Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

Modern Application Development Security

Dave Gruber, Senior ESG Analyst

AUGUST 2020

CONTENTS

Research Objectives 3

Research Highlights 4

Most think their application security program is solid, though many still push vulnerable code. 5

Multiple security testing tools are needed to secure the potpourri of application development and deployment models in use today. 11

Developer security training is spotty, and programs to improve developer security skills are lacking. 17

The proliferation of AppSec testing tools is an issue for many, with more than a third focusing investments on consolidation. 20

Organizations are investing, with more than half planning to significantly increase spending on application security over the prior year. 22

Research Methodology 26

Research Objectives

DevSecOps has moved security front and center in the world of modern development; however, security and development teams are driven by different metrics, making objective alignment challenging. This is further exacerbated by the fact that most security teams lack an understanding of modern application development practices. The move to microservices-driven architectures and the use of containers and serverless has shifted the dynamics of how developers build, test, and deploy code.

As a result, a convergence of application security tools is underway. Organizations are overwhelmed with the amount of and overlap in issues raised from multiple testing tools, complicating prioritization and mitigation, so integrated application security platforms are desired.

In order to gain insight into these trends, ESG surveyed 378 IT, cybersecurity, and application development professionals at organizations in North America (US and Canada) involved with securing application development tools and processes.

THIS STUDY SOUGHT TO:

Examine the buying intentions of application security teams regarding dev-time application security controls and gauge buyer preferences for different types of vendors' application security solutions.

Determine the extent to which security teams understand modern development and deployment practices, and where security controls are required to mitigate risk.

Understand the trigger points influencing application security investments and how decision makers are prioritizing and timing purchasing decisions.

Gain insights into the dynamics between development teams and cybersecurity teams with respect to the deployment and management of application security solutions.

Back to Contents

Research Highlights

Most think their application security programs are solid, though many still push vulnerable code.

Having a good application security program doesn't mean that organizations don't still push vulnerable code. The difference is that those that push such code do so knowingly and with a thorough understanding of the risks that they are taking. Application security requires a constant triage of potential risks, involving prioritization decisions that allow development teams to mitigate risk while still meeting key deadlines for delivery.

Multiple security testing tools are needed to secure the potpourri of application development and deployment models in use today.

As application security has matured, no single testing technique has helped development teams mitigate all security risk. This requires teams to employ multiple tools, often from multiple vendors, to secure the SDLC. Usage varies, as do the tools that organizations deem most important, but most organizations end up utilizing a "cocktail" of tools to satisfy their security needs.

Developer security training is spotty, and programs to improve developer security skills are lacking.

While most provide developers with some level of security training, more than 50% only do so annually or less often. While development managers are often responsible for this training, in many organizations, application security analysts carry the burden of performing remedial training for development teams or individual developers who have a track record of introducing too many security issues.

The proliferation of AppSec testing tools is an issue for many, with more than a third focusing investments on consolidation.

Like other categories of security controls, many organizations are employing so many tools that they are struggling to integrate and manage them. This reduces the effectiveness of the program and directs an inordinate amount of resources to managing tools. Nearly one-third of organizations are experiencing this issue and are therefore planning future investment to consolidate and simplify their tools proliferation.

Organizations are investing, with more than half planning to significantly increase spending on application security over the prior year.

While 44% plan on targeting application security investments toward cloud, one-third are focused on consolidation of tools to simplify the process. Others plan to invest in expanding the use of testing tools to a higher percentage of their development teams and applications.

Back to Contents

Most think their application security program is solid, though many still push vulnerable code.

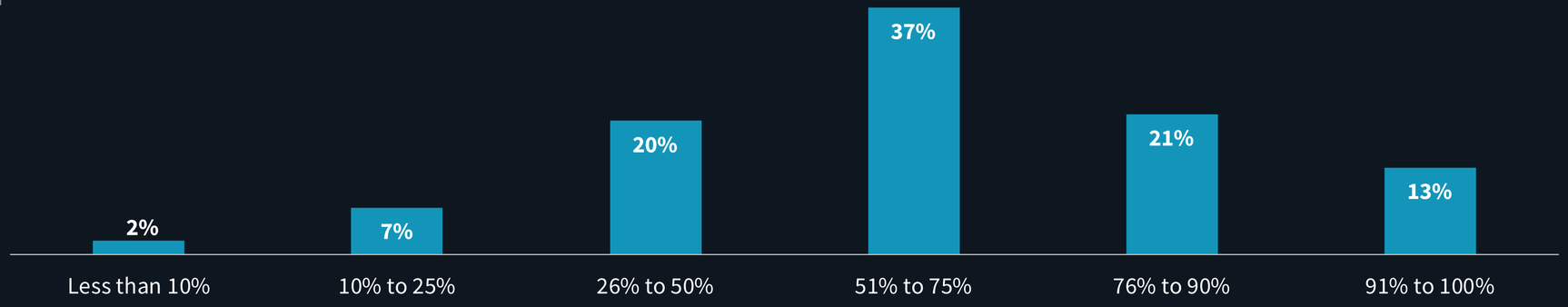
Most Think Their Application Security Program Is Pretty Good

Most organizations think that their application security programs are pretty good, with more than a third providing a rating of 9 or 10, and an overall mean of 7.92. This favorable assessment reflects continued investment and coverage levels in application security programs over the past few years. Still, code coverage is far from complete, with only 34% using AppSec tools on more than three-quarters of their codebase.

36%

give their application security programs a rating of 9 or 10

Codebase protected by AppSec tools

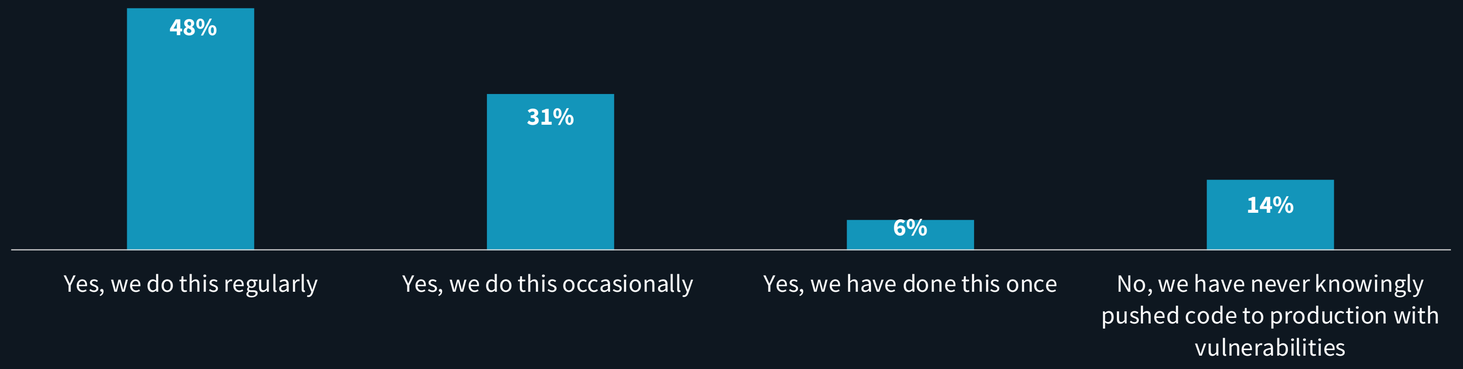


Back to Contents

Despite Good Programs, Most Still Regularly Push Vulnerable Code

Having a good application security program doesn't mean that organizations don't still push vulnerable code. The difference is that those that push such code do so knowingly and with a thorough understanding of the risks that they are taking. Application security requires a constant triage of potential risks, involving prioritization decisions that allow development teams to mitigate risk while still meeting key deadlines for delivery. Note that vulnerabilities discovered too late in the cycle often don't get mitigated, reinforcing the importance of shifting application security as far left as possible to leave enough runway to resolve critical issues in time for delivery.

