THE LINUX FOUNDATION | Research

CLOUD NATIVE COMPUTING FOUNDATION

2024 Cloud Native Security Report

How Organizations Are Addressing Security for Cloud Native Application Development

Stephen Hendrick, *The Linux Foundation*
Adrienn Lawson, *The Linux Foundation*
Jeffrey Sica, *The Linux Foundation*

Foreword by
Eddie Knight, *Sonatype*

October 2024

2024 Cloud Native Security Report

84% of organizations report their cloud native applications are **more secure** than they were two years ago.

76% of organizations report much or nearly all their **application development is cloud native.**

The #1 challenge in securing cloud native applications: **the complexity of software and infrastructure.**

The #1 vendor challenge in securing cloud native applications: **keeping up with emerging threats.**

40% of organizations experience cloud infrastructure and services **security incidents.**

63% of organizations are using static application security testing **(SAST) tools.**

51% of organizations use **manual code reviews** to assess security on every update.

49% of organizations use **CI/CD security testing** on every update.

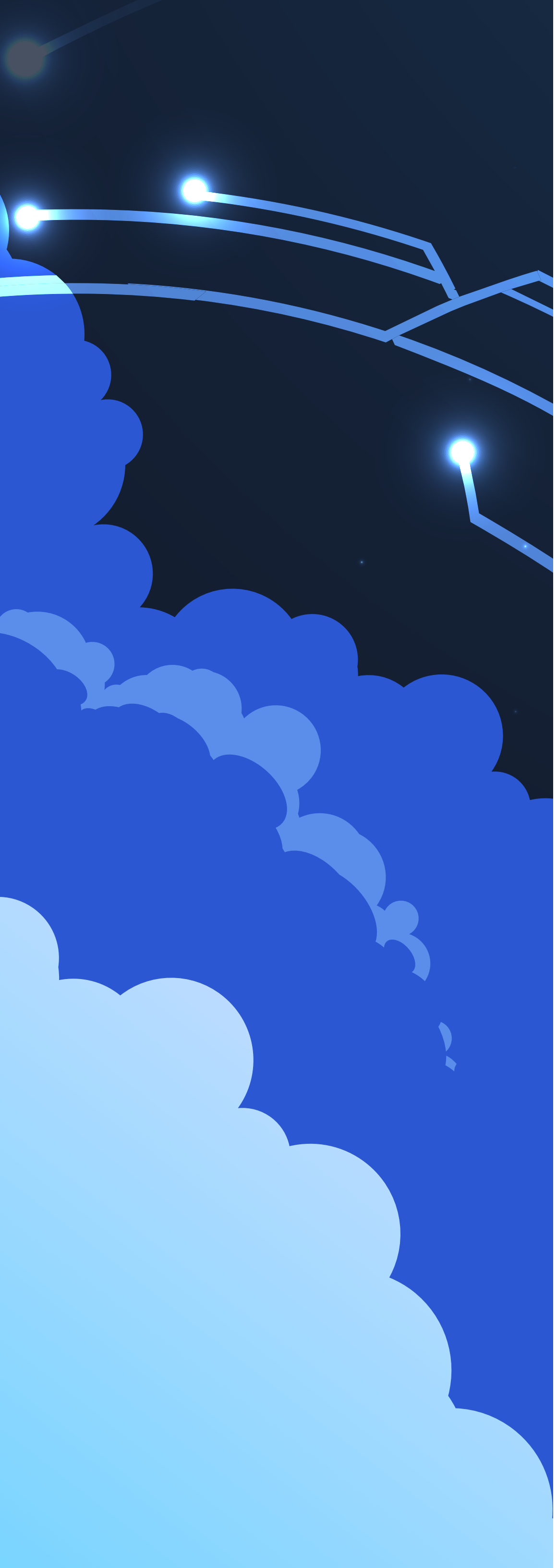
The #1 security assessment growth area: **vulnerability scanning and remediation.**

84% of respondents report that **manual code reviews** are either extremely important or important.

67% of respondents use **CNCF webinars / workshops & conferences** to stay informed about cloud native security tools & updates.

65% of respondents rely on **CNCF best practices** to make progress in securing their cloud native applications.

Contents



Foreword

The work produced by LF Research is a pillar of innovation across the open source community, for maintainers and users alike. This collaboration between CNCF and LF Research has demonstrated that significant progress is being made to improve the security of software globally, and reveals the elements that the community finds most valuable for cybersecurity.

In recent years we've seen a significant rise in the number of cyber attacks, including more malicious open source packages being produced in 2024 than all other years combined— and this report also shows that 76% of organizations now rely heavily on cloud native development. The attack surface of our most critical infrastructures is now larger and more complex than many of us thought was possible— but this report features a glimmer of hope: 84% of organizations report their cloud native applications are more secure today than they were two years ago.

Much of this hope stems from the rising usage of automation such as Software Composition Analysis (SCA) tools, which help identify vulnerabilities and mitigate risks related to the open source components that power modern applications. But simply having automated tooling is not enough— and many organizations seem to understand that. For the other half of the room, I'll remind you: Manual testing, policies, and reviews are essential. Without proper human review of SCA policy violations, evaluation of proper test coverage, and manual line-by-line security reviews, the attack surface is inadequately defended.

Beyond the tools and technologies, this report highlights another essential aspect of security: staying informed. The threat landscape is constantly evolving, and keeping up with the latest risks and best practices can be challenging. That's why 67% of respondents turn to CNCF webinars, workshops, and conferences. The reason that Sonatype has supported events such as KubeCon/CloudNativeCon for the past several years is that we know these spaces provide the most effective tools for participants to share knowledge and learn how to apply best practices in their own environments.

