DARKReading
RESEARCH

FEBRUARY 2023

```
elif _operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modif
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the activ
    #mirror_ob.select = 0
```

State of Code Security: The AppSec Maturity Marathon

Fortify
by opentext™

Executive Summary

As the software development life cycle becomes ever more complex and threats in the multi-cloud environment proliferate, security teams feel increasing pressure to tackle application security with more sophisticated tools and practices.

Application programming interfaces (APIs) represent a rapidly growing attack surface and an area where teams feel exceptionally vulnerable. Moreover, high-profile supply chain attacks have also become more common as code bases now rely heavily on open-source components.

Data from Dark Reading's recent survey on the state of code security indicates that many organizations are only beginning to shift their security postures in response to this landscape. While they're well aware of software supply chain attacks and feel vulnerable in that regard, most have not yet adopted dedicated tools to test APIs or code dependencies.

That said, organizations are catching up fast. They're making concrete plans to incorporate dynamic tools and software compositional analysis (SCA) for open-source components. Most have already implemented DevSecOps or plan to within the next year, and many are concentrating their code security investments on building out cloud infrastructure to keep up with an increasingly more hybrid environment.

Most organizations are making these expansions by mixing and matching the best tools from a variety of vendors. In making these choices, they prioritize accuracy, depth of vulnerability coverage, and strong integration with the existing developer workflow, so security concerns don't slow down the demanding pace of application development. This expanding set of needs requires a smart partner and multi-pronged approach to keep up.

Key Findings

Data from this study revealed that:

Many organizations are still at the starting line when it comes to implementing DevSecOps.

- 57% of organizations are implementing DevSecOps, and 29% plan to in the next year.
- 62% of organizations find and fix vulnerabilities during development.
- 14% are not implementing DevSecOps at all and have no plans to do so.
- Most are still relying on manual methods to find vulnerabilities:
  - » 64% use manual code review.
  - » 60% use manual application penetration testing.

Among a crowded list of security pain points, cloud challenges rise to the top.

- 31% of organizations cite securing cloud environments as their primary concern.
- 38% of organizations use hybrid methods (a mix of on-premises and cloud-based tools) for their application security deployments.
- 23% of respondents invest most of their code security budget in cloud infrastructure.

Static application security testing (SAST) has caught on. Most are not yet deploying dynamic methods, though they plan to do so.

- 56% use SAST and perform application security assessments.
- Only 45% have implemented dynamic analysis tools.
- Only 37% currently use interactive application security testing (IAST), a dynamic analysis tool. However, an additional 46% are planning to adopt IAST in six months or a year.

Everyone feels vulnerable around APIs, but small businesses aren't doing enough about it.

- API security is ranked as the No. 1 area where all organizations feel most vulnerable.
- But only 39% have a dedicated tool to test API security.
  - » Half of larger organizations but only 31% of smaller organizations tend to have a dedicated tool.
  - » 39% of small businesses treat API security the same as they do web applications.
  - » 18% of small businesses do not perform security testing on APIs at all.

Almost half plan to implement (SCA) in response to open-source component concerns.

- Open-source components are ranked as the second most vulnerable area.
- Maintaining security of the software supply chain is a bigger worry for larger organizations (27%) than smaller ones (18%).
- 26% of respondents are challenged by the frequent use of unsecured open-source code libraries.
- 46% are planning a move to SCA within the next year.

The Road to AppSec Maturity

The application security landscape has transformed at breakneck speed in recent years. The rapid pace of cloud adoption, boosted by the Covid-19 pandemic, now drives the workplace. The shift to cloud has also catalyzed an explosion in threats and breaches in general.

Meanwhile, application programming interfaces (APIs) are becoming the most rapidly expanding attack surface, but they're often misunderstood or left out of the security picture entirely. Moreover, open-source components play a vital part in accelerating time-to-market throughout the process — 98% of code bases now use them. But this development has also led to a software supply chain that is increasingly vulnerable. The Log4j vulnerability disclosed in late 2021 highlighted the challenges of managing and updating third-party software components used in software. The recent security breach at CircleCI was an eye-opening moment for many organizations, as they saw firsthand how their overall security was impacted when an application they relied on was compromised.