Do organizations push vulnerable code?



Why organizations push vulnerable code

Back to Contents

Most Still Experience Exploits

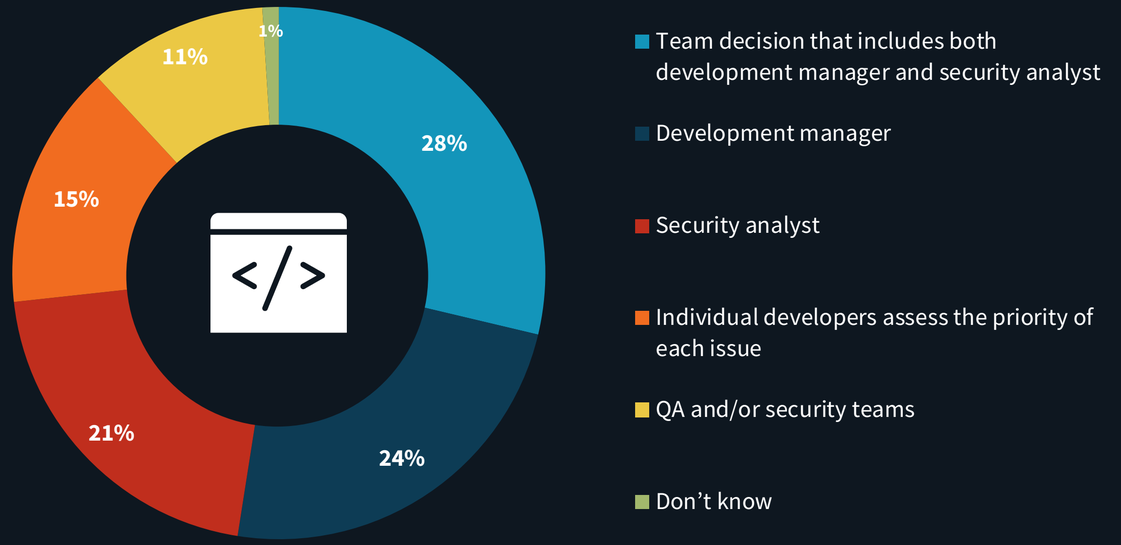
While increased investment in AppSec programs is reducing risk, 60% still report exploits from OWASP top-10 vulnerabilities. These exploits aren't necessarily tied to code where known vulnerabilities were identified, but this highlights the diligence that is required, including code coverage, testing frequency throughout the SDLC, and prioritization of identified vulnerabilities.

60%

have had production applications exploited by OWASP top-10 vulnerabilities in the past 12 months

So who makes the decision to ship code with known vulnerabilities? While many share this decision between a development manager and the security analyst, many teams leave the final decision to a single, responsible person. This reflects a variation in how different development organizations manage the overall application security process, with some putting ownership on the security team while others hold the development manager accountable.

Who makes the decision to push code?

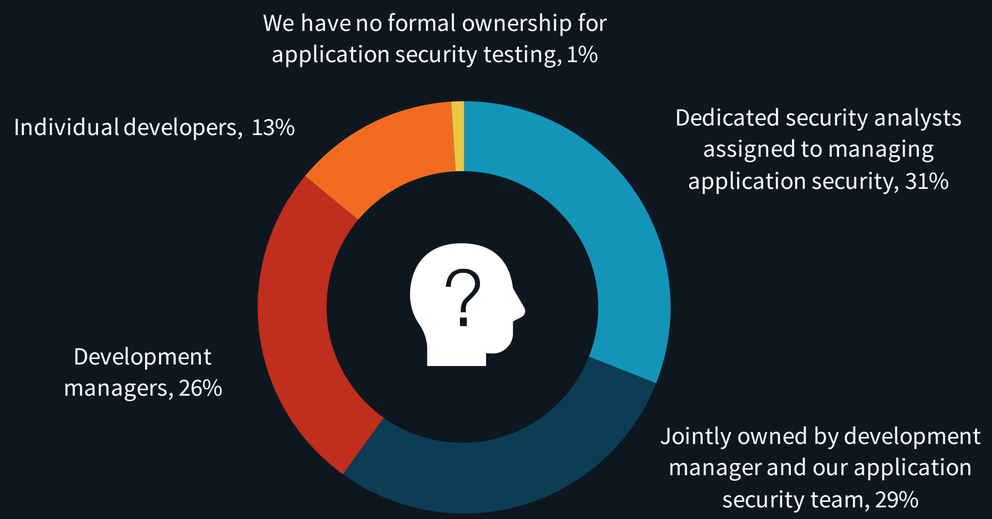


Back to Contents

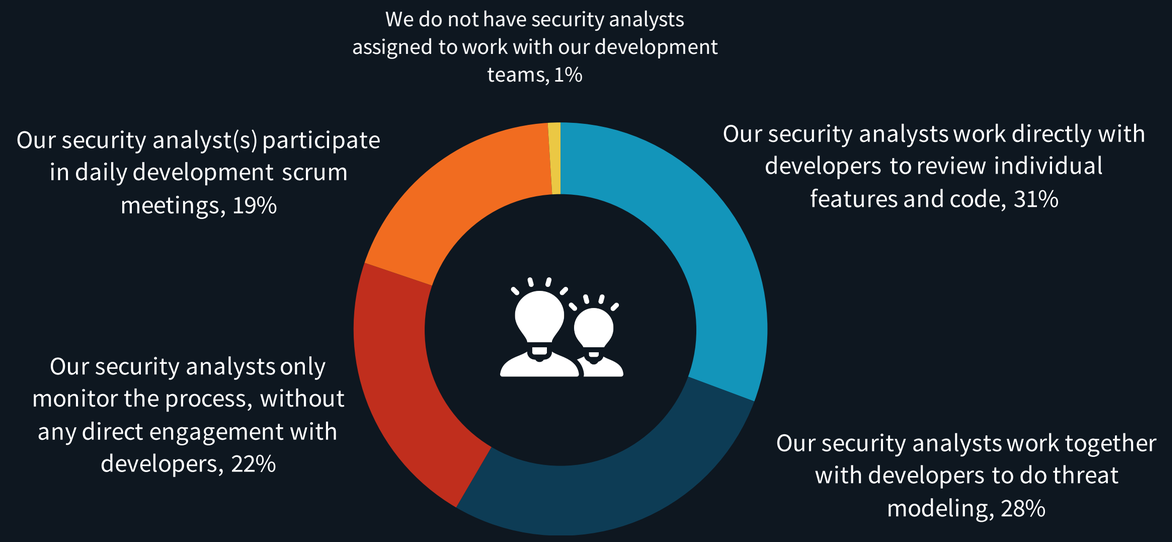
Security Analysts Are Increasingly Involved with AppSec Testing

In most organizations, the development manager or the application security analyst is responsible for the testing program, while 29% of organizations report that they jointly are responsible for the program. Security analysts play a major role in helping developers build applications securely. 78% of organizations report that their security analysts are directly engaged with their developers: 31% work directly with developers to review individual features and code, 28% work with developers to do threat modeling, and 19% participate in daily scrums. This high level of engagement drives both learning and oversight to ensure applications are built securely.