This report offers a clear picture of the current state of cloud native security and serves as a reminder that continuous learning and adaptation are essential, and multifaceted. Whether it's through leveraging the right tools or actively participating in community events, staying engaged and informed is key to keeping our systems secure in an ever-changing environment.

Eddie Knight, *CNCF TAG* Security Co-Chair, FINOS Technical Oversight Committee, Sonatype OSPO Lead

Introduction

The building blocks of cloud native computing—containerization and microservices architecture—began their IT ascent about fifteen years ago. Five years later, orchestration (Kubernetes) and DevOps (CI / CD) added key infrastructural and procedural elements that would foster industry-wide cloud native computing adoption. Building on past generational experience and best practices, cloud native computing saw the addition of tooling (often open source) to enable key capabilities, including automated provisioning, version control, on-demand scalability, decentralized manageability, API-driven interactions, observability, traffic management, and polygraph programming. The result has been that cloud native computing represents a thoroughly modern approach to application development, deployment, and operations.

However, the attributes that enable cloud native computing to be powerful, effective, and productive demand a sophisticated approach to cybersecurity. The distributed architecture of cloud native computing means that each microservice may have its own set of vulnerabilities, and the communication between services needs to be secure to prevent data breaches and unauthorized access. The dynamic nature of cloud native environments (frequent deployments, bidirectional scaling, and infrastructural changes) can make traditional security measures less effective and require security practices that are automated, scalable, and adaptable to new threats. The complexity of cloud native architectures, which include containers, serverless functions, and orchestration tools, increases the available attack surface with each component, introducing potential vulnerabilities that require monitoring and security on a continual basis.

The threat landscape is also continuously evolving with attackers developing new methods to exploit cloud environments. Continuous monitoring, threat intelligence, and adaptive security measures are all necessary to stay ahead of potential threats.

The Cloud Native Computing Foundation (CNCF) engaged Linux Foundation Research in March 2024 to develop and execute an empirical research study to understand how organizations are addressing cloud native security. The target audience included respondents who met the following criteria:

- Must be involved in the development of cloud native applications
- Must be familiar with how the organization they work for deals with the security of its cloud native applications
- The organization must be using cloud native technologies and techniques
- Must be employed

Survey development by Linux Foundation Research occurred in March 2024, and the survey was fielded in April 2024, yielding 200 completed surveys. For more information about the survey methodology and survey demographics, see the *About the survey* section toward the end of this report.

Cloud native security study findings

The relationship between the cloud native app security and the adoption of cloud native techniques

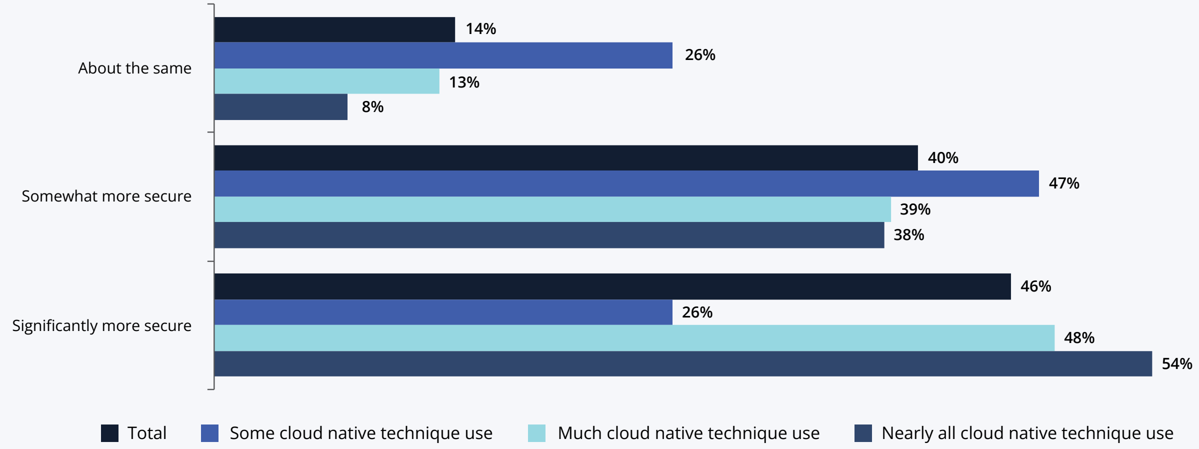
The focus of most organizations on cybersecurity over the last two years has been paying off. In this survey, when we asked organizations how secure their cloud native apps were compared to two years ago (Q21), only 1% (just three respondents) said less secure, 14% said about the same, and 85% said more secure as shown in FIGURE 1. The 85% saying more secure is composed of 40% that said somewhat more secure and 45% that said significantly more secure. This suggests that organizations have consciously been investing in cybersecurity.

When we look at the adoption of cloud native techniques (Q7, not shown), just 5% were beginning to use cloud native techniques, 19% reported some development was cloud native, 44% said much of their development was cloud native, and 33% said that nearly all their development was cloud native.

