CONTRAST SECURITY

PRIORITIES AND CHALLENGES FOR MODERN SOFTWARE DEVELOPERS

Survey Findings from Today’s Top-performing Technology Companies

TABLE OF CONTENTS

01 | EXECUTIVE SUMMARY

This report is based on a survey of development teams at some of the world's most technologically advanced companies. It explores development practices and the state of application security at these top-tier organizations. Even though these development teams have achieved substantial acceleration gains in digital innovation, they still face intense pressure to speed up release cycles and commit code more quickly. In response to this increasing pressure over time, modern software developers have become much more efficient by deploying methodologies like DevOps and using open-source code more frequently.

Modern developers at these global, fast-moving technology juggernauts have certain distinct attributes that differentiate themselves from many developers in other industry sectors—from the tools they use to their organizational cultures. Survey findings reveal that significant application security challenges exist, even for modern software development teams at the top of their profession:

- 85% admit their average application has an average of 10 or more vulnerabilities—and nearly half say they have over 20 per application
- Almost 75% of development teams cannot find highly specialized application security experts
- Nearly 80% spend too much time triaging and diagnosing application security alerts
- 88% must stop their work to remediate vulnerabilities at least once a week
- Nearly 50% of application tools are not integrated into the continuous integration/continuous deployment (CI/CD) pipeline

The data is not all pessimistic. Over one-third (36%) of developers say that at least one application security metric is among their top four performance measurements. A healthy majority of organizations (63%) have deployed an interactive application security testing (IAST) solution, the first step in a move away from older technology that slows development processes while providing inadequate security. And very importantly, 77% of developers want more training in—and responsibilities with—application security, highlighting their understanding of its importance.

Organizations should leverage this progress to move beyond legacy application tools and processes to an architecture. They should move toward a solution that provides continuous security and real-time feedback throughout the software development life cycle (SDLC)—virtually eliminating security-related coding delays while providing more complete protection against vulnerabilities and attacks. As companies make progress in this area, application security outcomes should improve.

KEY FINDINGS

WHAT IS WORKING

85% deploy to production multiple times per week

66% have adopted open-source libraries and frameworks for at least three-quarters of their applications

36%+ cite operational acceptance, median time to remediate (MTTR), or security vulnerabilities found among their top 4 areas for performance evaluation

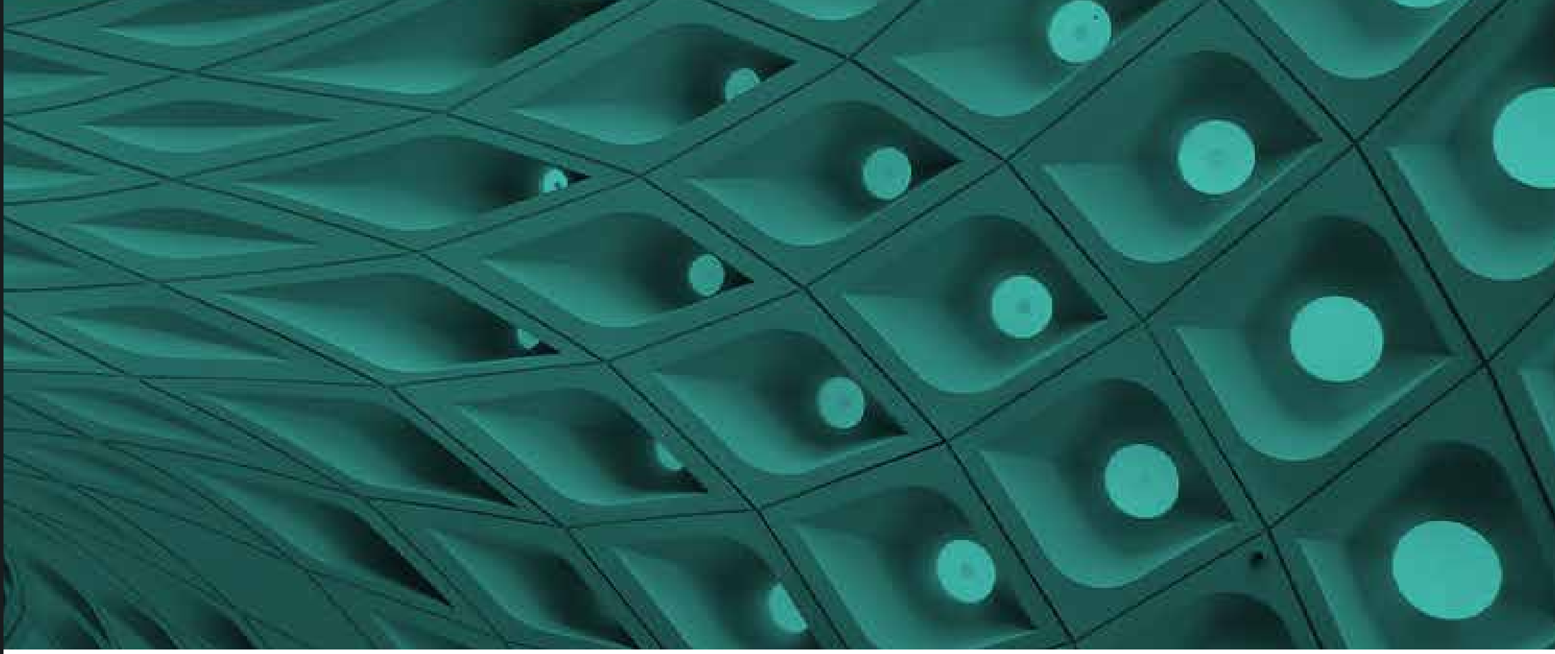
WHAT IS NOT WORKING

79% are under pressure to shorten release cycles and commit more code

88% must fix vulnerabilities at least weekly

85% indicate applications have an average of 10+ vulnerabilities

50% of most application security tools are not integrated into the CI/CD pipeline



02 | INTRODUCTION

The technology sector enjoys a reputation for innovation, profitability, and economic benefit for the communities in which it is located. Following a pattern set by the storied Silicon Valley in California, clusters of technology companies have sprung up in metropolitan areas across the U.S. and around the world, transforming regional economies and bringing an aura of success.

Technology companies are often perceived as unique, cutting-edge, and important for society. As a result, they can often recruit the “best and brightest” in a variety of technical roles, including software developers. As one application security architect in the survey remarked, working at a technology company “makes my resume more impressive.”

Recruiting top-tier technologists is business critical for companies in the industry, as the technology sector is a highly competitive space. Because they failed to adapt to rapid market changes, a list of technology behemoths from the 1990s and 2000s disappeared from the landscape or are a shadow of their former selves in the current marketplace. Newer, more innovative companies have emerged to replace them, while some older firms have been able to reinvent themselves and come back stronger than ever. Navigating these turbulent times requires a company’s software developers to be at the top of their game, putting out high-quality code at unparalleled speed.

“HIGH-TECH COMPANIES ALWAYS SET THE STANDARDS.”