In this complex environment, most organizations have a long road to travel before they have the application security maturity necessary to keep up with their needs. Many of them are still at the starting point when it comes to incorporating dynamic analysis tools in their testing cycle or even shifting their testing activities to earlier in the development life cycle. That said, specific concerns and areas that require attention vary by organization size.

Implementing DevSecOps

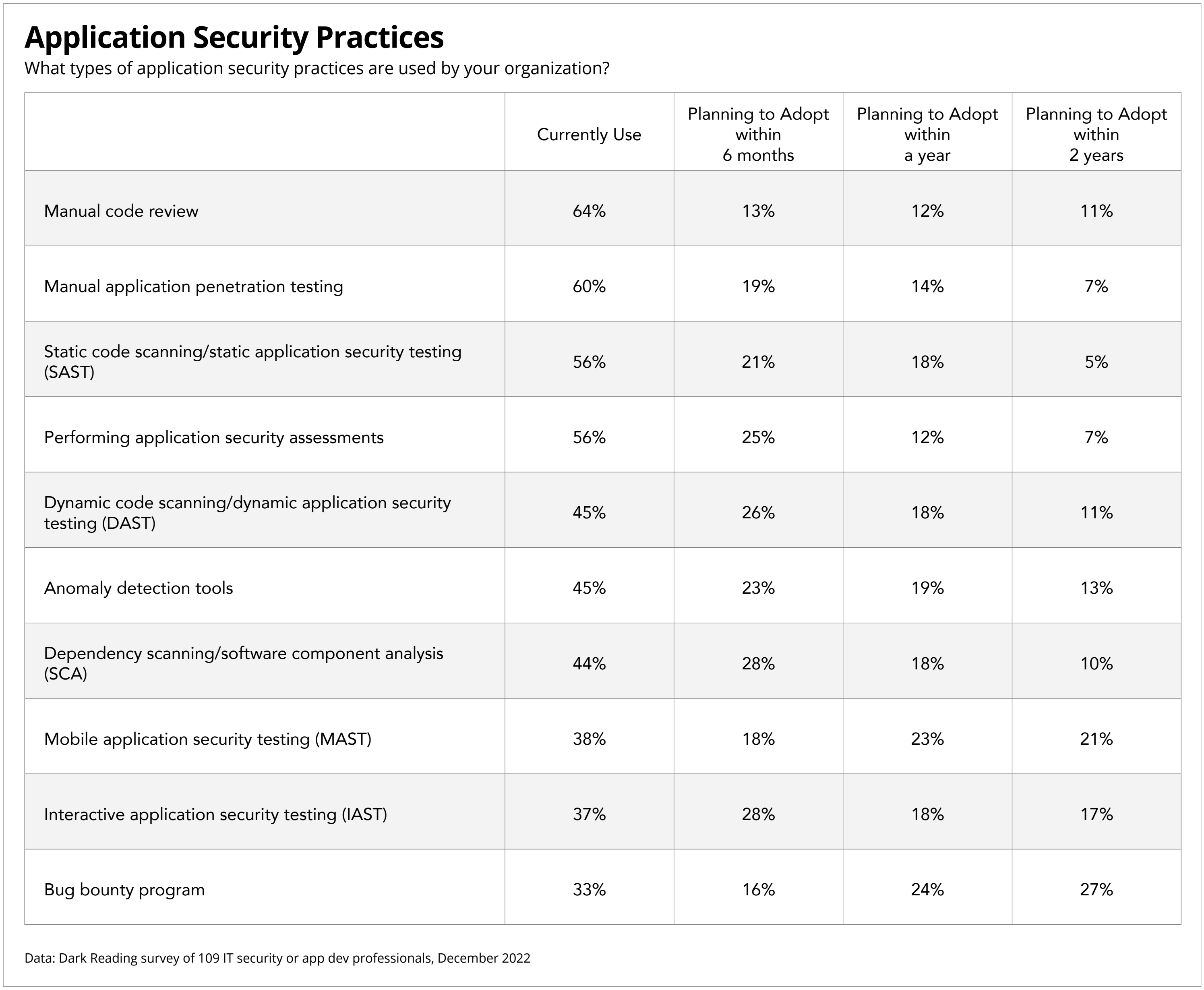
While organizations differ in terms of their maturity, the direction they need to take on this road is clear: They must "shift left" so that security protocols are implemented earlier in the software development life cycle — a critical aspect of the trending practice often referred to as DevSecOps. This practice also brings together developers and security teams to avoid a siloed approach while keeping up the development pace.