FIGURE 1

DEEPER CLOUD NATIVE ADOPTION SUGGESTS INCREASED PERCEIVED SECURITY IN CLOUD NATIVE APPLICATIONS

How secure are you cloud native apps compared to 2 years ago? (select one) segmented by: To what extent has your organization adopted cloud native techniques (select one)



2024 Cloud Native Security Survey, Q21a x Q7a, Sample Size = 188

However, when we compare these improvements in application security to what extent the organization has adopted cloud native techniques, a more nuanced picture begins to emerge. Of the 14% of organizations that reported no material change in their application security, the mix of organizations included 26% that said some of their application development was cloud native, 13% that reported that much of their application development was cloud native, and just 8% that said that nearly all their application development was cloud native. At the other end of the security continuum, of the 45% of organizations that reported their applications were significantly more secure, the mix of organizations included 26% that said some of their application development was cloud native, 47% that reported that much of their application development was cloud native, and 54% that said that nearly all of their application development was cloud native. So, one can infer that greater adoption of cloud native techniques leads to better security or that increased security drives more organizations to adopt cloud native techniques. The degree to which organizations have adopted cloud native techniques may influence their perception of security improvement. Those deeply invested in cloud native technologies feel more secure, likely due to better and more integrated security practices. Either way, it's a win.

The leading challenges in securing cloud native applications by scope of cloud native development

The leading challenges that organizations experience in securing their cloud native applications depend on where they are in their cloud native journey. FIGURE 2 shows the top eight leading challenges, which showcase several key findings.

Complexity remains consistent: Across all levels of adoption, complexity remains a top challenge, indicating that as cloud native techniques become more integral to operations, the systems' intricacies and the need for sophisticated management increase.

Emerging threats and advanced adoption: Higher levels of cloud native adoption correlate with an increased emphasis on security challenges related to emerging threats, reflecting the ongoing need for vigilance and continuous improvement in security capabilities.

Regulatory compliance: As organizations deepen their reliance on cloud technologies, compliance with regulations becomes more challenging, underscoring the need for robust governance frameworks.

The challenge of beginning a cloud native journey: FIGURE 2 generally shows a dichotomy between organizations that are early in their cloud native journey compared to organizations where much or nearly all development is cloud native. Money (37%) and lack of security awareness (32%) are leading challenges for organizations where just some development is cloud native but far less so for other more mature cloud native organizations. Alternatively, keeping up with threats (29%), secure deployment (24%), and regulatory compliance (21%) are far less of a concern for organizations where just some development is cloud native but far more so for other more mature cloud native organizations.

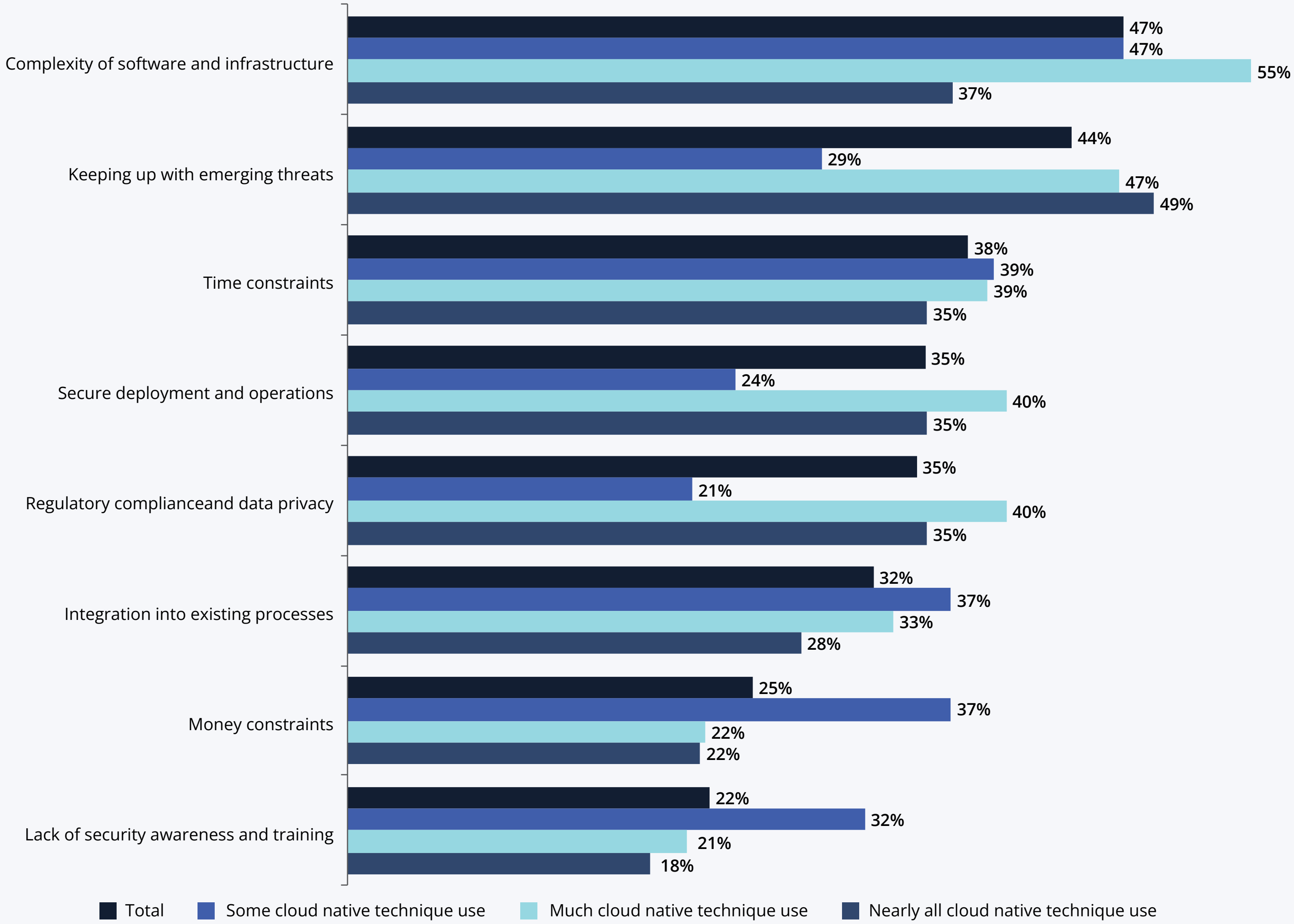
The leading challenges in securing cloud native applications by type of organization

Securing cloud native applications will always have its challenges, but these challenges vary considerably depending upon whether the organization is a vendor / service provider or end-user organization (an organization whose product is industry-focused and is an "end user" of IT products and / or services). FIGURE 3 again shows the leading challenges in securing cloud native applications but this time segmented by type of organization.