– SURVEY RESPONDENT, SOFTWARE ARCHITECT

METHODOLOGY FOR THIS STUDY

This study is based on a survey conducted in August 2020 that sought to gauge the state of application security at larger technology companies. Respondents were part of the development teams at organizations with anywhere from a couple thousand employees to more than 100,000. These professionals are busy: Nearly one-third (32%) of teams represented in the survey develop and manage more than 800 applications, and 63% are responsible for more than 250 (Figure 1).

The analysis of the survey results includes overall responses as well as cross-analysis of responses by factors such as the size of each development team, the number of applications managed, and the job title of each respondent. From this analysis, we identified several insights about the state of application security for top-tier development teams, and where those efforts need to head in the future.

Q HOW MANY NON-SAAS-BASED APPLICATIONS (VIZ., THOSE DEVELOPED IN-HOUSE OR BY A THIRD PARTY) ARE DEVELOPED AND MANAGED BY YOUR ORGANIZATION'S DEVOPS TEAM?

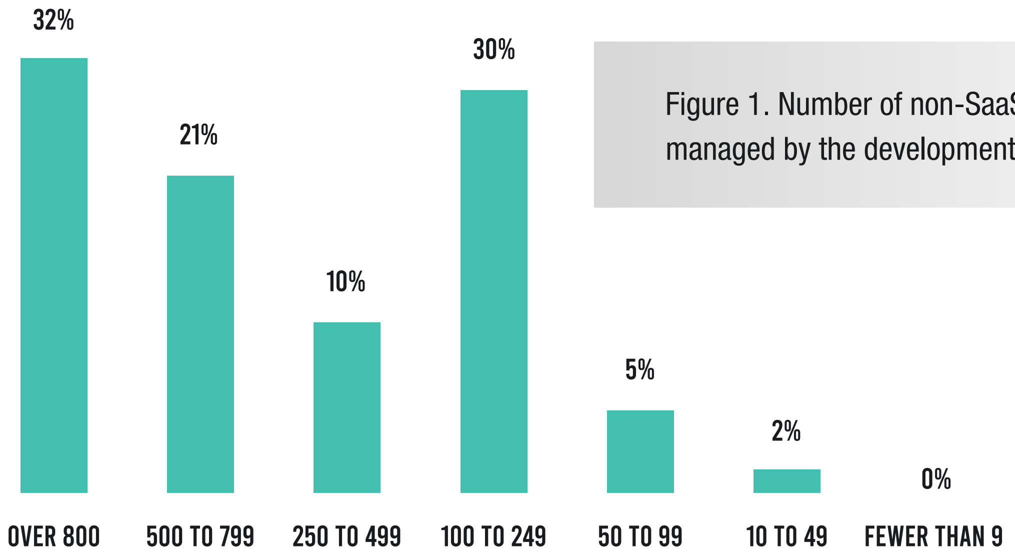
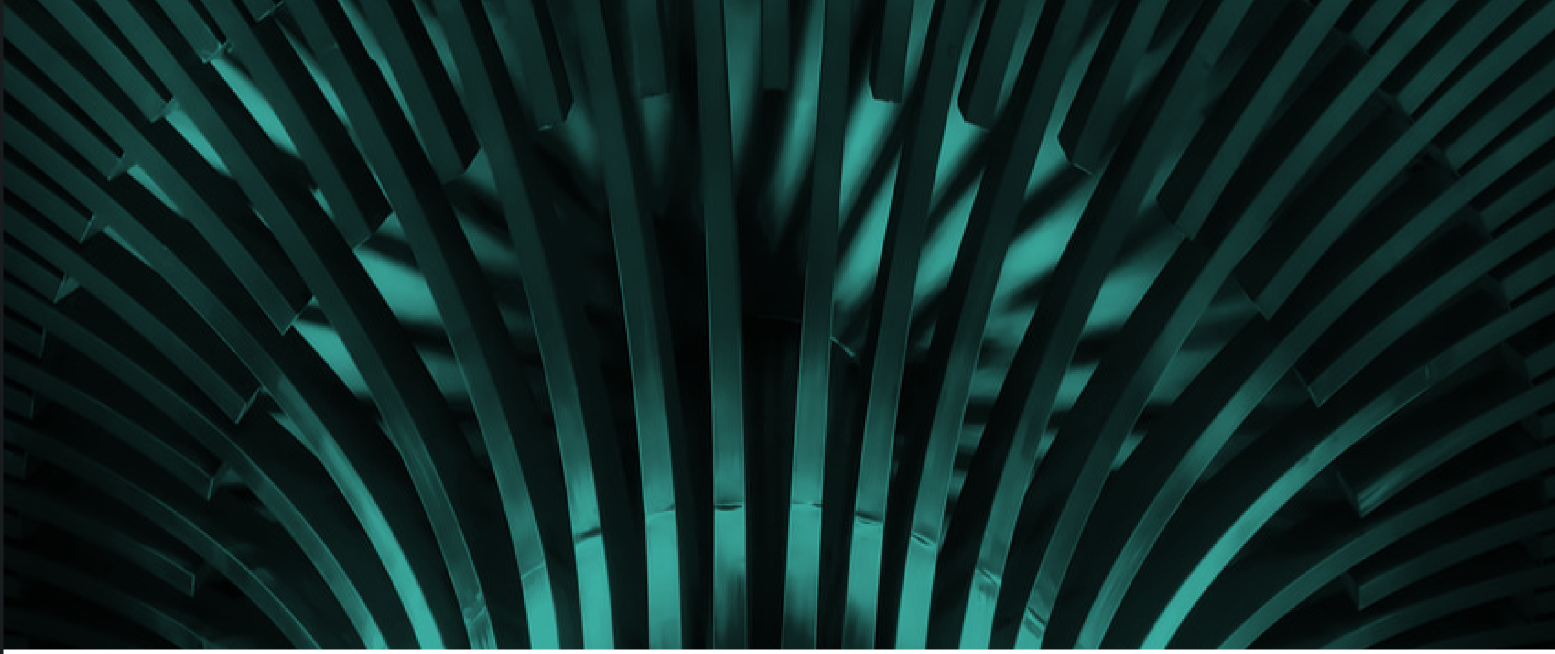


Figure 1. Number of non-SaaS-based applications managed by the development team.

> "SUCCESSFUL HIGH-TECH COMPANIES ARE ADEPT AT RECOGNIZING THE POSSIBILITIES ASSOCIATED WITH TECHNOLOGICAL ADVANCEMENTS AND NURTURING CORPORATE CULTURES THAT ENABLE THEM TO SEIZE ON THOSE OPPORTUNITIES."
>
> – SURVEY RESPONDENT, QA ENGINEER



03 | APPLICATION SECURITY INSIGHTS FROM TOP-TIER DEVELOPERS

AN ANALYSIS OF THE SURVEY RESULTS YIELDED SEVERAL USEFUL INSIGHTS ABOUT THE STATE OF APPLICATION SECURITY AT LARGE COMPANIES:

INSIGHT: MODERN DEVELOPERS SEE THEIR ROLE AS UNIQUE, AND MTTR IS AN IMPORTANT MEASUREMENT

Developers in technology companies have mixed opinions about whether their role is significantly different than it would be in a different industry. An analysis of a freeform question in the survey finds that just 15% of respondents believe there is no difference in objectives between development teams at technology companies and in other industries, and very few respondents noted glaring differences. One noteworthy perspective, voiced by 9% of respondents, is the belief that technology companies' development teams see their objectives change more rapidly than in other industries.