Application security testing ownership



How security analysts are helping to improve programs



Back to Contents

10 Elements of the **Most Effective** AppDev Security Programs

1. Application security controls are highly integrated into the CI/CD toolchain.
2. Application security best practices are formally documented.
3. Application security training is included as part of the ongoing development security training program.
4. Development managers are responsible for communicating best practices to developers.
5. A high percentage of developers participate in formal application security training programs.
6. Security issue introduction is tracked for individual development teams.
7. Formal processes and metrics track continuous improvement of application security.
8. Continuous improvement metrics are tracked for individual development teams.
9. Security issues are tracked during the code development process.
10. Automated risk aggregation tools roll up risk to keep senior development leaders informed.

Back to Contents

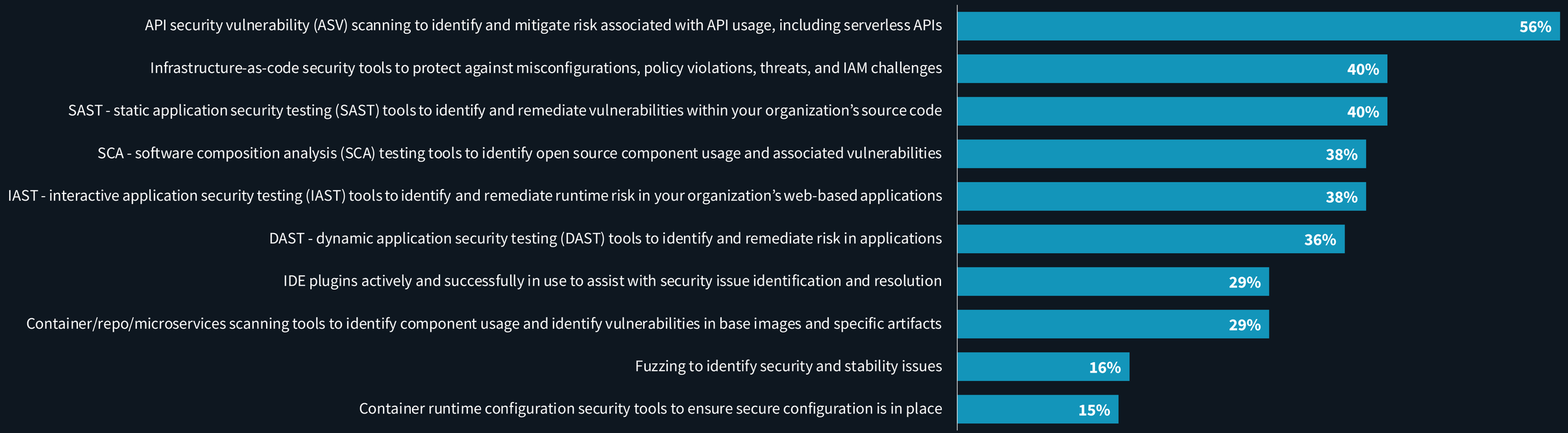
Multiple security testing tools are needed to secure the potpourri of application development and deployment models in use today.

A Wide Variety of AppSec Testing Tools Are in Use

As application security has matured, no single testing technique has helped development teams mitigate all security risk. This requires teams to employ multiple tools, often from multiple vendors, to secure the SDLC. Usage varies, as do the tools that organizations deem most important, but most organizations end up utilizing a "cocktail" of tools to satisfy their security needs.

As new development and deployment models emerge, new testing tools emerge to secure them. Some matriculate back into broader testing platforms while others stand alone for the long haul.

Application security testing ownership

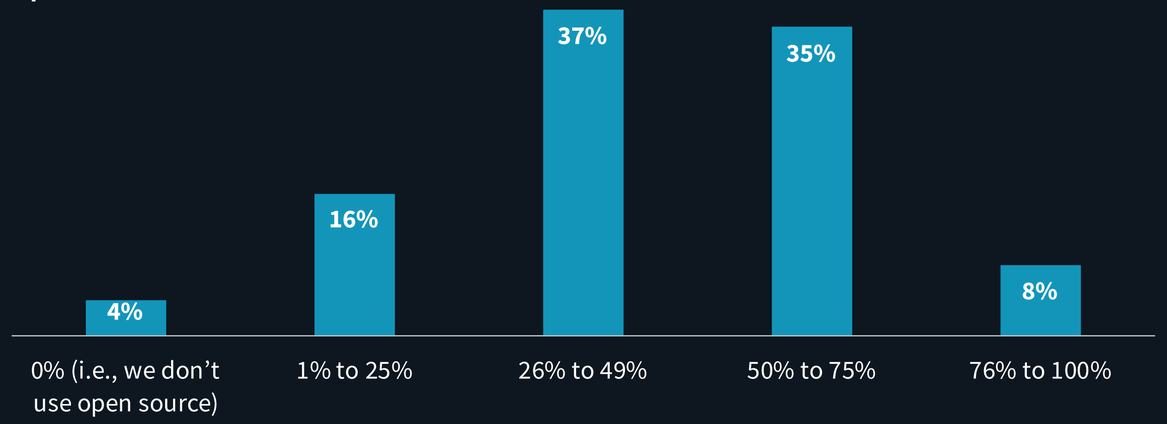


Back to Contents

Modern Codebases Are Heavily Dependent on Open Source, But Less Than Half Are Currently Using Open Source Security Controls

While different types of testing tools have been around for years, adoption is still not where it should be. For example, while the use of open source software in modern application development is significant, still less than half of development teams report currently utilizing open source security testing tools. While many have plans to do so, this unsettling trend demonstrates the current state of application security testing adoption in many companies today.

