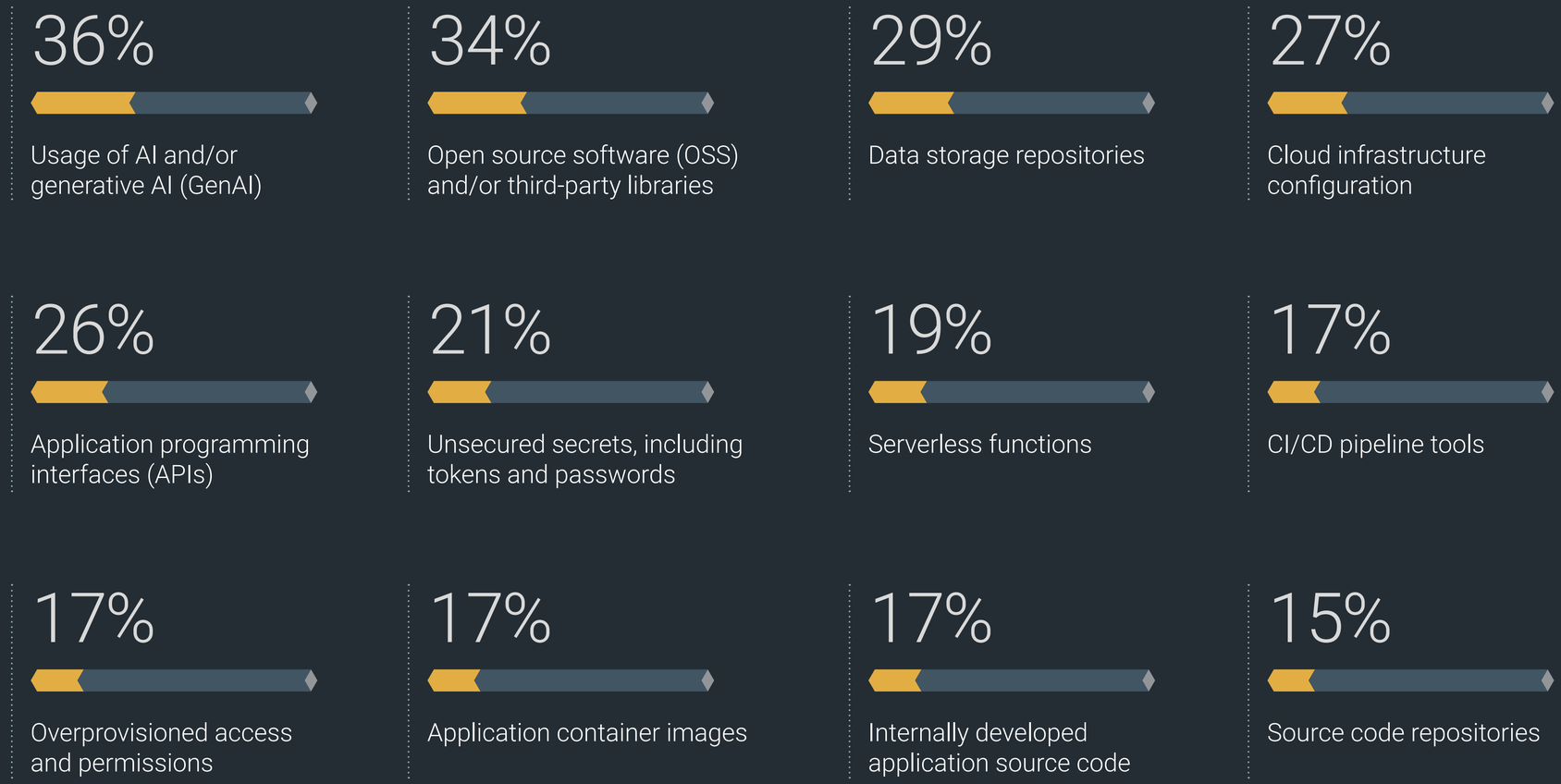
Cloud-native Applications Present Many Cybersecurity Challenges

Multiple Cloud-native Application Elements Are Susceptible to Compromise

Organizations express concern about the vulnerability of multiple elements of the cloud-native application stack, but the coming wave of AI usage was most commonly identified. OSS and/or third-party libraries, data storage repositories, cloud infrastructure, and APIs were also identified as susceptible to compromise.

Respondents are also concerned about areas related to how developers work. For example, there is concern around secrets, pipeline tools, access and permissions, containers, and source code repositories. While all these elements enable developers to work quickly, the chance for mistakes becomes greater as development scales.

Most vulnerable elements of the cloud-native application stack.