Despite this ambivalence about the industry as a whole, many respondents see differentiation in their own programs. In another freeform question, 28% said that the tools their teams use make their environment unique, while 18% cited the extraordinary nature of the team members themselves (Figure 2).

Q WHAT MAKES YOUR DEVELOPMENT ENVIRONMENT UNIQUE? AND WHAT CHALLENGES DOES THIS PRESENT?

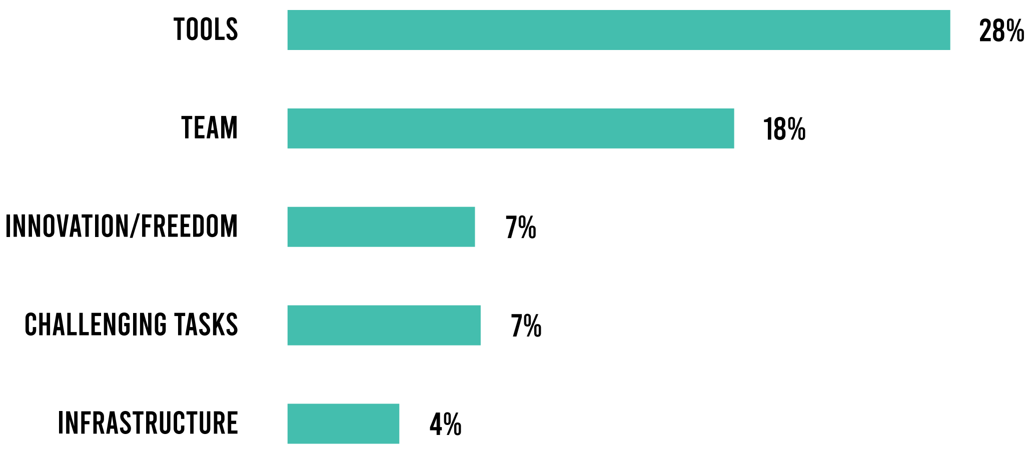


Figure 2. Unique characteristics of respondents' development environment.

HOW TEAMS ARE EVALUATED

When it comes to how these professionals are evaluated, the survey asked respondents to rank the top four criteria included in their performance review. Mean time to remediate (MTTR) vulnerabilities was among the most commonly cited metrics, with 20% of respondents placing it in the top two and 36% placing it in the top four (Figure 3). Only operational acceptance was cited by more respondents in the top four, at 38%, though fewer respondents put this in the top two. Another application security metric, the number of security vulnerabilities found, is the third most-cited factor both for the top two and the top four.

One optimistic note: MTTR is a top-four metric not only for those tasked with application security (83% of application security architects). Even for those with development-related job titles, security crops up regularly—60% of cloud architects, 50% of integration specialists, and 42% of web developers.

Q PLEASE RANK THE TOP FOUR OF THE FOLLOWING IN TERMS OF THEIR LEVEL OF IMPORTANCE CONCERNING HOW YOU ARE EVALUATED.

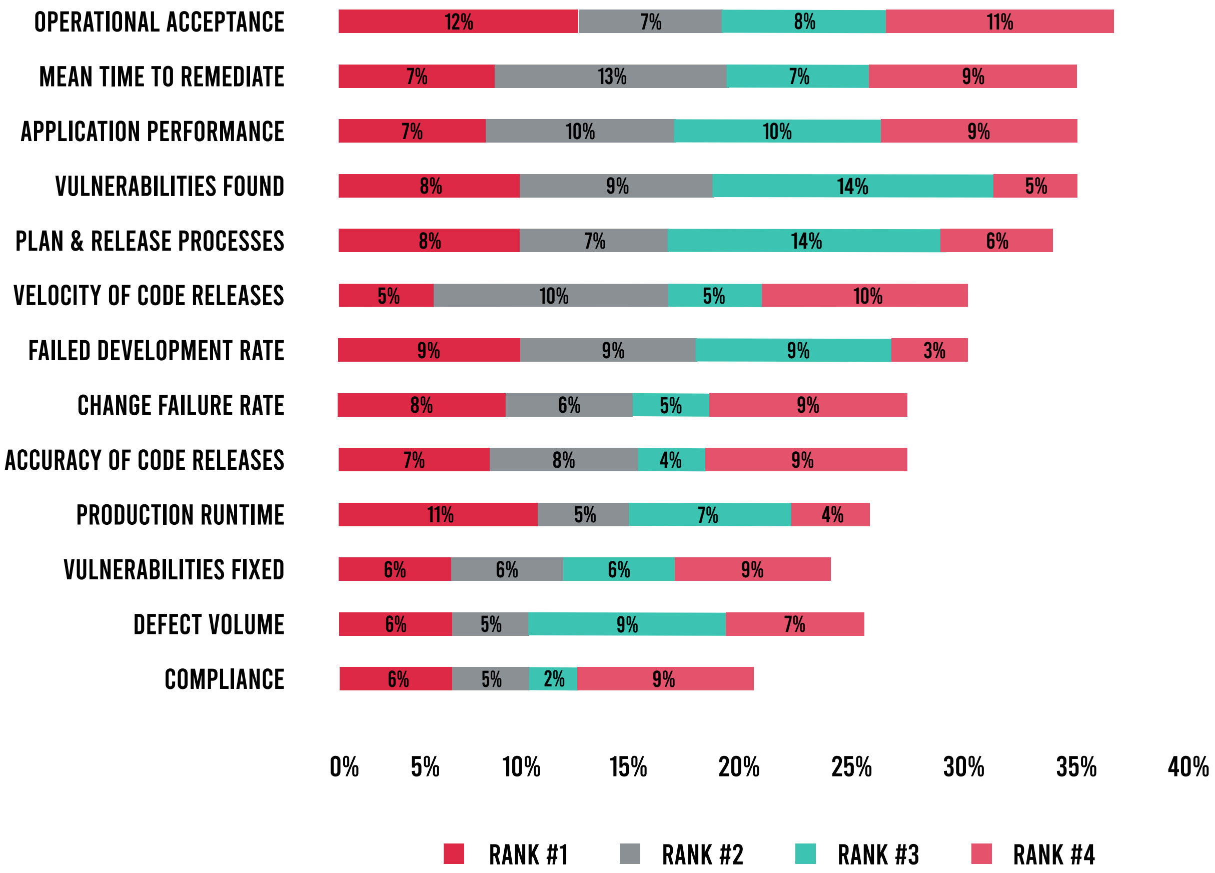


Figure 3. Percent of respondents who ranked performance criteria in the top 4 most important for their evaluations.