Percentage of codebase pulled from open source



48%

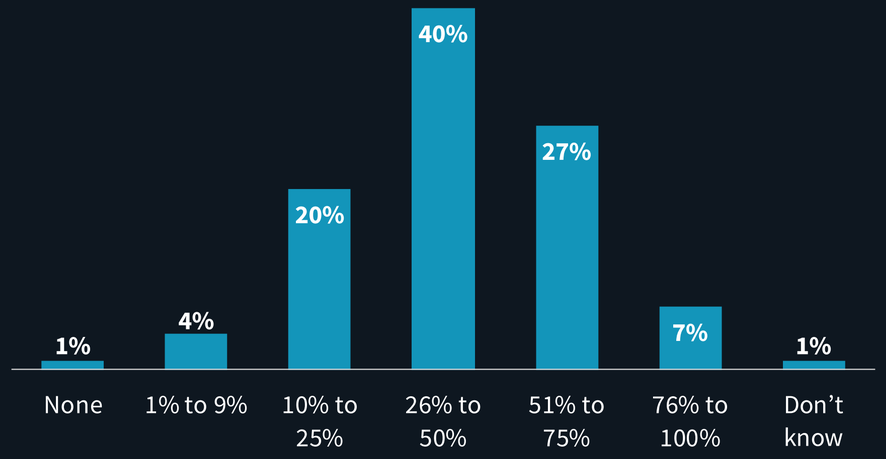
have already invested in specific security controls to scan for open source vulnerabilities.

Back to Contents

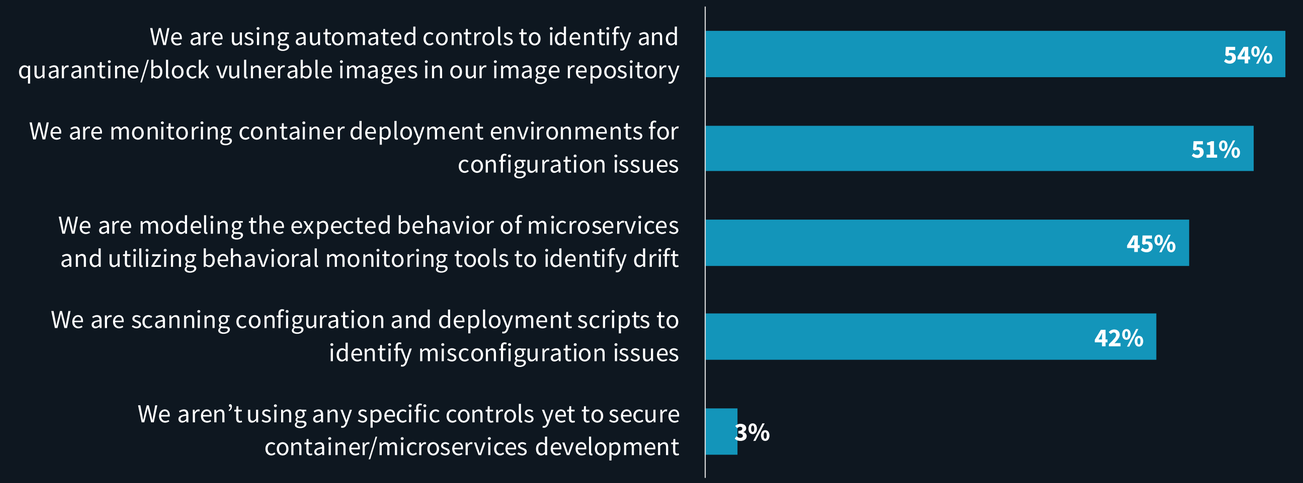
Microservices Container Development Is Gaining Steam

In some cases, more modern development and deployment models get security attention sooner. Here we see that microservices container development has become widely adopted in a relatively short period of time, and that the use of specific security controls has followed along with it. Other cloud development and deployment models are seeing similar patterns of adoption.

Percentage of development teams using containers



Controls in place to secure containers



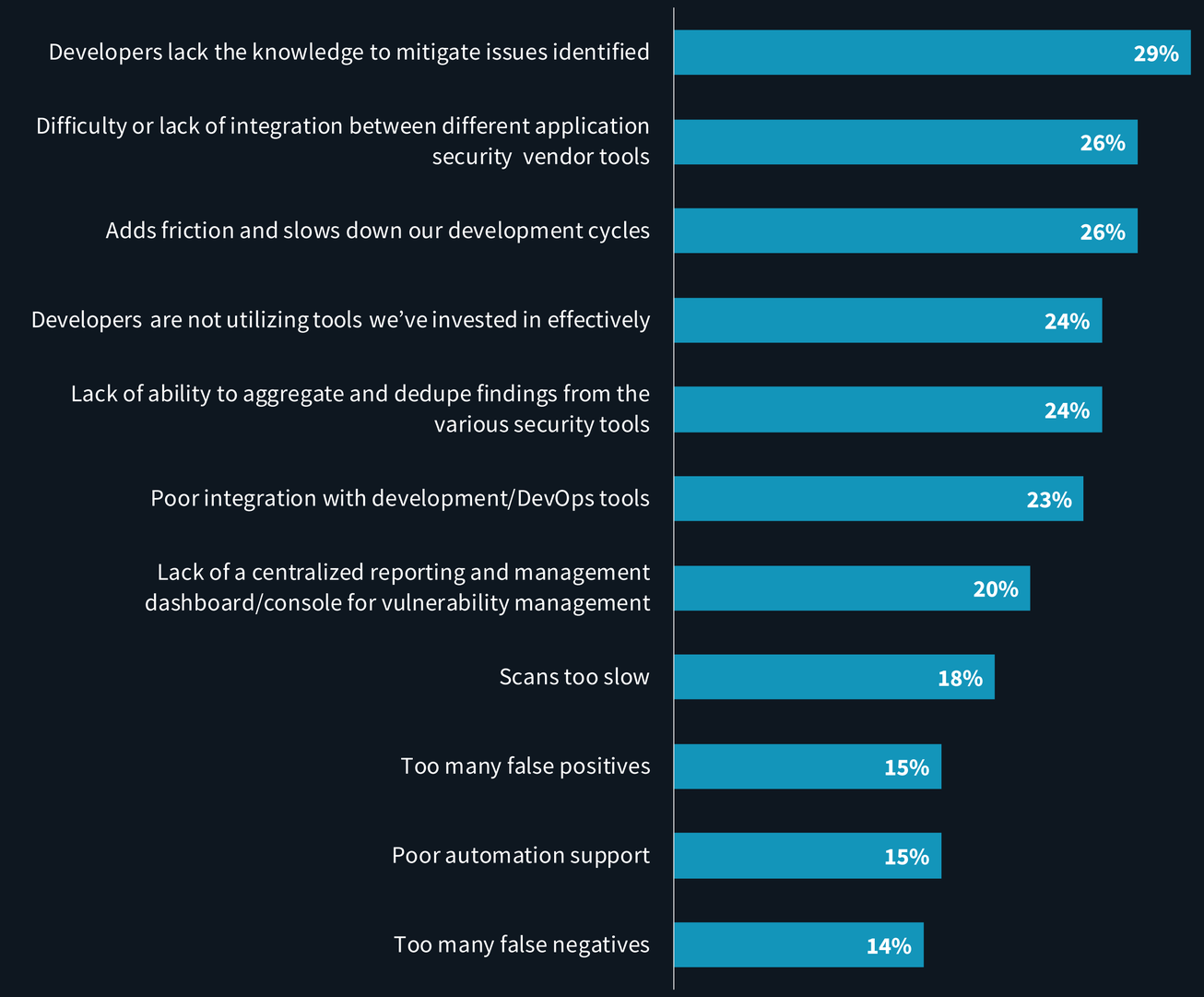
Back to Contents

Challenges with Current Testing Tools

Ultimately, it's up to developers to mitigate identified security issues; however, many report that the most common challenge with their current tools is that their developers lack the knowledge to do so. Security tools vendors provide guidance through just-in-time training or recommended fixes, but the developer ends up with the work. Issue mitigation is often tied to better understanding how and why certain code introduces issues, so developer security training should gradually address this issue.