According to survey results, while the majority (57%) of organizations are implementing DevSecOps, almost 3 in 10 (29%) haven't yet, but plan to do so in the next year. This sizable proportion of respondents is still at an early stage of the AppSec road. Another fairly large group has even further to travel: A full 14% of respondents are not implementing DevSecOps at all and have no plans to do so. Taken together, 43% of organizations are lagging behind on a practice that has become indispensable.

Many of them may be too reliant on manual processes, which may keep them from bounding ahead in AppSec maturity. Almost two-thirds of survey respondents use manual code review (64%), and 6 in 10 use manual application penetration testing **(Figure 1)**. These organizations likely have a long way to go before they can fully implement DevSecOps.

Organization size provides some insight, but it doesn't change this picture entirely. While the proportion already implementing DevSecOps shoots up to 63% for larger companies (i.e., those employing 5,000 people or more), almost 4 in 10 (38%) of them are still making plans to implement DevSecOps or haven't done so yet. Even the bigger players in software development could do with accelerating their steps along the maturity road, and many are gearing up to make the shift soon. Keep in mind the analysis of data for the two company size segments is based on fewer than 100 respondents.

Figure 1.



Application Security Practices

What types of application security practices are used by your organization?

	Currently Use	Planning to Adopt within 6 months	Planning to Adopt within a year	Planning to Adopt within 2 years
Manual code review	64%	13%	12%	11%
Manual application penetration testing	60%	19%	14%	7%
Static code scanning/static application security testing (SAST)	56%	21%	18%	5%
Performing application security assessments	56%	25%	12%	7%
Dynamic code scanning/dynamic application security testing (DAST)	45%	26%	18%	11%
Anomaly detection tools	45%	23%	19%	13%
Dependency scanning/software component analysis (SCA)	44%	28%	18%	10%
Mobile application security testing (MAST)	38%	18%	23%	21%
Interactive application security testing (IAST)	37%	28%	18%	17%
Bug bounty program	33%	16%	24%	27%

Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

That said, smaller businesses (those with fewer than 5,000 employees) are more likely to rely on manual processes instead of implementing sophisticated methods. Of security practices surveyed, only manual code review is used by most smaller organizations (65%). All the other security practices listed (including dynamic and static analyses) were used by fewer than half of small business respondents.

The Path to Shifting Left

Most organizations are at least making plans to "shift left" and implement security testing earlier in the software development life cycle. Eight in 10 organizations (81%) are either currently performing application security assessments or plan to within the next six months. However, even those who are further along may be lagging when it comes to adopting the increasingly sophisticated tools available at multiple points in the life cycle. And organizations are still catching up to the vulnerabilities inherent in their use of open-source components.

More than half (56%) of all organizations use static application security testing (SAST) and perform application security assessments. That is, most organizations are likely testing source code for a range of known vulnerabilities early in the software development process, before the application is executable. This suggests that most security teams are well on the way to shifting left. This progression is even more pronounced among larger organizations — two-thirds of them (67%) use SAST.

However, organizations of all sizes still lag in terms of implementing dynamic analysis (45%) at different points in the life cycle. Organizations need to reach this important milestone and combine static and dynamic methods to achieve comprehensive AppSec practice.