> “SOFTWARE ENGINEERING IS A [UNIQUE] CULTURE.”
>
> – SURVEY RESPONDENT, CLOUD ARCHITECT

INSIGHT: MODERN DEVELOPERS ARE UNDER INTENSE PRESSURE TO SHORTEN RELEASE CYCLES

The pressure for more speed in the development process is not unique to technology companies. According to one study, 68% of organizations have a mandate from the CEO that nothing should be allowed to slow down the development process—including security concerns.[1]

If anything, this pressure to develop software more quickly is more intense in technology companies. Nearly 8 in 10 (79%) of respondents agree or strongly agree that they are under pressure to shorten release cycles and commit more code (Figure 4). The figure is even higher for those holding several specific job titles, including build engineer (88%), QA engineer (80%), and application security architect (83%). The latter role may be something of a surprise, though they are likely to bear the brunt of complaints when it comes to security-related delays.

Q ARE YOU UNDER INCREASED PRESSURE TO SHORTEN RELEASE CYCLES AND COMMIT MORE CODE?

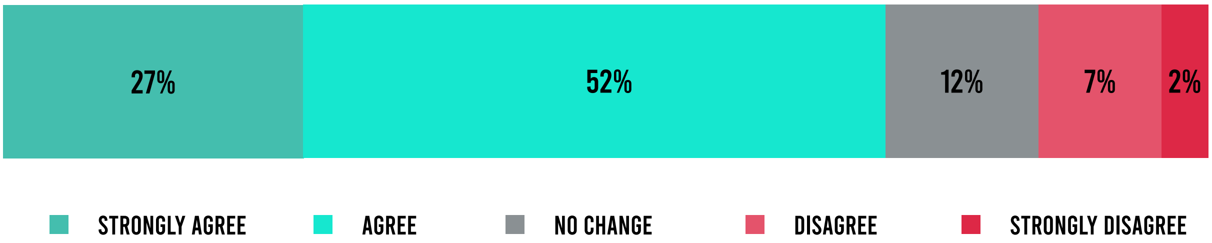


Figure 4. Percent of respondents under increased pressure to shorten release cycles and commit more code.

IMPROVING PROJECT EFFICIENCY

In response to this pressure—and the business needs that precipitate it—technology sector development teams are cranking out code at unprecedented speed. Fully 85% of respondents report that they deploy code to production at least multiple days per week, with a solid majority (62%) doing so at least daily (Figure 5).

Q ON AVERAGE, HOW OFTEN DO YOU DEPLOY TO PRODUCTION?

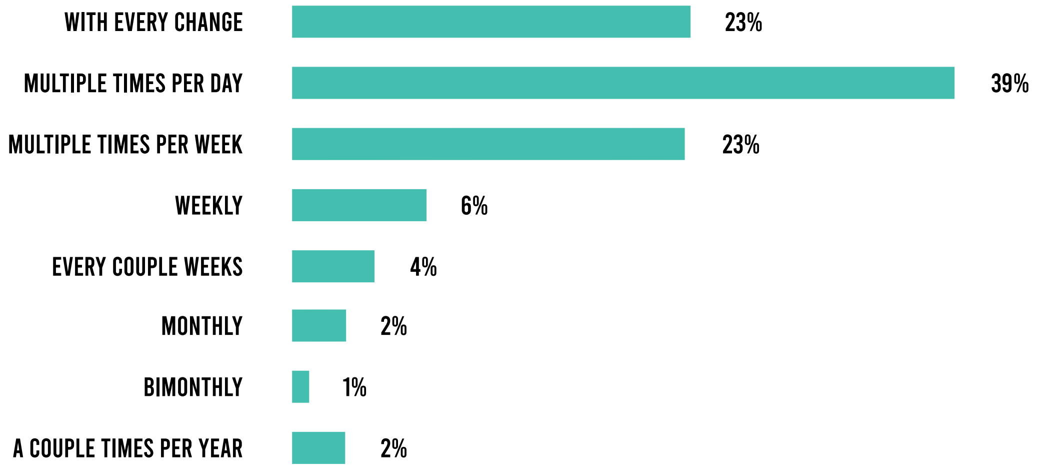


Figure 5. Percent of respondents whose companies deploy into production at given frequencies.

Another strategy that is increasingly deployed to speed the development process is the use of open-source libraries and frameworks. Forrester recently found a 40% jump in the use of open-source code in one year.[2] At the same time, the number of vulnerabilities identified in open-source code is skyrocketing at an unprecedented clip.[3] Among the respondents to this survey, two-thirds report that open-source libraries and frameworks have been adopted in at least 75% of applications (Figure 6).

Q WHAT IS YOUR LEVEL OF OPEN-SOURCE LIBRARY AND FRAMEWORK ADOPTION?

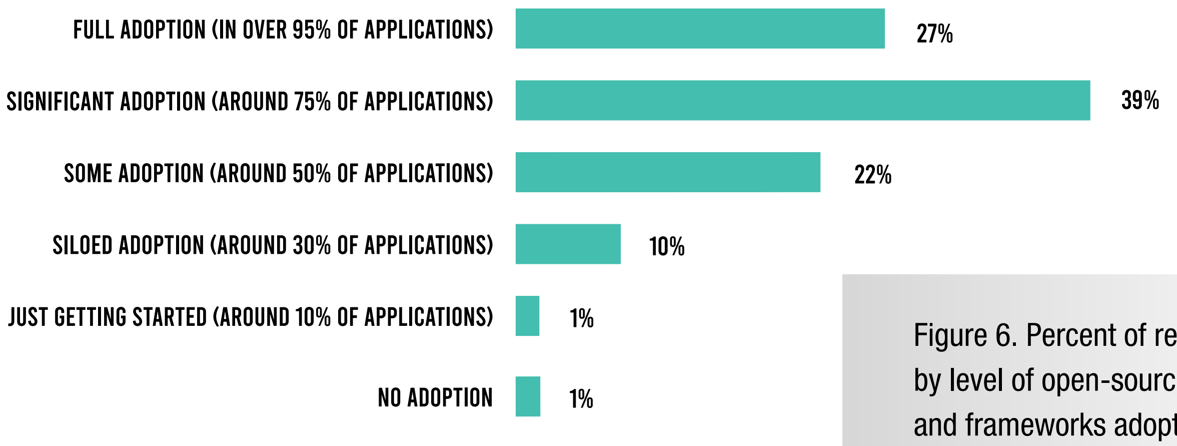


Figure 6. Percent of respondents by level of open-source libraries and frameworks adoption.