Others struggle with integrating with other AppSec tools, while many still worry about the friction that AppSec adds, slowing the overall development process.

Top challenges with current testing tools

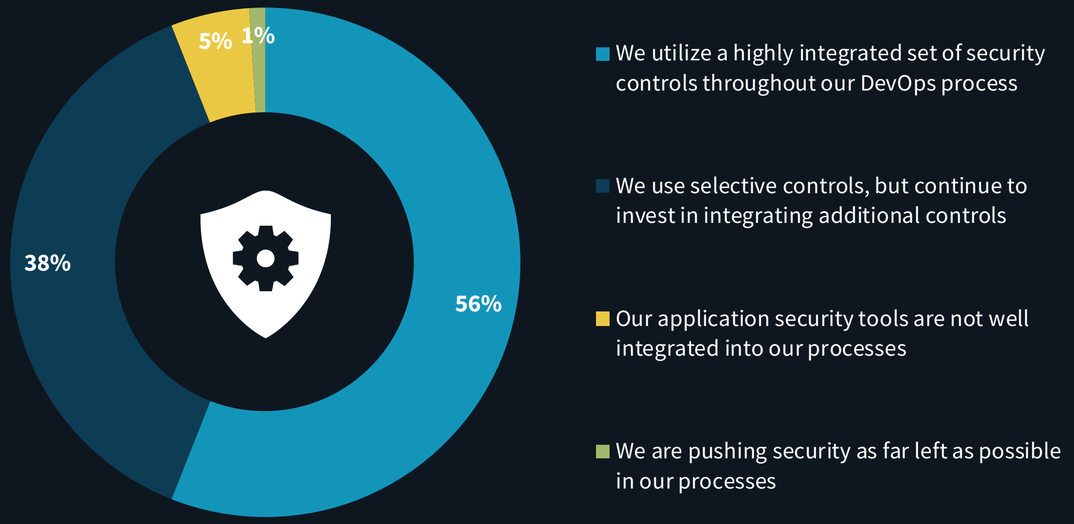


Back to Contents

DevOps Integration Is Important to Improving Application Security Programs

Most believe that automating application security testing throughout the SDLC can make the biggest impact on the success of their program. DevOps integration reduces friction and shifts security further left, helping organizations identify security issues sooner. While developer education and improved tools and processes will no doubt also improve programs, automation is central to modern application development practices.

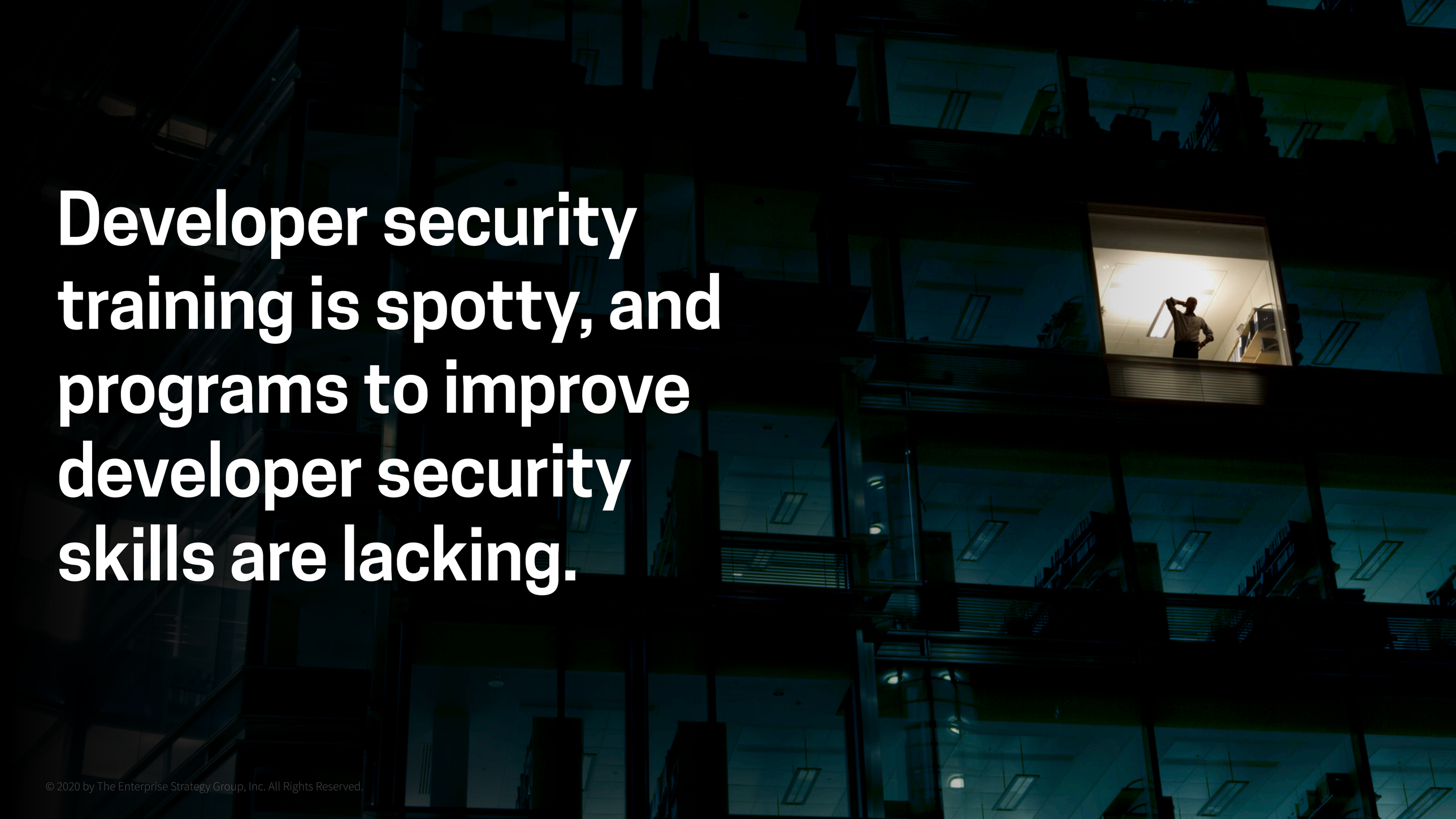
Level of DevOps and AppSec integration



43%

believe DevOps integration is most important to improving AppSec programs.