Moreover, only 45% currently use anomaly detection tools, and less than 4 in 10 use mobile application security testing (MAST) (38%) or interactive application security testing (IAST) (37%). A dynamic testing tool, IAST is usually positioned in the testing or quality assurance stage of the software development life cycle and allows for earlier vulnerability patching. Its low implementation rate suggests that organizations have not yet fully adopted a "shift left" approach, though they may be on that road. This holds true for larger organizations as well — they also lag when it comes to their use of MAST (38%) and IAST (36%).

That said, many organizations committed to a growth path are planning ahead. Almost half of respondents (46%) are planning to adopt IAST in six months or a year. The same proportion is also planning a move to software composition analysis (SCA), which allows teams to analyze and track their dependencies, including open-source components. The plans to implement SCA are especially encouraging, suggesting that companies are taking action to tackle dependency vulnerabilities. It's likely that high-profile attacks, such as Log4j, have prompted teams to make plans and manage their open-source components appropriately.

Key Implementation Challenges

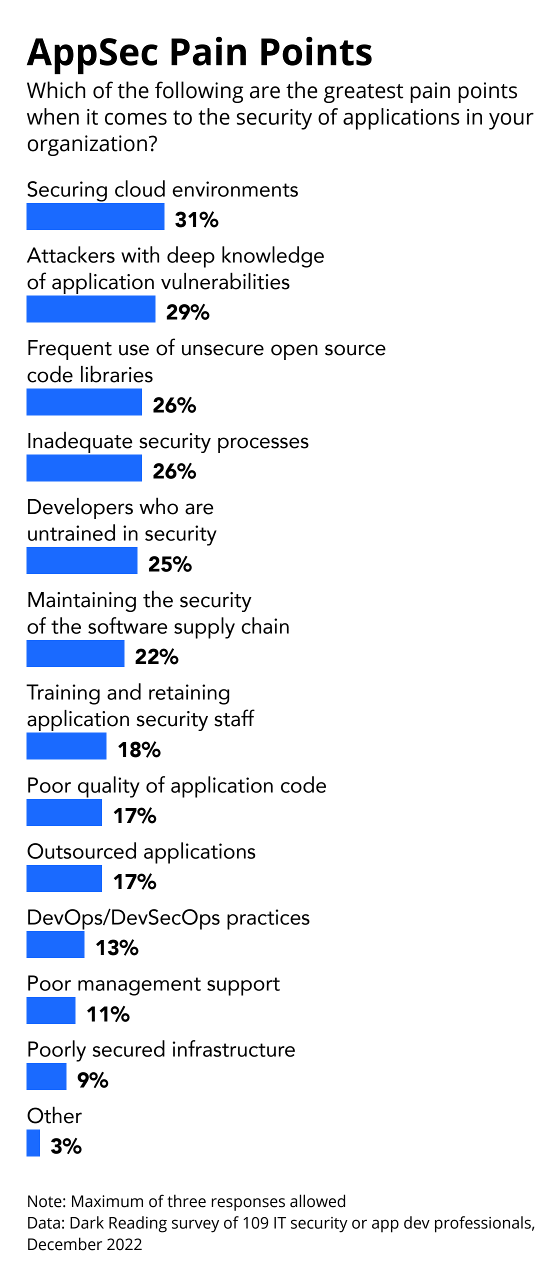
While many organizations are trying to pick up steam along the road to maturity, a wide range of challenges spell headaches for them. This is especially true for larger organizations — no one specific security pain point listed in the survey was cited by more than 29% of those respondents. This highlights the growing complexity of challenges faced and points to the value of a single partner with deep expertise to address all of them.

The Cloud Challenge

While other challenges crowd the room, managing security tools and processes across the hybrid multi-cloud environment is the top challenge to implementing DevSecOps. The cloud is cited by 31% of organizations as their No. 1 concern among a list of pain points, and it's consistent across different organization sizes **(Figure 2)**. Integrating a range of tools is difficult at the best of times, but it's additionally hard for teams to weave those threads together across the hybrid environments that are increasingly becoming the norm for workplaces.

While it's everyone's top headache, the cloud does make matters more difficult for smaller businesses that may have smaller

Figure 2.



AppSec Pain Points

Which of the following are the greatest pain points when it comes to the security of applications in your organization?