> "MY SUCCESS IS MEASURED BY WHETHER I COMPLETE TASKS BY THE GIVEN DEADLINE AND NOT IF THEY ARE SECURE."
>
> – SURVEY RESPONDENT, WEB DEVELOPER

INSIGHT: MODERN DEVELOPMENT TEAMS HAVE DEDICATED APPLICATION SECURITY HEADCOUNT AND USE A VARIETY OF APPLICATION SECURITY TOOLS

As applications have grown in importance at organizations, they have also been the target of more attacks.[4] As a result, most large technology companies now largely rely on professionals with specific skills in application security—rather than entrusting the larger security team or software developers to play that role. For 57% of respondents, that dedicated headcount is a part of the security team while just

1% have that headcount reporting to the development team (Figure 7). Having a software security group that focuses on application security is consistent with the guidelines from the Building Security In Maturity Model (BSIMM).[5]

Q DO YOU HAVE A DEDICATED HEADCOUNT RESPONSIBLE FOR APPLICATION SECURITY?

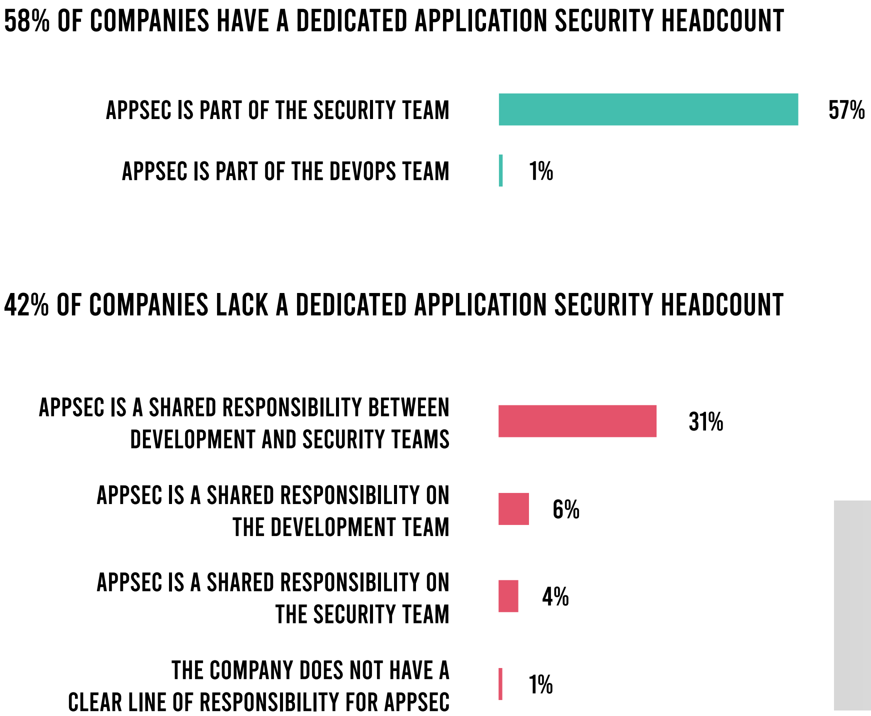


Figure 7. Existence and reporting structure of dedicated application security professionals.

APPLICATION SECURITY TOOLS IN USE

As noted above, many survey respondents believe the tools they use differentiate their teams. In the case of application security tools, an astounding 65% report that they primarily rely on solutions developed in-house (Figure 8). In these instances, development teams have gone out and designed and built their own application security tools.

Q WHAT BEST DESCRIBES YOUR APPLICATION SECURITY TOOL APPROACH (SELECT ONE)?

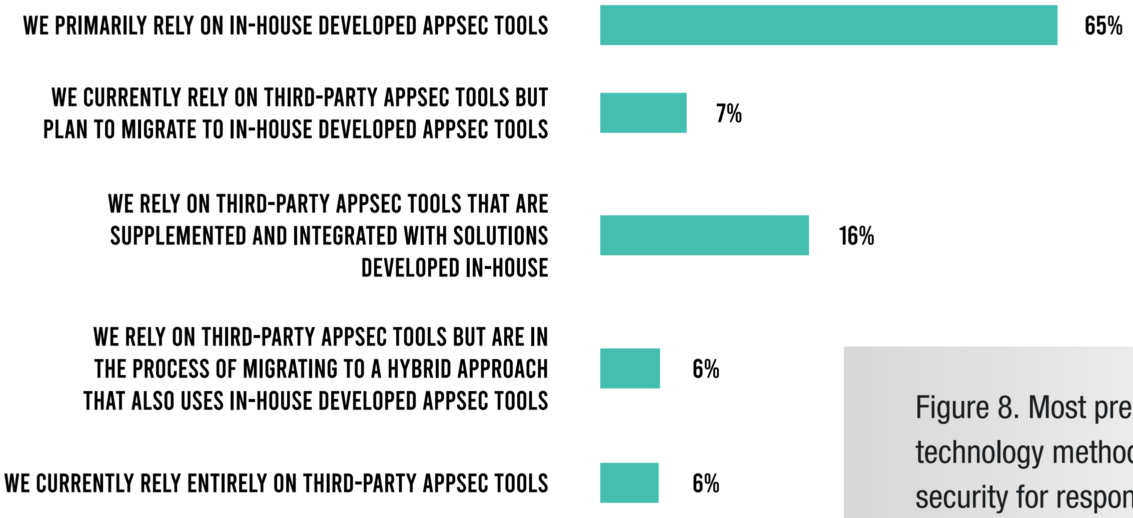


Figure 8. Most predominant technology method of application security for respondents.

By far, the most commonly used tools (Figure 9) are static application security testing (SAST; 62%) and dynamic application security testing (DAST; 52%). These legacy application security solutions have existed for close to two decades and have their limitations in terms of both security and efficiency.[6] Surprisingly few use another piece of legacy technology for open-source code: software composition analysis (SCA) tools (21%).

Fortunately, newer, more effective application security technology is also in place at many technology companies. Interactive application security testing (IAST) is in use at 63% of organizations, and runtime application self-protection (RASP) technologies are present at 38%. Unfortunately, many application security tools of all types remain unintegrated with the CI/CD pipeline. This is true of close to 4 in 10 IAST users and a small majority of RASP users. A lack of integration results in manual security processes, and almost inevitably, security-related delays to coding.

Q WHAT APPLICATION SECURITY TOOLS ARE YOU USING (ANSWER THOSE THAT APPLY)?