FIGURE 2

LEADING CHALLENGES IN SECURING CLOUD NATIVE APPLICATIONS BY SCOPE OF CLOUD NATIVE DEVELOPMENT

What are the biggest challenges you face in securing your cloud native applications? (select all that apply) segmented by: To what extent has your organization adopted cloud native techniques

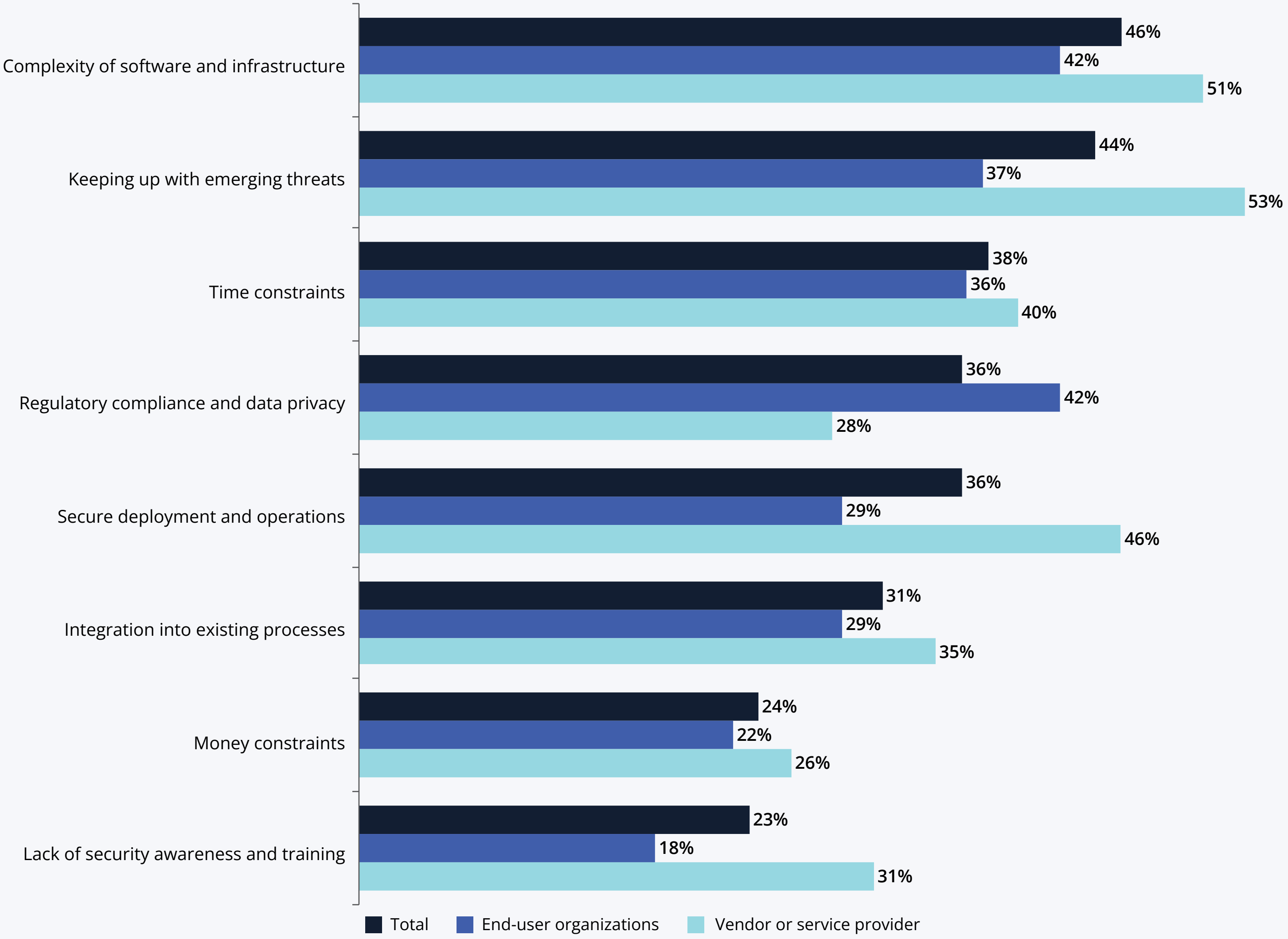


2024 Cloud Native Security Survey, Q20 x Q7a, Sample Size = 190, Valid Cases = 190, Total Mentions = 601

FIGURE 3

LEADING CHALLENGES IN SECURING CLOUD NATIVE APPLICATIONS BY ORGANIZATION TYPE

**What are the biggest challenges you face in securing your cloud native applications? (select all that apply)
segmented by: What type of organization or entity do you work for? (select one)**



2024 Cloud Native Security Survey, Q20 x Q13a, Sample Size = 188, Valid Cases = 188, Total Mentions = 597

FIGURE 3 shows that keeping up with emerging threats (53%), complexity of software and infrastructure (51%), and secure deployments (46%) are the three leading concerns for vendors and service providers. End users see complexity of software and infrastructure (42%), keeping up with emerging threats (37%), and time constraints (36%) as their leading challenges. Vendors and service providers are also significantly more concerned about all these challenges than end users except for regulatory compliance. The reason could be that software vendors and service providers face more acute challenges in securing cloud native applications because they must manage security across multiple clients, environments, and infrastructures, all while maintaining compliance with diverse regulations, defending against sophisticated attacks, and upholding stringent SLAs. The complexity, scale, and higher stakes involved in their operations make securing cloud native environments particularly challenging for these organizations.