Note: Maximum of three responses allowed
Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

teams and fewer resources to integrate their tools. The cloud environment is the primary obstacle for 37% of organizations with fewer than 5,000 employees.

Open-source Risks

The fallout from recent high-profile attacks is borne out by the data: Organizations are very concerned about dependencies. More than a quarter (26%) of respondents are challenged by the frequent use of unsecured open-source code libraries.

Larger organizations are more concerned, perhaps stemming from their greater awareness, but also from the need for organizations with a range of varied applications to incorporate more dependencies into their code. Open-source components rank as the second most vulnerable area overall **(Figure 3)**, but are top ranked for larger organizations. However, open-source security only ranks fourth on the list of vulnerable areas for smaller organizations. This suggests that the risk is not on their radar as much as it should be, considering that 98% of all code bases now use open-source components.

Figure 3.

Organizational Vulnerability

Where do you feel your organization is most vulnerable?

	Overall Rank	Score
Security of our APIs	1	303
The security of our open source components	2	277
Cloud-native applications	3	271
Accuracy and depth of our security tests	4	265
Other	5	69

Note: Rank is based on a weighted score. Answers are weighted and scores are a sum of all weighted counts.
Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

This worry among larger organizations extends to the broader subject of supply chain risks — maintaining the security of the software supply chain is a bigger worry for larger organizations (27%) than smaller ones (18%). Organizations with a broader suite of applications and larger teams are generally more concerned about vulnerabilities that may creep in through widespread component use.

API Security and Orchestration

The No. 1 ranked area where all organizations feel most vulnerable is the security of their APIs. This makes sense, considering that APIs constitute the attack surface experiencing the most growth in the software development life cycle. Some estimate losses of up to $23 billion linked to API-related breaches in 2022. The worry is particularly acute among small businesses — for them, this concern outranks open-source components.

This sense of vulnerability may arise in part, because small businesses are not doing enough to adopt a secure posture when it comes to APIs. That may be due to not knowing enough about API security, or it could be that their security to-do list has other high-priority items to focus on and only a small team to handle them. Half of larger organizations tend to have a dedicated tool to test the security of their APIs — but only 31% of smaller organizations have taken this step. Almost 4 in 10 (39%) of small businesses tend to treat APIs the same as they do web applications when it comes to handling their security. Meanwhile, 18% of them do not perform security testing on APIs at all (versus 3% of larger organizations).

Entrenched Organizational Habits

Longstanding organizational and process issues in the software development life cycle also raise difficult obstacles. Organizational culture is ranked as the second biggest challenge to implementing DevSecOps, regardless of organizational size **(Figure 4)**. To address entrenched habits in their teams, security professionals need to make bigger-picture changes to meaningfully shift their

Figure 4.

Challenges to Implementing DevSecOps

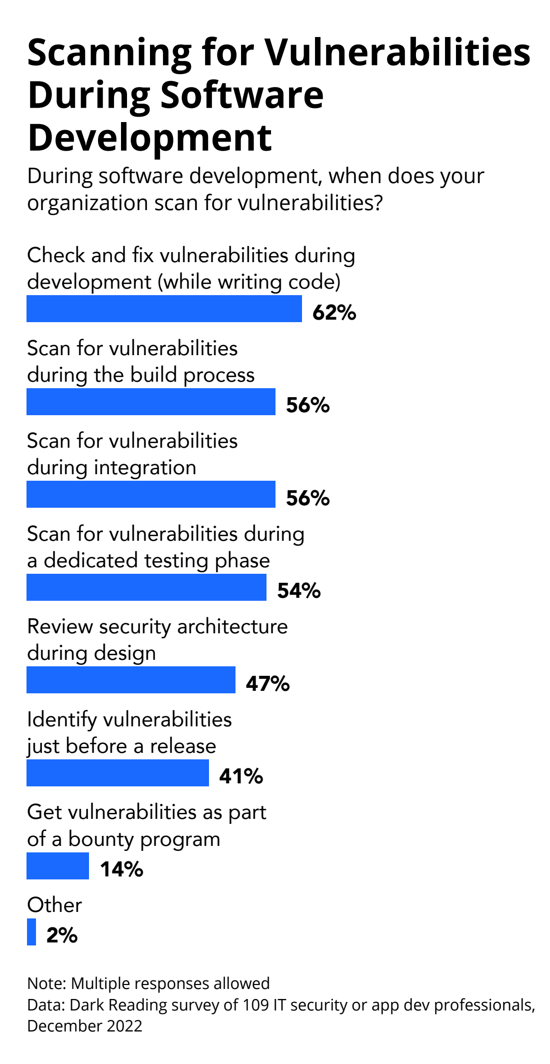
Please rank the challenges your organization faces when trying to implement DevSecOps, from most challenging to least challenging.