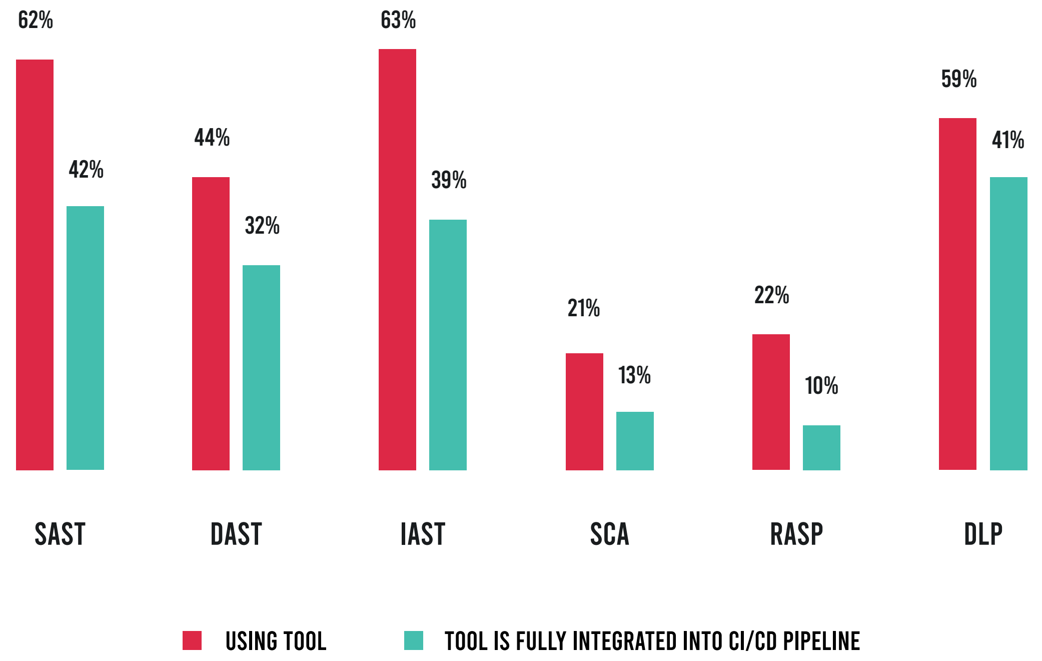


Figure 9. Percent of respondents who use each application security tool and percent who report the tools are fully integrated into their CI/CD pipeline.

> "SPEED CAN BE IMPROVED IF A TEAM USES THE RIGHT TOOLS, BUT A LACK OF KNOWLEDGE [OF THOSE TOOLS] CAN CREATE CHALLENGES."
>
> – SURVEY RESPONDENT, BUILD ENGINEER

INSIGHT: MODERN DEVELOPMENT TEAMS STRUGGLE WITH APPLICATION SECURITY OUTCOMES

Many developers also reveal inconsistencies and potential gaps in application security. When asked to rate which application security challenges were problematic at their organizations, solid majorities reported that they spend too much time triaging and diagnosing alerts (79%) and have too many application security tools (71%), false positives (69%), and false negatives (68%; Figure 10).

Six in 10 said they spend too much time coordinating with their security team on vulnerability remediation—a figure that increases to 69% for teams managing more than 800 applications. And nearly three-quarters (73%) say they are unable to find and retain application security specialists. Many of theseissues are related to the constant pressure to develop software quickly.

Q RATE THE FOLLOWING APPLICATION SECURITY CHALLENGES.

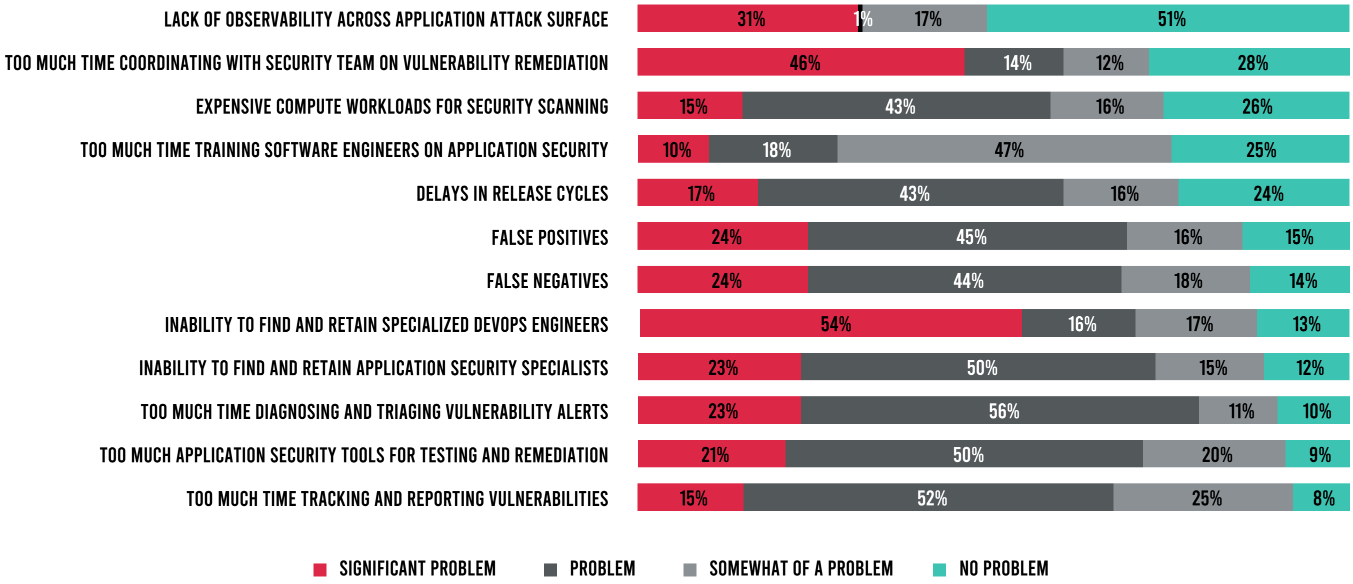


Figure 10. The most pressing application security challenges.

SECURITY STRUGGLES WITH DEVELOPMENT TOOLS

Furthermore, respondents express reservation about the security of their development tools (Figure 11). Container security is a particular struggle, with only 30% expressing confidence and 50% flatly saying they are not confident. That number increases to 62% that are not confident among teams managing fewer than 250 applications.

Confidence is only slightly more common when it comes to application programming interfaces (APIs; 36%) and CI/CD infrastructure (33%). These tools are critical in helping teams achieve faster speed, but a lack of adequate security may be offsetting these benefits at many organizations.

Q

WHAT IS YOUR LEVEL OF SECURITY CONFIDENCE WHEN IT COMES TO THE FOLLOWING AREAS (VIZ., YOU HAVE FULL VISIBILITY AND THE ABILITY TO IDENTIFY AND REMEDIATE ALL VULNERABILITIES)?

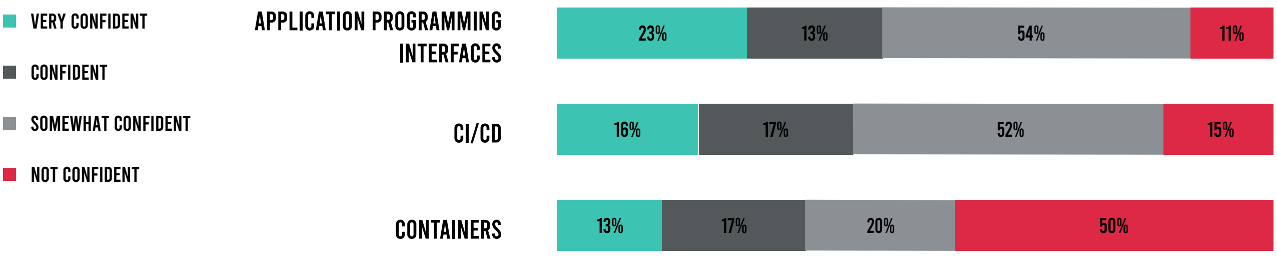


Figure 11. Percent of respondents with confidence in application security in API, container, and CI/CD security.