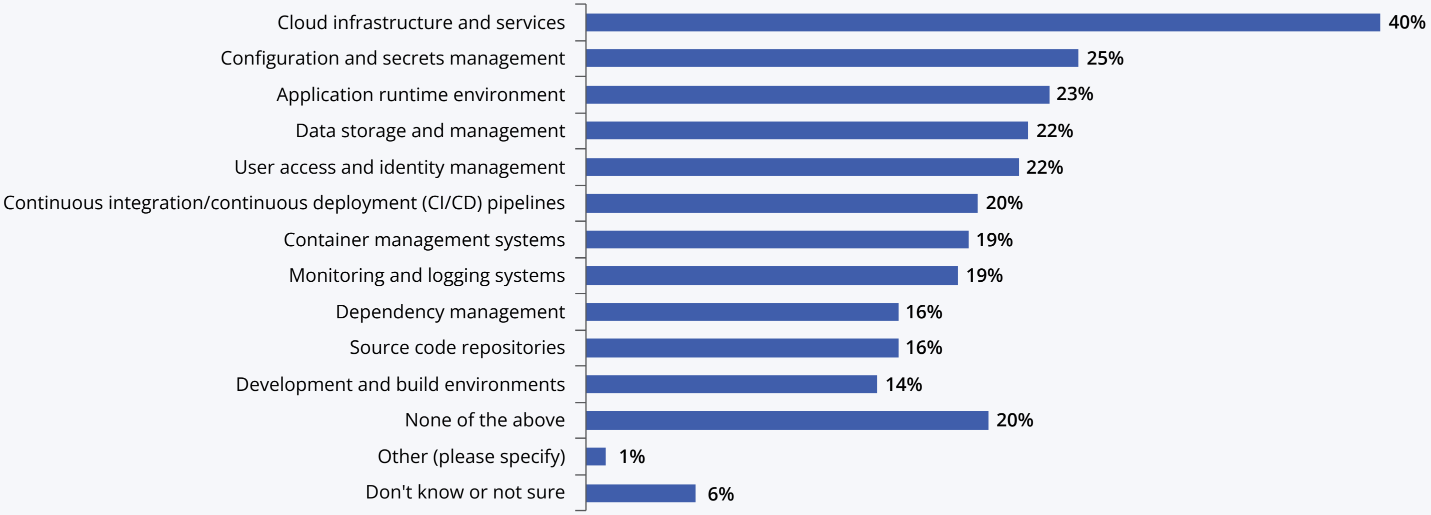
Cloud infrastructure and services dominate where security incidents occur

FIGURE 4 shows that security incidents are most likely to occur in cloud infrastructure and services by a considerable margin. The primary reason for this is that cloud environments are both highly dynamic and ephemeral. Continual change can make it difficult to maintain consistent security policies, leading to potential

FIGURE 4

WHERE ORGANIZATIONS ARE EXPERIENCING SECURITY INCIDENTS

In which areas of cloud native software development have you experienced security incidents over the last two years? (select all that apply)



2024 Cloud Native Security Survey, Q22, Sample Size = 200, Valid Cases = 200, Total Mentions = 519

gaps that attackers can exploit. Cloud infrastructure also involves multiple layers—virtualization, networking, storage, and application layers—each of which introduces potential vulnerabilities. The complexity of managing and securing these layers increases the likelihood of misconfigurations and security oversights.

The data in FIGURE 4 highlights the varied nature of security within cloud native environments (development and / or deployment), with infrastructure, configuration management, and application runtimes highlighted as primary concerns. Organizations must adopt a comprehensive security strategy that encompasses these areas to mitigate risks effectively. The data suggests a significant spread of vulnerabilities across various components of cloud native systems, reinforcing the need for an integrated and proactive approach to cloud security.

Security incidents highlight the cybersecurity risks inherent in a cloud native journey

When we segment the areas of cloud native software development where there has been a report of security incidents in the last two years by the adoption of cloud native techniques, we observe some disconcerting patterns. FIGURE 5 shows the leading areas where organizations in each segment have experienced security incidents.

The significantly lower level of security incidents observed in organizations just beginning to develop cloud native applications is largely due to their smaller, less complex environments; a more cautious and focused approach to security; and the opportunity to build security expertise as they gradually adopt cloud native practices. As organizations mature and expand their cloud native

FIGURE 5

WHERE SECURITY INCIDENTS ARE BEING EXPERIENCED SEGMENTED BY LEVEL OF CLOUD NATIVE USE

In which areas of cloud native software development have you experienced security incidents over the last two years? (select all that apply)
segmented by: To what extent has your organization adopted cloud native techniques (select one)

Leading areas experiencing incidents	Some cloud native technique use	Much cloud native technique use	Nearly all cloud native technique use
1	Application runtime environment (18%)	Cloud infrastructure and services (49%)	Cloud infrastructure and services (42%)
2	Cloud infrastructure and services (18%)	Data storage and management (29%)	Configuration and secrets management (29%)
3	Dependency management (18%)	Monitoring and logging systems (28%)	User access and identity management (28%)
Percentage of respondents who selected "None of the above"	37%	13%	22%

2024 Cloud Native Security Survey, Q22 x Q7, Sample Size = 190, Valid Cases = 190, Total Mentions = 500

deployments, the increased complexity, broader attack surface, and greater integration with other systems make security management more challenging, leading to a higher likelihood of incidents.