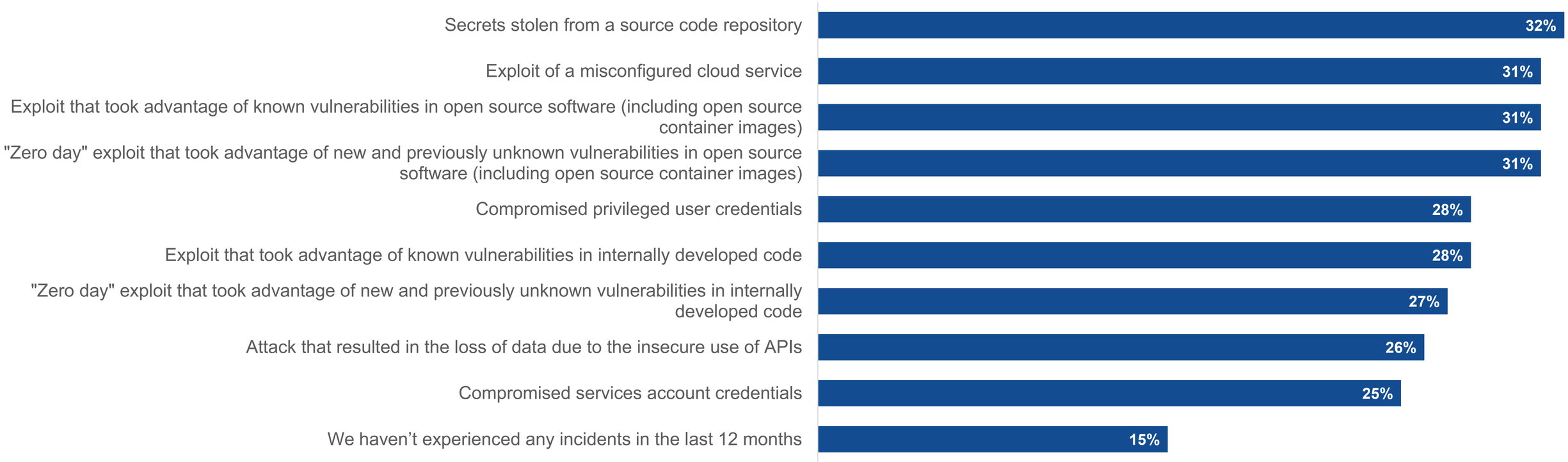
BACK TO CONTENTS

Cybersecurity Incidents Stemming From Cloud-native Applications

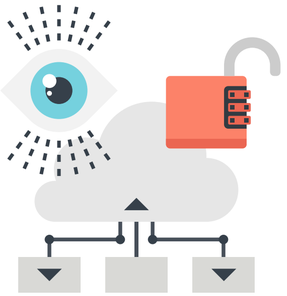
Despite reporting that they have a number of tools in place, the majority of organizations experienced a cybersecurity incident involving their cloud-native application stack in the last 12 months. These include stolen secrets, exploits of misconfigured cloud services, exploits of vulnerabilities, and compromised access issues.

Many of these should be preventable with the tools already in place, indicating the need for a modern approach that can scale with faster development processes.

Cybersecurity incidents experienced in the last 12 months caused by cloud-native applications.



BACK TO CONTENTS



Many Suffer Serious Effects From Cloud-native Application Security Incidents

The organizations that experienced cybersecurity incidents in their cloud-native application environments have felt an array of adverse effects. The incidents have had severe ramifications on the business, including data loss, business disruption, application downtime, customer data loss, malware, and compliance fines.

The fact that organizations suffered these impacts while having many security tools and processes in place emphasizes the need to ensure application security programs can support scale and growth.

Impacts of cybersecurity incidents caused by cloud-native applications.

41%	40%	39%	39%	38%
Data loss or exfiltration	Business process disruption	Application downtime	Customer data loss	Unauthorized access to sensitive information
30%	28%	28%	26%	2%
Malware moved laterally	Introduction of backdoors	Compliance violations and/or fines	Inability to meet service level agreements (SLAs)	None of the above

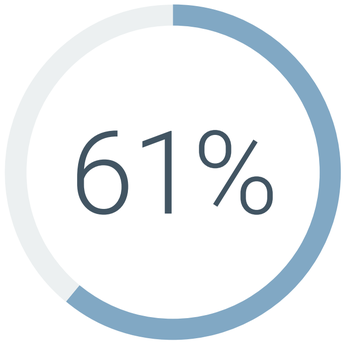
BACK TO CONTENTS

Application Security Roles and Responsibilities Dynamics Convey the Need for Cross-team Collaboration