Back to Contents

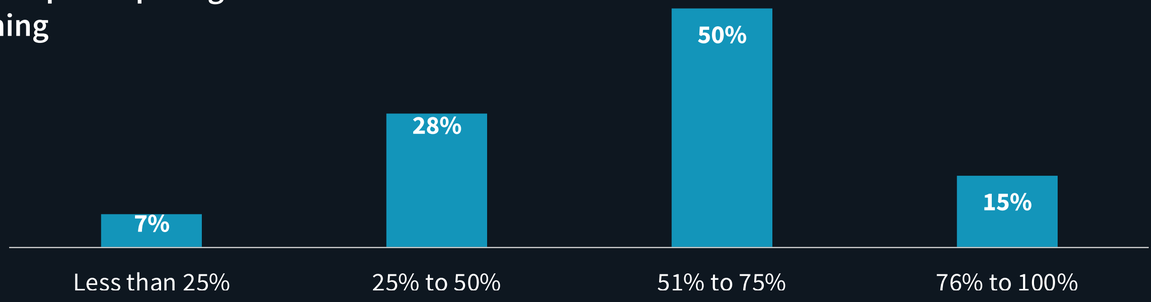


Developer security training is spotty, and programs to improve developer security skills are lacking.

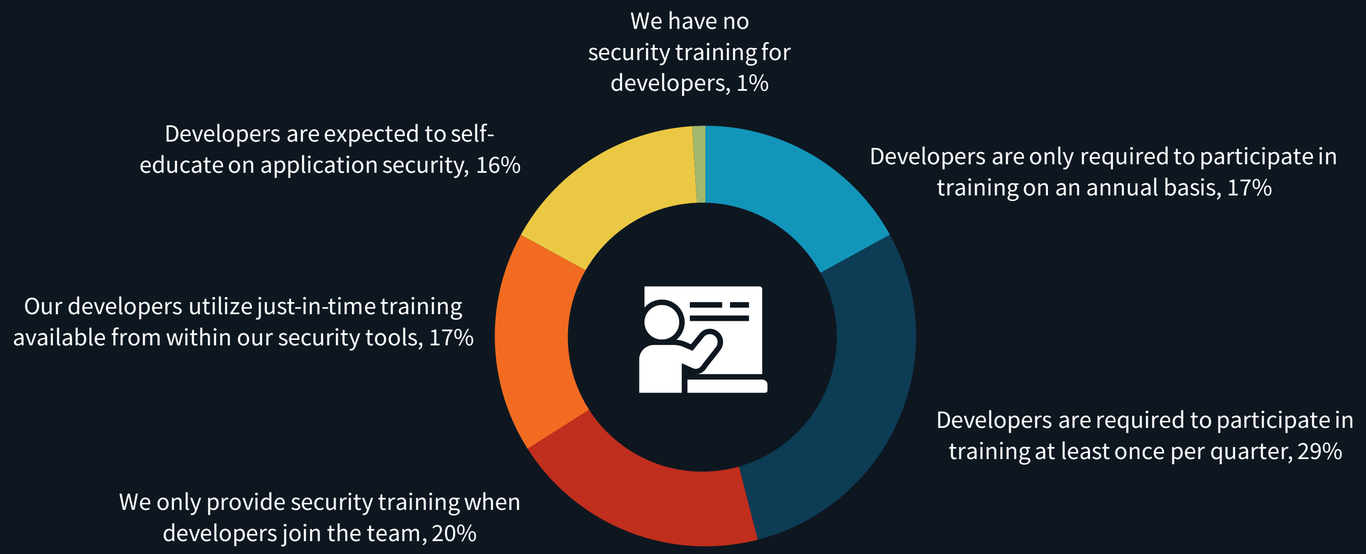
Most Require Developers to Consume AppSec Training

Most organizations require their developers to consume some amount of application security training, but 35% say that less than half of their development teams are participating in formal training. Only 15% report that all their developers are participating. As for frequency, less than half require their developers to engage in formal training more than once per year.

Percentage of developers participating in formal security training



Security training requirements for application developers

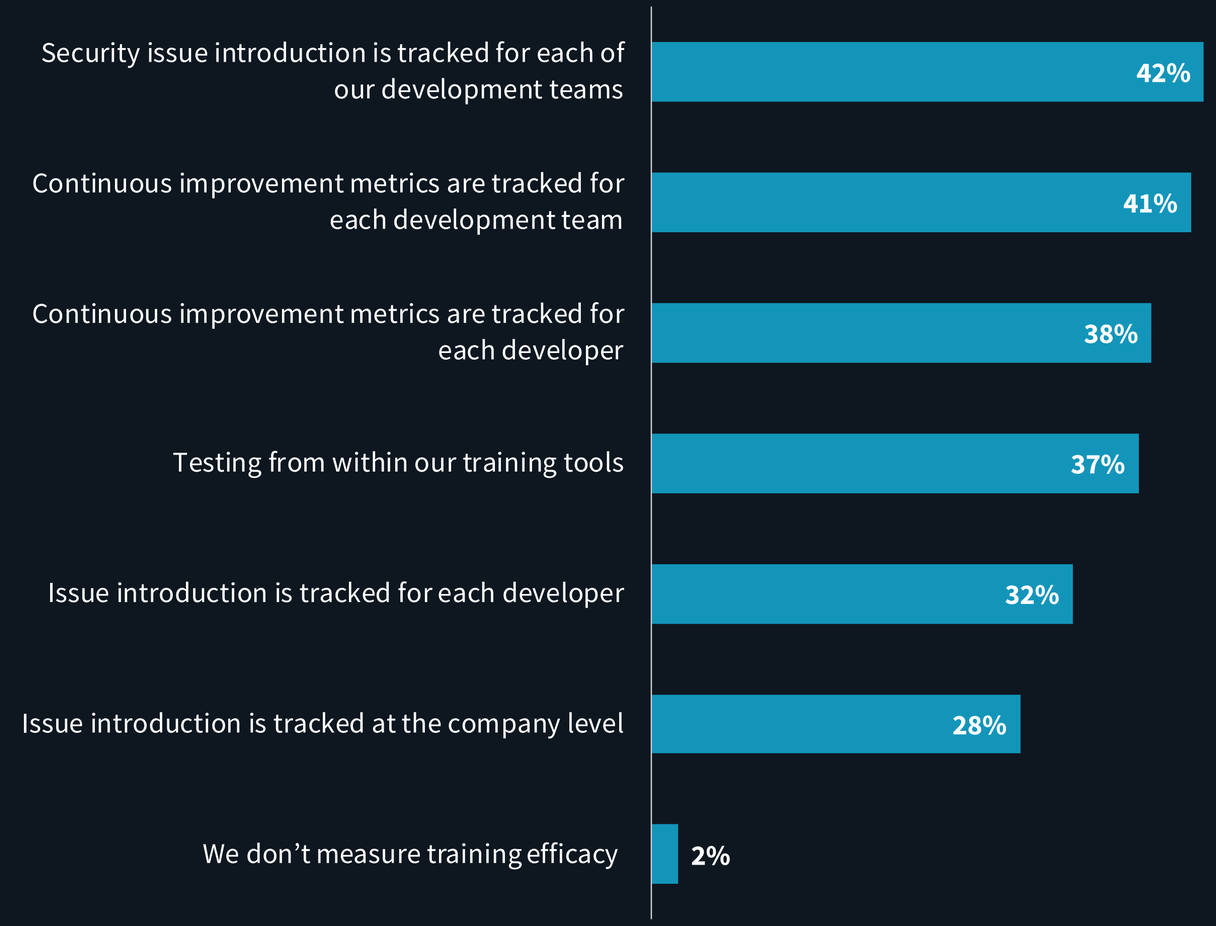


Back to Contents

Most Lack Programs to Measure the Effectiveness of Developer Security Training

Continuous improvement of security programs requires the measurement of issue introduction by development teams and individual developers. Slightly more than 40% report tracking both issue introduction and continuous improvement metrics, enabling targeted efforts to improve those teams and individuals who introduce the most issues.