Organizations with extensive cloud native development experience more security incidents primarily due to the increased complexity, scale, and dynamic nature of cloud native environments. The frequent changes, reliance on third-party components, challenges in monitoring and incident response, and the need for a mature security culture all contribute to the higher likelihood of security incidents in these organizations. As they scale their cloud native practices, the complexity and potential attack surface expand, making security management more challenging.

The data indicates that as organizations increase their use of cloud native technologies, the types of security incidents experienced evolve and often increase in certain areas, reflecting both the growing complexity of environments and the higher capabilities for detection. The shift in challenges from basic infrastructure in lower adoption levels to more sophisticated areas like configuration and secrets management in higher adoption stages supports the need for advanced security strategies tailored to the maturity level of cloud native adoption.

How survivorship bias can skew perceptions of security in cloud native applications

FIGURE 6 is a visual representation of survivorship bias. This demonstrative diagram shows where returning WW2-era planes were hit. The suggestion that the red clusters should be reinforced exemplifies selection bias, as the planes analyzed did not include any with severe enough damage to crash and not return. The sample only included planes with light enough damage to return home. Therefore, the correct action is to reinforce the parts where less damage is visible.

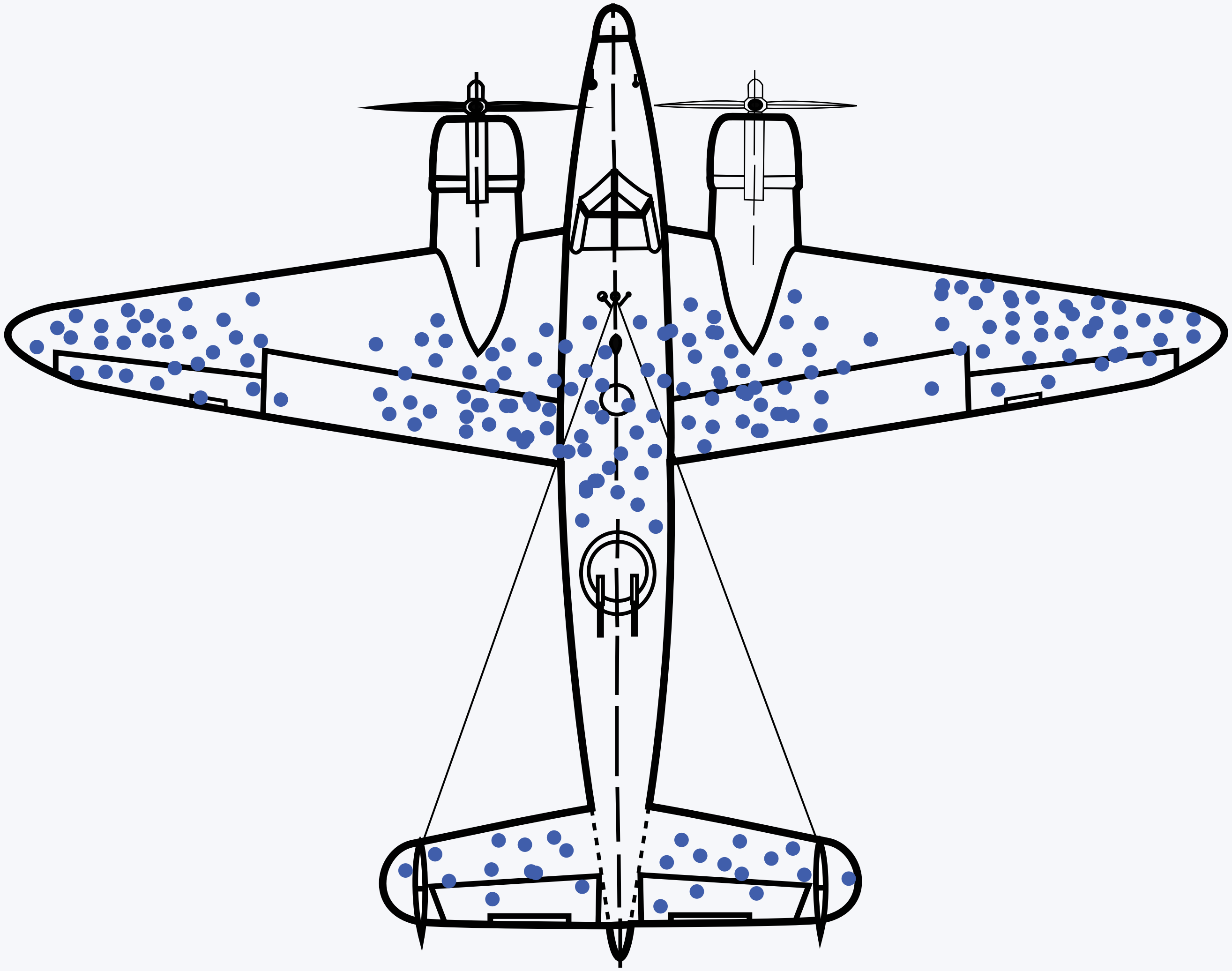
Survivorship bias or survival bias is the logical error of concentrating on entities that passed a selection process while overlooking those that did not. This can lead to incorrect conclusions because of incomplete data.

Survivorship bias is crucial to consider when interpreting data on security incidents related to cloud native technologies. Higher incident reporting in more mature cloud native organizations does not inherently point to poorer security but may indicate a greater awareness and better detection of security issues. This can skew perceptions, making it appear that higher adoption correlates directly with higher risk, whereas it may actually signal more robust security practices and detection capabilities.