	Overall Rank	Score
Managing DevOps tools/processes across hybrid environment (multi-cloud, on-prem)	1	398
Organizational culture	2	333
Inability to scale testing or remediation to match velocity of dev	3	306
Weak integrations (unable to "shift security left")	4	295
Securing outsourced, third-party and open-source code	5	267
Friction added to CI/CD pipeline due to slow scans	6	264
Enabling developers to write secure code	7	253

Note: Rank is based on a weighted score. Answers are weighted and scores are a sum of all weighted counts.
Base: 92 respondents who have already implemented or are planning to implement DevSecOps in the next year
Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

security postures.

Figure 5.



Note: Multiple responses allowed
Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

According to survey results, 45% of organizations use email (among other tools) to share vulnerabilities with developers. And almost half (49%) of large organizations are accustomed to this unsecured practice. Email notification poses a serious security issue, while adding inefficiencies to the process. Developers may miss important messages and having to review lengthy inboxes may slow them down.

For larger organizations, weak integrations (inability to "shift security left") constitute the third-biggest challenge to implementing DevSecOps. For smaller organizations, the inability to scale testing or remediation to match development velocity comes in third.

In terms of the software development life cycle, most (62%) organizations do check and fix vulnerabilities during development **(Figure 5)**. This is a promising sign of their AppSec maturity. In particular, the best-prepared organizations can "shift left" and bring SCA and dynamic code analysis into the developer toolkit. That said, this approach does vary by size — 59% of smaller organizations fix vulnerabilities during development, compared to 68% of larger organizations. Almost half of smaller organizations identify vulnerabilities just before a release (49%) — only 27% of larger organizations delay security assessment in this way.

Factors Influencing Tool Adoption

As organizations attempt to overcome challenges and progress further on the AppSec maturity road, many are adopting sophisticated new tools and prioritizing cloud infrastructure. However, they may still be constrained in fully adopting these tools, due to their size and priorities.

Top Priorities: Accuracy, Depth, Integration

Organizations across the board have similar priorities when it comes to choosing tools and investing in code security. They all prioritize accuracy and depth of vulnerability coverage (ranked number 1) as well as developer and operations tool integration (ranked second) **(Figure 6)**. These considerations come in as the top two, regardless of organization size.

Figure 6.

Selecting Security Tools

Please rank the following from high to low in importance when selecting security tools for your organization.

	Overall Rank	Score
Accuracy and depth of vulnerability coverage	1	482
Developer and ops tool integration	2	430
Language and framework coverage	3	362
Deployment options of the tools	4	355
Reporting and dashboarding	5	330
Ability to test the latest technology	6	250
UX	7	198

Note: Rank is based on a weighted score. Answers are weighted and scores are a sum of all weighted counts.
Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

Consistent with current trends, organizations prize tools that integrate into existing developer workflow and deployment platforms, rather than standalone options that could be overlooked or slow the process down. It follows that code security — embedding security into the code process — is an important consideration as well. In this regard, a third (33%) of organizations are investing the most in security solutions and almost a quarter (24%) in developer tools and cloud infrastructure.