IMPACTS ON APPLICATION SECURITY OUTCOMES

These struggles are reflected in specific outcomes reported by respondents. For example, an astounding 85% report that the average application in development has more than 10 vulnerabilities (Figure 12), while nearly half (44%) have more than 20. And 69% of organizations must remediate software vulnerabilities at least once every two to three days (Figure 13).

Q HOW MANY VULNERABILITIES DOES THE AVERAGE APPLICATION IN DEVELOPMENT HAVE?

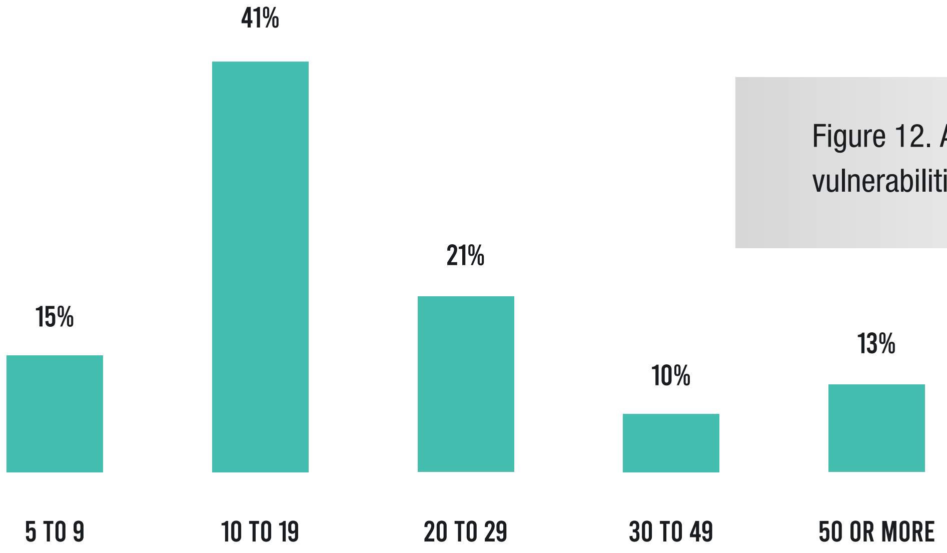


Figure 12. Average number of vulnerabilities per application.

Q HOW OFTEN DOES YOUR DEVELOPMENT TEAM NEED TO FIX VULNERABILITIES?

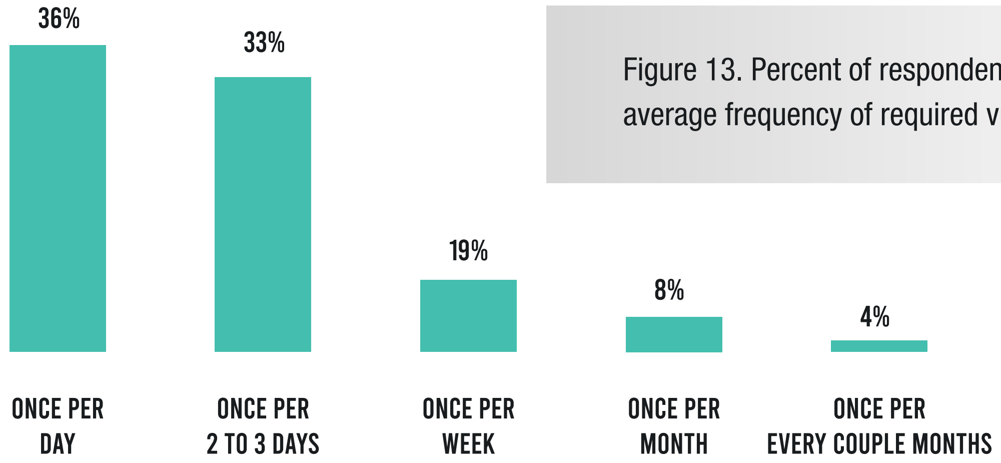
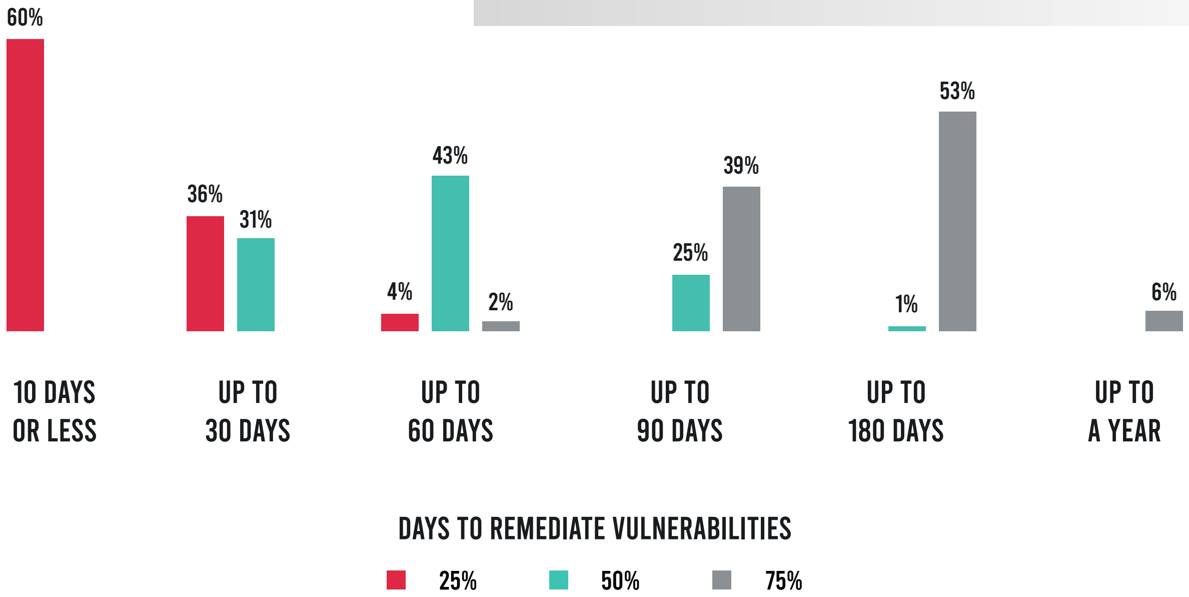


Figure 13. Percent of respondents reporting average frequency of required vulnerability fixes.

Q HOW LONG DOES IT TAKE YOU TO REACH THESE REMEDIATION MILESTONES?

Figure 14. Time to reach application security milestones.



When asked how many days it takes to remediate 25%, 50%, and 75% of vulnerabilities on the average application, the figures reflect relatively slow remediation times (Figure 14). Only 31% of respondents reach the 50% milestone (the *median* time to remediate) within 30 days, and only 41% reach the 75% milestone within 90 days.