How security training efficacy for application development teams is measured



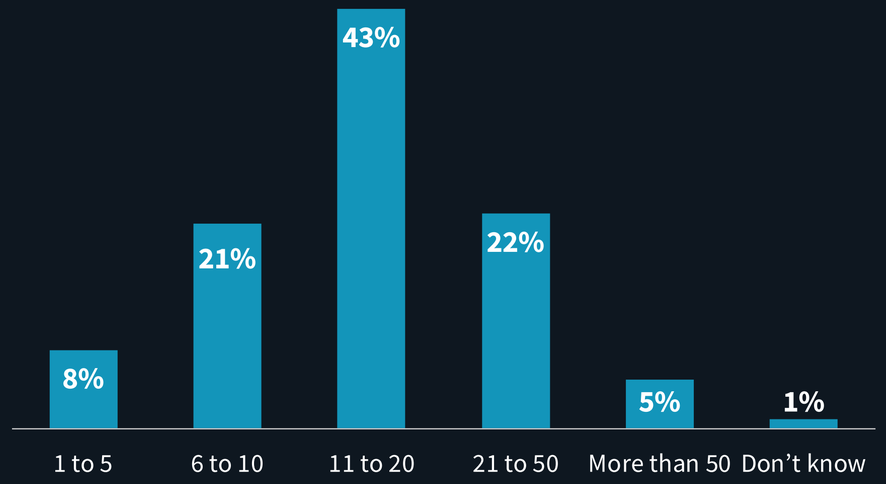
Back to Contents

The proliferation of AppSec testing tools is an issue for many, with more than a third focusing investments on consolidation.

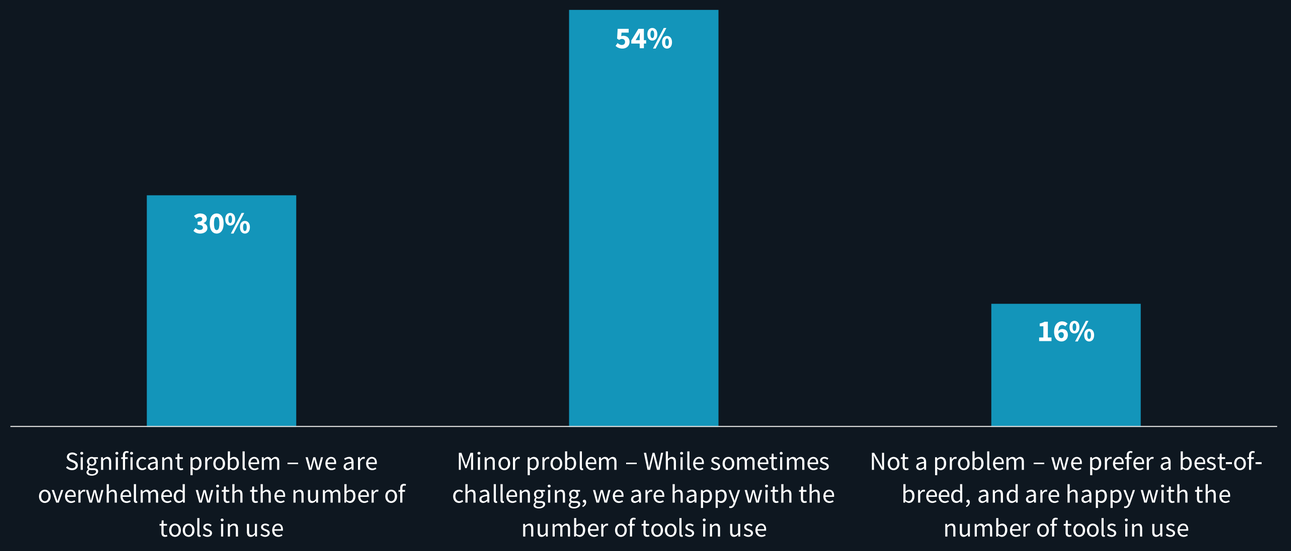
AppSec Tools Proliferation Is Driving Investments to Consolidate

Like other categories of security controls, many organizations are employing so many tools that they are struggling to integrate and manage them. This all too often results in a reduction in the effectiveness of the program and directs an inordinate amount of resources to managing tools. With 72% utilizing more than ten tools, complexity is becoming a key issue.