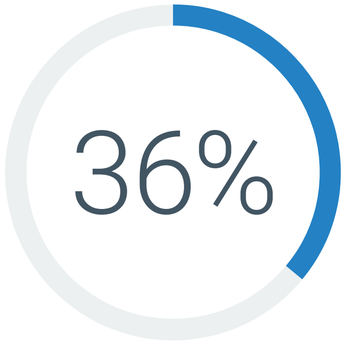
The Need for Developer-focused Security Solutions

In modernizing application security, organizations need to adopt developer-focused security solutions to enable business growth. It follows then that nearly two-thirds (61%) of organizations identify shifting some security responsibilities to developers as a *high priority.* This is important for enabling security team success in becoming facilitators of rapid development instead of adding friction or slowing operations down.

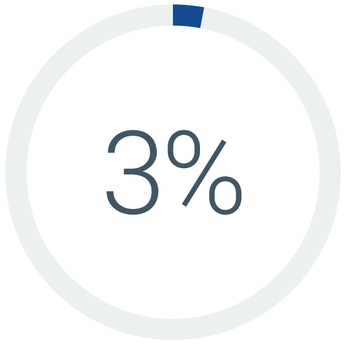
Priority level for adopting developer-focused security solutions.



It's a high priority



It's important but not a high priority



It's not a priority at all

"In modernizing application security, organizations need to adopt **developer-focused security solutions to enable business growth**."