These figures suggest that organizations struggle with timely remediation of vulnerabilities, which can pose significant costs. One study found that the cost of fixing a software vulnerability after the design phase increases sixfold if the vulnerability is found during implementation, fifteenfold if it is detected in testing, and a hundredfold if it is identified in production.[7]

RECOGNITION OF A NEED FOR APPLICATION SECURITY KNOWLEDGE

Given these struggles, it is not surprising that 77% of developers expressed a desire to receive more training in application security and potentially assume greater responsibility in the area (Figure 15). This adds a positive note to this discussion, as development professionals want to be a part of the solution. From their perspective, delivering secure code in an efficient way contributes toward the goals they are measured by—even if metrics like MTTR are not included in their performance reviews.

Q IS APPLICATION SECURITY AN AREA WHERE YOU ASPIRE TO ASSUME GREATER RESPONSIBILITY AND SPEND MORE TIME IN TRAINING?

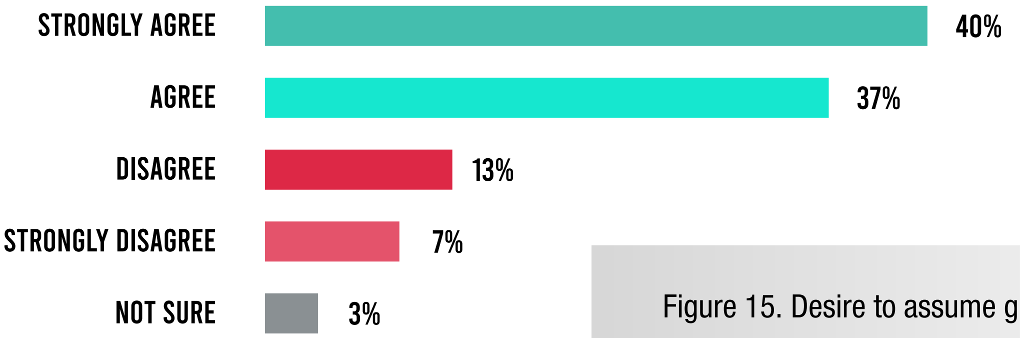


Figure 15. Desire to assume greater responsibility and spend more time in training on application security.

“WE CANNOT INTEGRATE [APPLICATION SECURITY TOOLS] PROPERLY WITH OUR IN-HOUSE SECURITY SOLUTIONS.”

– SURVEY RESPONDENT, MANAGER OF SOFTWARE ENGINEERING

04 | CONCLUSION

Modern development teams have improved their speed and efficiency dramatically over the past several years. Survey findings indicate that 85% of teams now deploy code into production at least multiple times per week—and many do so even more frequently. Open-source libraries and frameworks have achieved near universal use, and two-thirds (66%) of teams use them in more than three-quarters of their applications. Despite these great strides, today’s rapidly evolving digital marketplace makes further business acceleration a top priority. Nearly eight in 10 developers (79%) report that they feel pressure to move even faster.

INCREASED RISK

The result is often increased risk for organizations. Data from this survey confirms the reality that application security is truly a work in progress for developers—even at some of the world’s largest and most innovative companies. At the same time, applications are increasingly targeted by attackers. Verizon’s latest “Data Breach Investigations Report” found that 43% of data breaches this past year were the result of a web application vulnerability—a figure that more than doubled over the previous year.[8]

Survey data indicates that 85% of companies have an average of 10 or more vulnerabilities per application, and at 61% of organizations more than one-quarter of discovered vulnerabilities still exist after 90 days. More than two-thirds of developers (68%) struggle with false negatives in their application security tools, bringing significant risk that vulnerabilities will slip into production.

SECURITY-RELATED DELAYS TO DEVELOPMENT

These application security struggles also serve to delay the development process when management is pushing to accelerate it. Nearly nine in 10 developers (89%) must interrupt their work at least weekly to fix vulnerabilities. Nearly eight in 10 (79%) respondents spend too much time triaging and diagnosing alerts—including false positives (69%), for which legacy application security tools are notorious.[9] Six in 10 spend too much time coordinating with the security team. And since approximately half of application security solutions in place are not integrated with the CI/CD pipeline, the result is often manual work to correlate unconnected tools. It is obvious that developers simply cannot tolerate the myriad security-related delays they now experience.

To be clear, it is not that developers do not care about security: 77% would like more training and responsibility in the field—and this can be seen as one of the bright spots of this report. Likewise, their management recognizes the critical role of application security. A significant minority of modern developers (36%) have security-focused metrics as a significant part of their performance review. And nearly six in 10 organizations (58%) now have dedicated application security headcount. While the onboarding of these specialized security professionals can be seen as a positive development, it is equally clear that such a strategy cannot scale to the accelerating demands on the development team. Nearly three-quarters (73%) of respondents state that finding such talent is a struggle.

TAKEAWAYS FOR NEXT STEPS

While the survey data indicates much room for improvement when it comes to outcomes, there are also bright spots. More than six in 10 (63%) of organizations are off to a good start with the deployment of an IAST solution. Pairing such a solution with a security tool for open-source libraries and frameworks, as well as with a RASP offering that extends continuous protection into production that blocks exploits in real time, empowers developers to leverage modern application security technology across the software development life cycle (SDLC).

But simply finding a set of point application security solutions that use newer technology is inadequate. As is the case with all aspects of cybersecurity, integration is key. Application security solutions that are disconnected from each other—and from different development tools and processes—prevents security observabililty.

Security observability is achieved by ingesting the data of security attributes from within running applications or APIs, across distributed systems, in a format that can be easily analyzed and actioned. An instrumentation approach unlocks security observability, and enables teams to ask the right questions as to why their software is not secure and respond effectively. This empowers development, operations, and security teams to improve their application risk posture while significantly improving business outcomes.

[1] "52% of Companies Sacrifice Cybersecurity for Speed," Threat Stack, March 13, 2018.

[2] Amy DeMartine, et al., "Application Security Market Will Exceed $7 Billion by 2023," Forrester, updated March 29, 2019.

[3] Liam Tung, "Open-source Security: This is why bugs in open-source software have hit a record high," ZDNet, March 13, 2020.

[4] "2020 Application Security Observability Report," Contrast Security, July 24, 2020.

[5] Sammy Migues, et al., "Building Security in Maturity Model, Version 10 (BSIMM10)," BSIMM, accessed September 4, 2020.

[6] "A Major Roadblock to Business Innovation: How Traditional AppSec Delays DevOps Release Cycles," Contrast Security, April 30, 2020.

[7] Mukesh Soni, "Defect Prevention: Reducing Costs and Enhancing Quality," iSixSigma, accessed April 9, 2020.

[8] "2020 Data Breach Investigations Report," Verizon, April 2020.

[9] "A Major Roadblock to Business Innovation: How Traditional AppSec Delays DevOps Release Cycles," Contrast Security, April 30, 2020.

CONTRAST
SECURITY

240 3rd Street
Los Altos, CA 94022
888.371.1333

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.