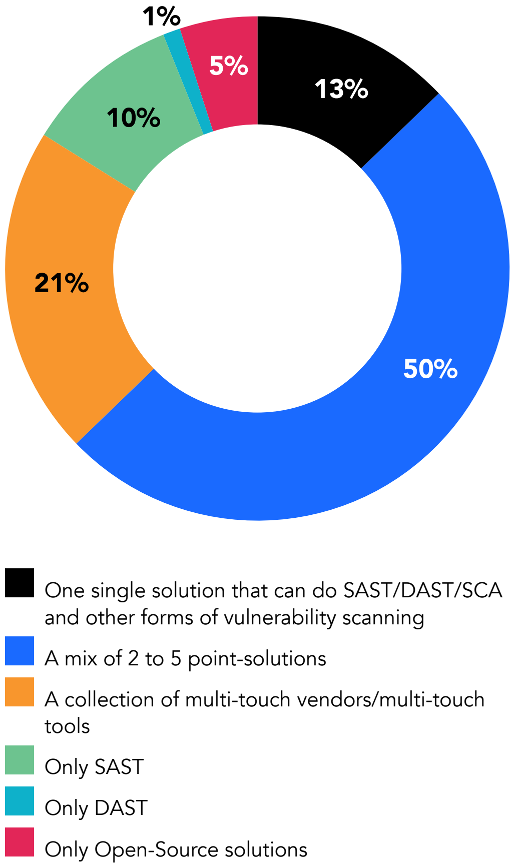
The Mix-and-Match Approach

In general, most organizations mix and match vendors and tools to manage their application security needs. Seven in 10 (71%) respondents say they use 2 to 5 point solutions or a collection of multi-touch vendors or tools **(Figure 7)**. This shoots up to 81% of larger organizations. Only 13% of organizations use a single solution to take care of all their needs.

Figure 7.

Number of AppSec Tools

How many application security tools or platforms do you use to manage your application security program?



Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

The proliferation of this approach is understandable, considering the complex environment. Organizations would rather mix best-of-breed options than rely on a one-size-fits-all solution that might not afford the coverage depth that is a top priority for them. However, the mix-and-match strategy does result in more tools to manage for overstretched staff.

The Shift to Hybrid Cloud Deployment

Over a third (38%) of organizations use hybrid methods (a mix of on-premises and cloud-based) to deploy AppSec. It's encouraging that more than a third of organizations have adapted to the rapidly changing workplace and implemented hybrid methods that are more likely to capture the range of vulnerabilities in this landscape. That said, most organizations are still primarily deploying AppSec either on-premises (34%) or in the cloud (26%) without committing thoroughly to the hybrid environment.

This does vary a great deal by organization size. Almost half of larger organizations (49%) use hybrid methods, whereas less than a third (29%) of smaller organizations do so. Instead, smaller organizations are more likely to rely on cloud-based methods alone (35%), whereas only 15% of larger organizations do so.

However, there's evidence that more organizations are shifting their attention toward the cloud when it comes to code security. Almost a quarter (23%) of respondents invest most of their code security budget in cloud infrastructure. It's the top category for large organizations — almost 3 in 10 (29%) of them invest most of their budget there. This promises an even greater shift towards hybrid models in the software development life cycle in the near future.

Reflecting on Outcomes, Tracking Success

For organizations seeking to progress in their AppSec maturity, it's critical to track their past security successes and mistakes and reflect on results. While survey respondents looking back at their AppSec experiences are concerned about finding real vulnerabilities that they don't have time to fix, more of them are worried about the impact of false negatives and positives. This attitude is more pervasive among smaller organizations than larger ones.

False Positives and Negatives

Six in 10 respondents say that they find too many false positives and almost as many say they worry about finding false negatives **(Figure 8)**. Both of these concerns make sense, considering the increasing time pressure on security teams. With limited resources at hand, they're concerned about wasting that precious time on unnecessary issues. And chasing after false positives also affects the team's remediation time for actual vulnerabilities.

For larger organizations, however, finding false negatives (60%) is less of a worry than finding more issues than they can remediate (70%). They have greater resources at their disposal and are also dealing with higher stakes when breaches do occur. It follows that fewer (49%) smaller organizations worry about finding more issues than they can remediate. With smaller teams and more responsibilities per team member, false positives and negatives are the immediate headache.

Figure 8.