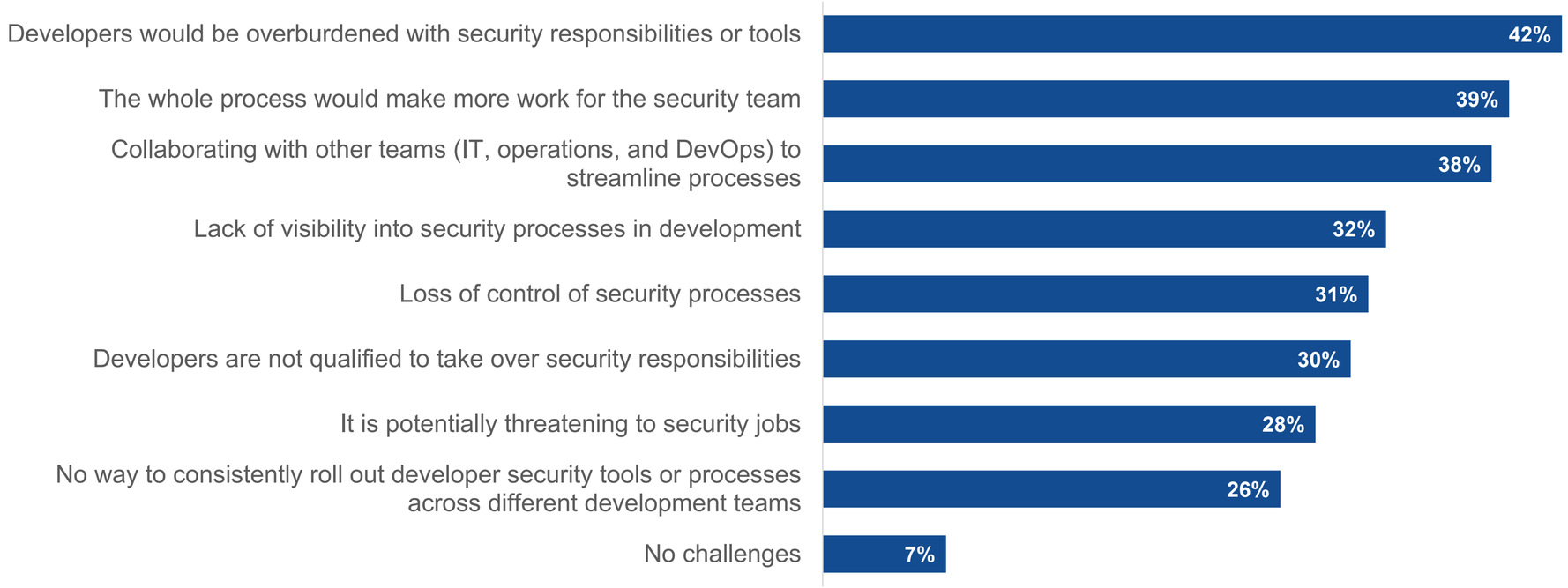
BACK TO CONTENTS

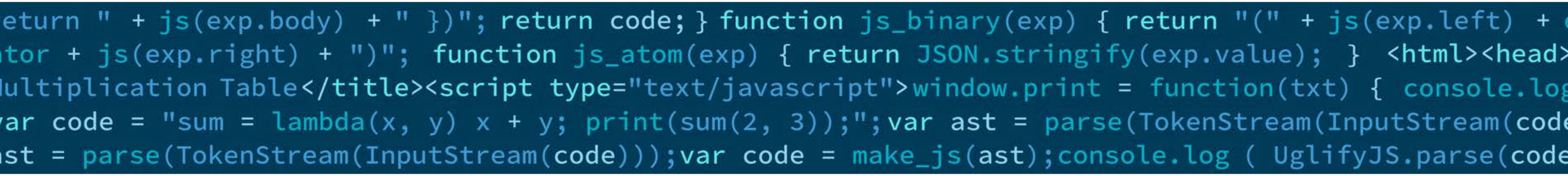
Helping Developers Secure Their Applications

Just as DevOps shifted operations left to enable developers to provision their own infrastructure, DevSecOps shifts security responsibilities left, empowering developers to secure their applications.

However, despite the obvious benefits associated with this approach, nearly all organizations face or expect to face challenges in giving developers more security responsibilities. The data indicates the need for solutions that make it easy for developers to secure their own code within their workflows, while enabling security teams to retain visibility and control even if developers are taking on more security tasks.

Challenges organizations face with giving developers more security responsibilities.





BACK TO CONTENTS

"The research shows potential room for improvement in **ensuring that security teams have visibility into the security testing for all applications**."

The Need for Visibility Into Security Testing in Development

The research shows potential room for improvement in ensuring that security teams have visibility into the security testing for all applications.

Specifically, more than half (59%) of organizations report their security teams have visibility into security testing for all applications, whereas 39% said they only have visibility for certain applications and 2% reported not having visibility into security testing status for applications.

Security teams' visibility into security testing statuses of applications.

They have **visibility for all applications**

They only have **visibility for certain applications**

They don't have visibility into security testing statuses of applications

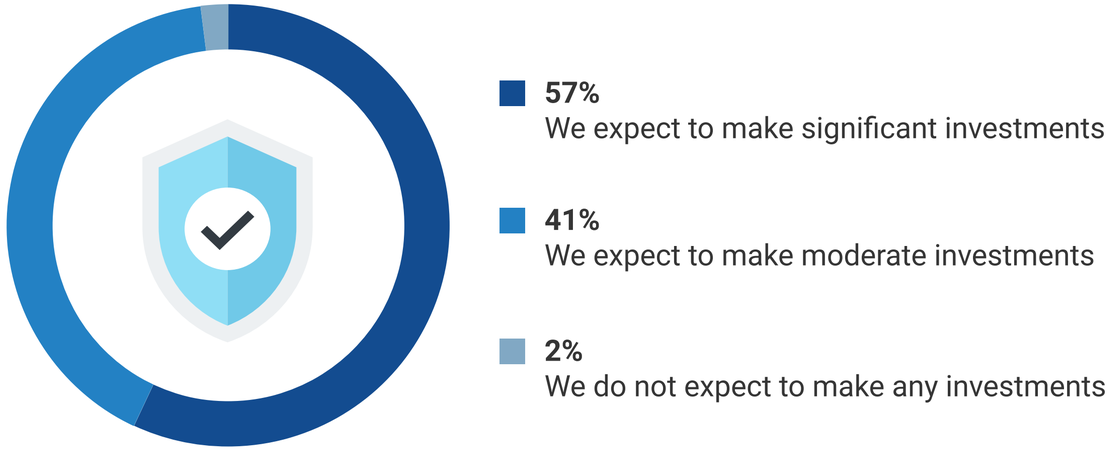
BACK TO CONTENTS

Organizations Are Investing in Efforts to Modernize Application Security Programs

Majority of Organizations Are Investing in Modernizing Application Security, With a Preference for Best-of-breed Tools From Multiple Vendors

Looking ahead, the vast majority of organizations are investing in efforts to modernize their application security, including 57% *making significant investments*. When asked about their preferences for selecting security tools, nearly half (48%) of respondents reported preferring best-of-breed security tools from multiple security vendors, while a third prefer integrated tools from a single vendor.

Investment plans to modernize approach to application security.



- **57%** We expect to make significant investments
- **41%** We expect to make moderate investments
- **2%** We do not expect to make any investments

Preference for selecting security tools to modernize application security programs.