Individual AppSec tools in use



Tools proliferation is a problem for many

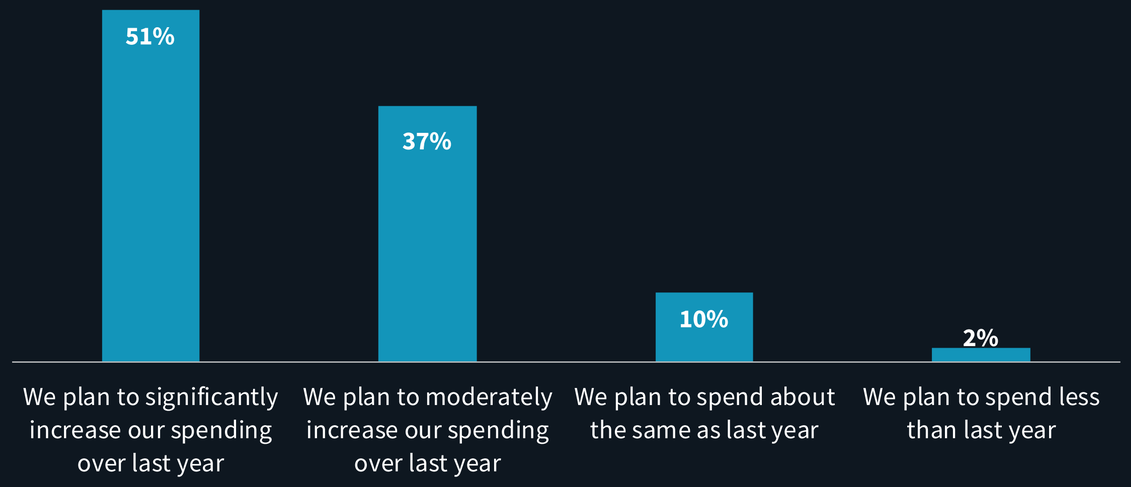


Back to Contents

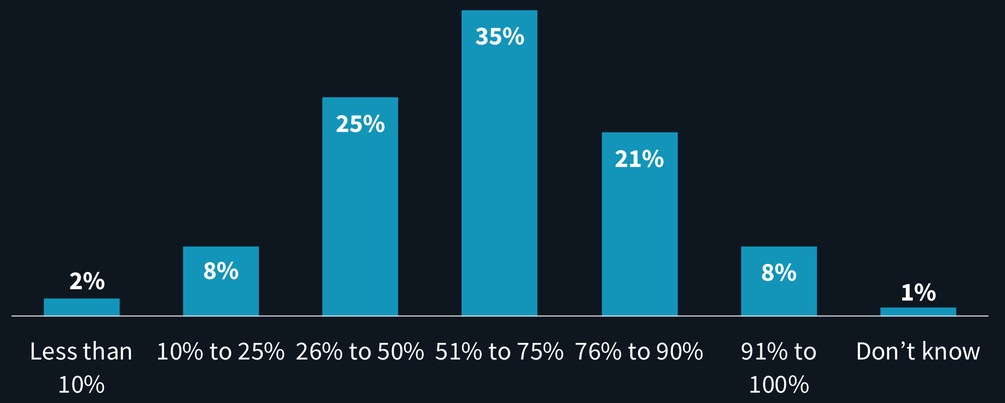
AppSec Spending Will Continue, but Code Coverage Will Still Be Lacking

While most expect to significantly increase application security spending over last year, only 30% will protect more than three-quarters of their codebase 12 months from now.

Expected budget change for AppSec tools over the next 12 months



Percentage of codebase expected to be protected by AppSec tools within 12 months

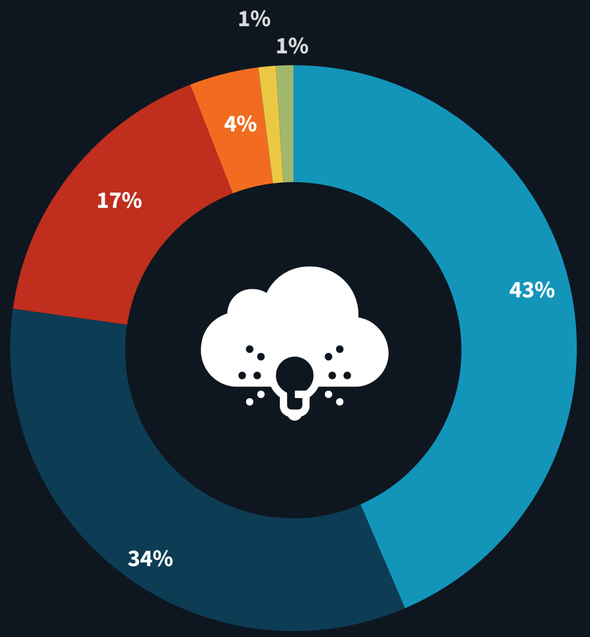


Back to Contents

AppSec Tools Investments Vary, Leaning Toward Securing Cloud Application Development

While 44% plan on targeting application security investments toward cloud, one-third are focused on consolidation of tools to simplify the process. Others plan to invest in expanding the use of testing tools to a higher percentage of their development teams and applications.

Application security investment priorities for next 12 months



- Our investments are weighted toward securing our cloud application development process
- Our investments are focused on consolidation of tools to simplify the overall process
- Our investments are focused on deploying application security across a higher percentage of our development teams and applications
- Our investments are focused on improving the efficacy of our application security program
- None of the above
- Don’t know

Back to Contents

Snyk is a developer-first security company that helps software-driven businesses develop fast and stay secure.

Snyk is the only solution that seamlessly and proactively finds and fixes vulnerabilities and license violations in open source dependencies and container images. Snyk's solution is built on a comprehensive, proprietary vulnerability database, maintained by an expert security research team in Israel and London. With tight integration into existing developer workflows, source control (including GitHub, Bitbucket, GitLab), and CI/CD pipelines, Snyk enables efficient security workflows and reduces mean-time-to-fix. For more information or to get started with Snyk for free today, visit https://snyk.io.

LEARN MORE

About ESG

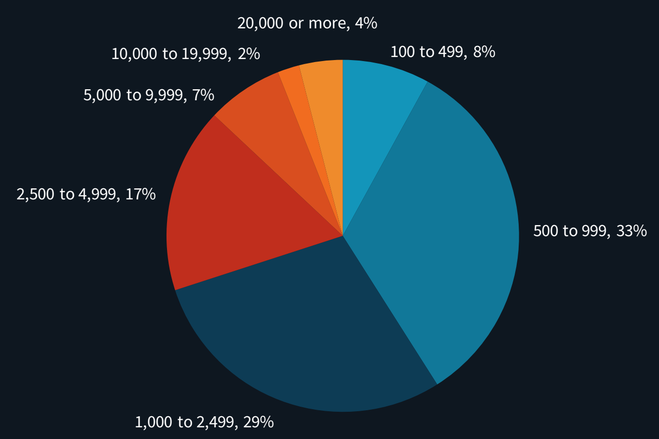
Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

Research Methodology

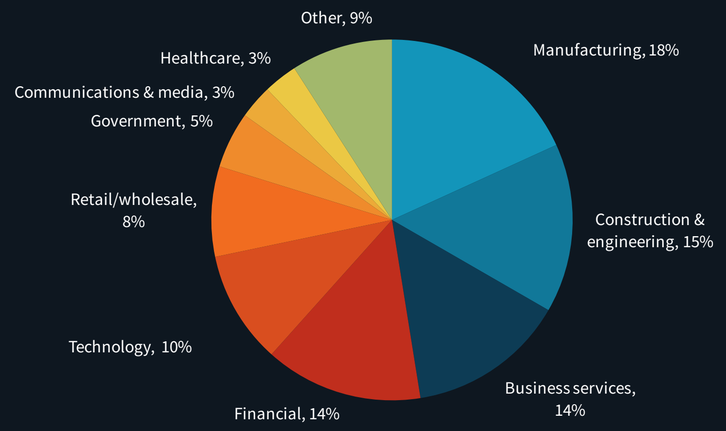
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between June 12, 2020 and June 20, 2020. To qualify for this survey, respondents were required to be IT or cybersecurity professionals with insight and responsibility for securing AppDev technologies and processes or application development professionals involved with securing application development tools and processes. 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 378 IT, cybersecurity, and application development professionals.

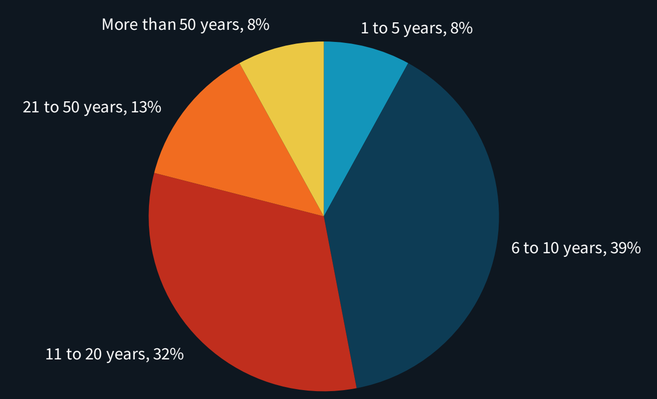
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY INDUSTRY



RESPONDENTS BY AGE OF ORGANIZATION



Back to Contents

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.