FIGURE 5 highlights the very different experiences of organizations early in their cloud native journey (some cloud native technique use) compared to those who are well into their journey (much or nearly all cloud native technique use). The potential for survivorship bias in cybersecurity is a concern to organizations early in their cloud native journey. The reduced scale of cloud native operations in these organizations generally leads to a more simplistic approach to security, fewer identifiable incidents, and a greater share of organizations that have not experienced incidents across those areas presented in FIGURE 5. These organizations are likely to underestimate the importance of implementing more comprehensive security measures as they scale up their cloud native activities. The troublesome finding described in FIGURE 7 in the next section is yet another indicator that organizations early in their cloud native journey need to not just learn from their own experiences but also learn from the experiences of organizations who have achieved a mature cloud native status.

FIGURE 6

BEYOND THE NUMBERS: HOW SURVIVORSHIP BIAS CAN SKEW PERCEPTIONS OF SECURITY IN CLOUD NATIVE APPLICATIONS



Martin Grandjean (vector), McGeddon (picture), US Air Force (hit plot concept),
CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons

Security assessments and testing tools are a critical aspect of cloud native computing

The granularity and complexity of cloud native development requires a larger portfolio of bespoke testing tools. The positive finding in FIGURE 7 is that the cardinality and degree of testing tool use is now significantly greater than in past surveys. The average number of security assessment techniques in use is now 4.5 compared to between 2 to 3 in past surveys from 2022 and 2023.

Static application security testing (SAST) and software composition analysis (SCA) tools are cornerstones of security testing, and their penetration is over 60% in organizations where much or nearly all application development is cloud native. However, these same tools have much less penetration in organizations where only some of their app dev is cloud native.

Another exciting development is that between 49% to 57% of organizations are using manual code inspection, which is the gold standard in security testing. Manual code inspection is valuable for its contextual understanding, ability to catch subtle and complex issues, and role in improving overall code quality and security culture—but it is resource-intensive and may not scale well in large projects. Automated tools like SAST, SCA, and WAS / DAST are excellent at quickly identifying known vulnerabilities and ensuring compliance with established security practices, but they cannot replace the nuanced analysis and judgment that experienced human reviewers bring to the table. In practice, the best approach is often a combination of both—leveraging the speed and coverage of automated tools alongside the depth and insight of manual code inspection. This hybrid approach helps organizations maximize security while managing the limitations of both methods.

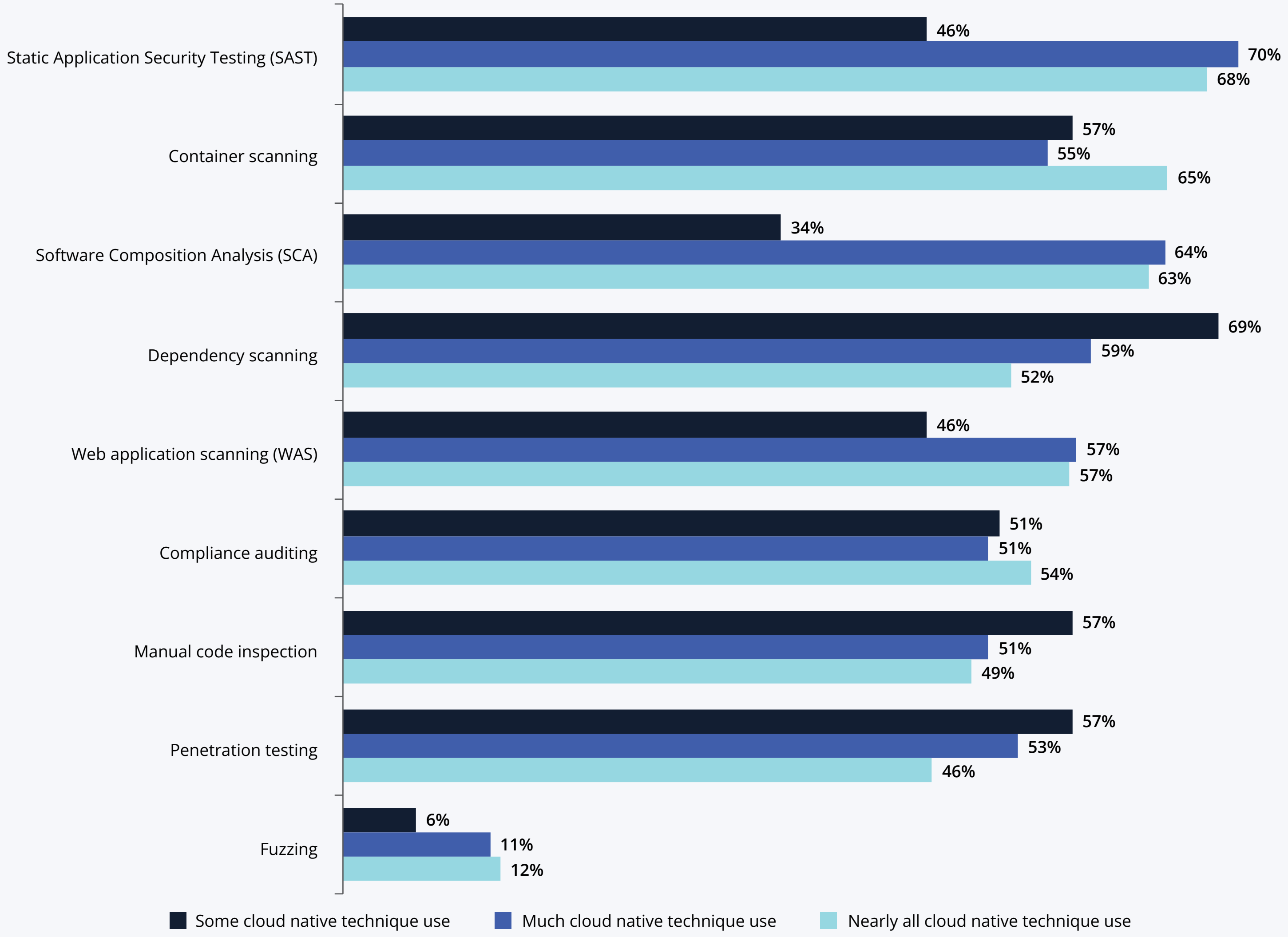
> *Static application security testing (SAST) and software composition analysis (SCA) tools are cornerstones of security testing, and their penetration is over 60% in organizations where much or nearly all application development is cloud native*