- **48%** We prefer **best-of-breed** security tools from multiple security vendors
- **33%** We prefer **integrated** security tools from a single vendor
- **10%** We prefer using **open source** security tools
- **8%** We prefer a platform to enable us to use multiple tools from **multiple vendors and/or open source**

BACK TO CONTENTS

LEGIT SECURITY

ABOUT

Legit is a new way to manage your application security posture for security, product and compliance teams. With Legit, enterprises get a cleaner, easier way to manage and scale application security, and address risks from code to cloud. Built for the modern SDLC, Legit tackles the toughest problems facing security teams, including GenAI usage, proliferation of secrets and an uncontrolled dev environment. Fast to implement and easy to use, Legit lets security teams protect their software factory from end to end, gives developers guardrails that let them do their best work safely, and delivers metrics that prove the success of the security program. This new approach means teams can control risk across the business – and prove it.

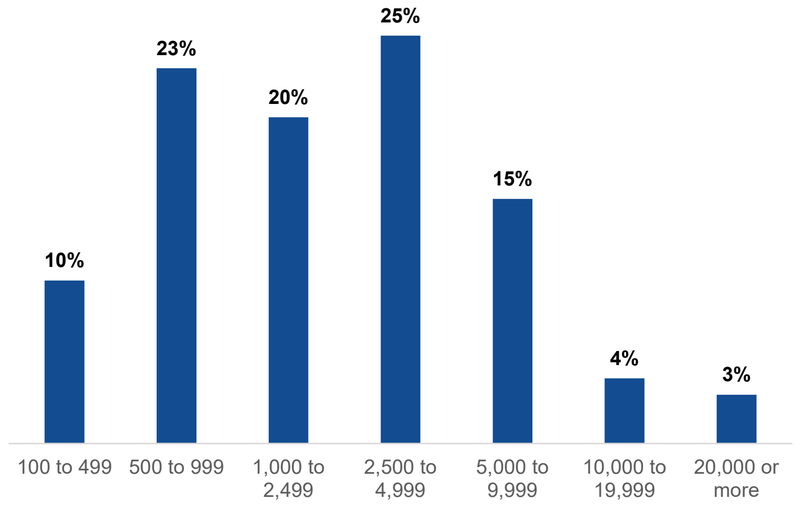
LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

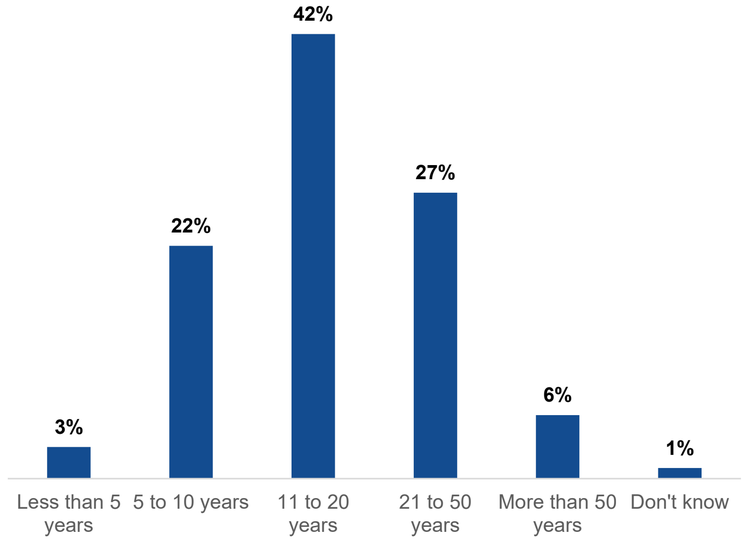
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America between May 20, 2024, and June 14, 2024. To qualify for this survey, 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.

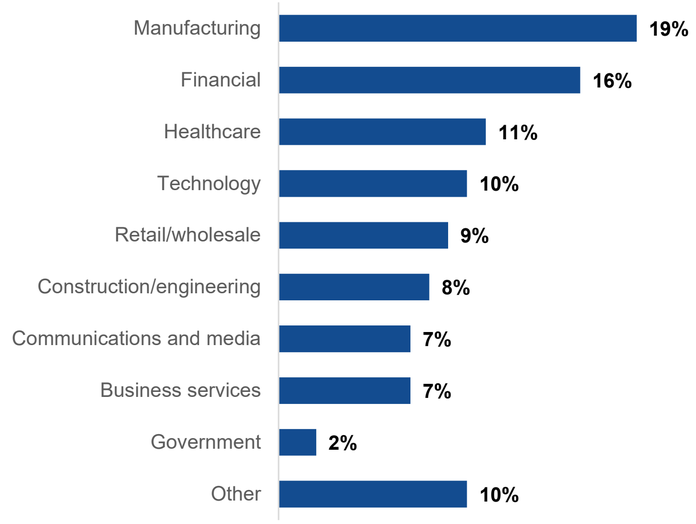
Respondents by number of employees.



Respondents by age of organization.



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.