Security Tool Results

While thinking about the security tools in use by your organization and the type of security results you get, to what degree do you agree or disagree with each of these?

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
We find more issues than we can remediate	21%	37%	21%	16%	5%
Our tools are very accurate	21%	26%	35%	18%	0%
We find too many false positives	18%	44%	23%	13%	2%
Our security tools just scratch the surface of all that we need to do	17%	30%	26%	24%	3%
We worry about finding false negatives	14%	46%	22%	16%	2%

Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

Tracking Success

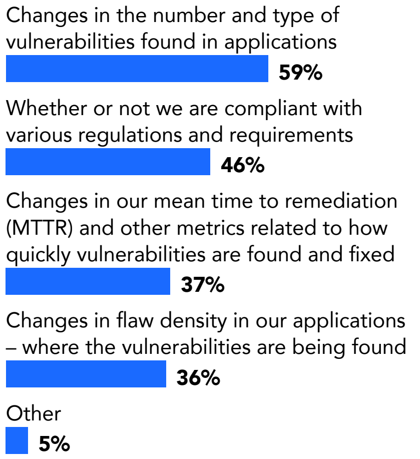
Most organizations track or manage the success of their application security program by looking at changes in the number and type of vulnerabilities found (59%) **(Figure 9)**. Additionally, almost half (46%) track whether or not they are compliant with various regulations and requirements.

Speed metrics such as mean time to remediation (MTTR) are more important to larger organizations (42%) as compared to smaller ones (32%). This worry corresponds to larger organizations' concern about finding more vulnerabilities than they can remediate quickly enough to keep up the development team's pace.

Figure 9.

Tracking AppSec Program Success

How does your organization manage or track the overall success of the application security program?



Note: Multiple responses allowed
Data: Dark Reading survey of 109 IT security or app dev professionals, December 2022

Takeaways From This Report

While many organizations are fast catching up to a changing code security landscape by implementing DevSecOps and mixing the best tools from a variety of security vendors, others still lag on the road to AppSec maturity.

Larger organizations, in particular, have made strides to shift their security postures to encompass a wider range of the development life cycle and begin scanning for vulnerabilities earlier in the process.

But increasingly, this "shift left" approach isn't enough to keep up. The right partner can help organizations "shift everywhere" by incorporating dynamic analysis tools in combination with static tools to arrive at a more comprehensive approach to application security.

This approach must also include testing and discovery for APIs — the most rapidly growing sector of the attack surface. And considering recent high-profile attacks, "shift everywhere" must also address the supply chain's reliance on dependencies by including software composition analysis (SCA).

Robust application security isn't a sprint — it's a distance race with many potential obstacles along the way. The right partner can help organizations navigate the growing number of complex obstacles to arrive at a security posture that works for the long haul.

About OpenText and Fortify

Fortify enables you to build software resilience from an industry-leading AppSec partner you can trust. Fortify static, dynamic, interactive, and open source security testing technologies are available on premises, SaaS, or as a managed service — offering organizations the flexibility they need to build an end-to-end software security assurance program.

Learn more at www.fortify.com

Survey Methodology

Dark Reading conducted a survey on behalf of OpenText in November and December 2022 to understand the state of application security in North American organizations. The final dataset consisted of 109 cybersecurity and application development professionals at organizations with a dedicated application security team. The totals for the breakdown of data by company size referenced in this report are 62 respondents at companies with fewer than 5,000 employees, and 47 respondents at companies with 5,000 or more employees.

Respondents hold job titles such as cybersecurity managers/directors, application development managers or group leaders, IT executives, and application security team members. Companies of all sizes are represented, with 23% of respondents at companies with fewer than 500 employees, 34% at companies with 500 to 4,999 employees, and 43% at companies with 5,000 or more employees. Respondents work in more than 17 industries, such as banking, financial services, technology manufacturing, non-computer manufacturing, consulting, education, and government, to name a few.

The survey was conducted online. Respondents were recruited via email invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database; Informa Tech is the parent company of Dark Reading. Informa Tech was responsible for all survey design, survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.