This leads us to a troublesome finding in FIGURE 7 which is that organizations that use some cloud native techniques are laggards in their adoption of SAST, SCA, and WAS / DAST. Given that these three tool categories account for the highest penetration of use by organizations where much or nearly all their application development is cloud native, the dichotomy in penetration is startling.

FIGURE 7

SECURITY ASSESSMENTS IN USE SEGMENTED BY LEVEL OF CLOUD NATIVE DEVELOPMENT

What types of security assessments do you perform? (select all that apply) segmented by: To What extent has your organization adopted cloud native techniques (select one)



2024 Cloud Native Security Survey, Q19 x Q7, Sample Size = 190, Valid Cases = 190, Total Mentions = 865, DKNS responses excluded

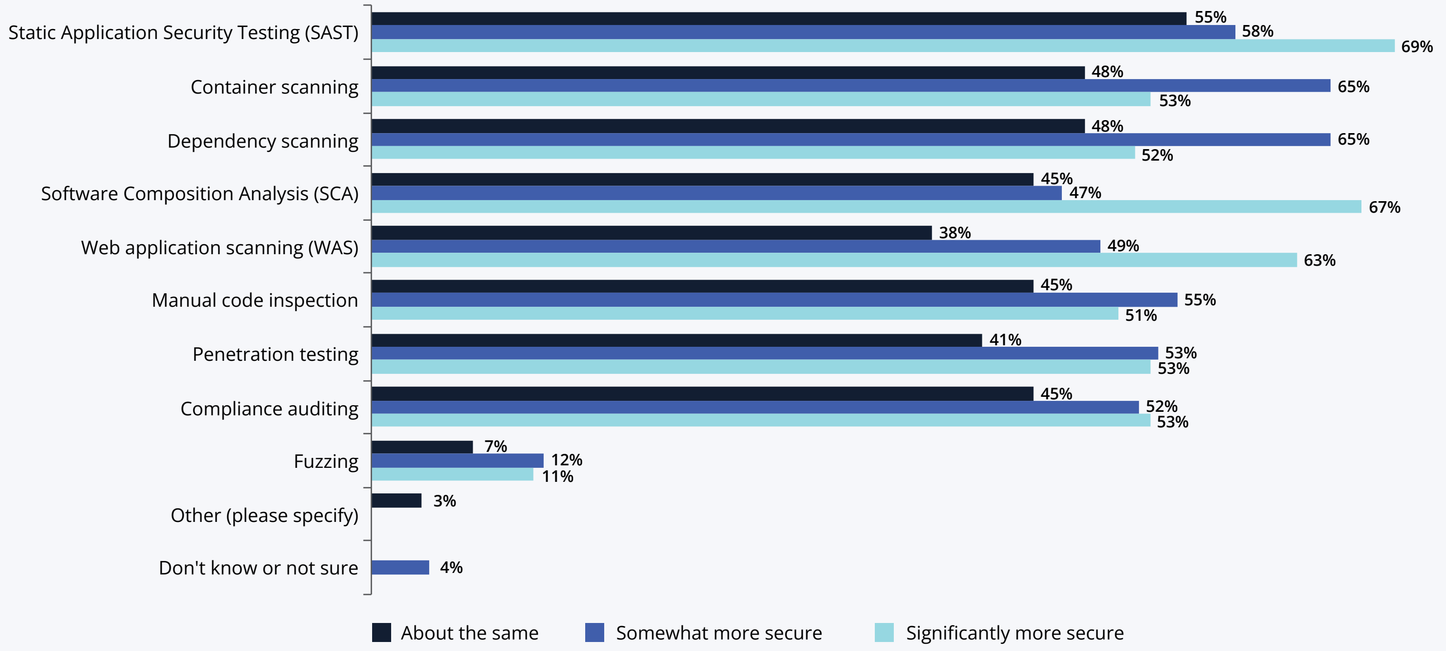
An increased use of security tools is having a positive impact on the security of cloud native applications

The increased use of security tools shown in FIGURE 7 is delivering its intended results. As mentioned in FIGURE 1, 84% of respondents believe that their cloud native applications are more secure than they were two years ago. FIGURE 8 segments the use of security tools and assessments segmented by perceptions of how security has improved. Using the "About the Same" response as a baseline, significant gains in security occur when using SAST, SCA, and WAS (DAST) tools. Container scanning and dependency scanning also show material gains.

FIGURE 8

SECURITY ASSESSMENTS IN USE SEGMENTED BY HOW THE SECURITY OF CLOUD NATIVE APPLICATIONS HAS CHANGED

What types of security assessments do you perform? (select all that apply) segmented by: How secure are you cloud native apps compared to 2 years ago? (select one)



2024 Cloud Native Security Survey, Q19 by Q21a, Sample Size = 197, Valid Cases = 197, Total Mentions = 891

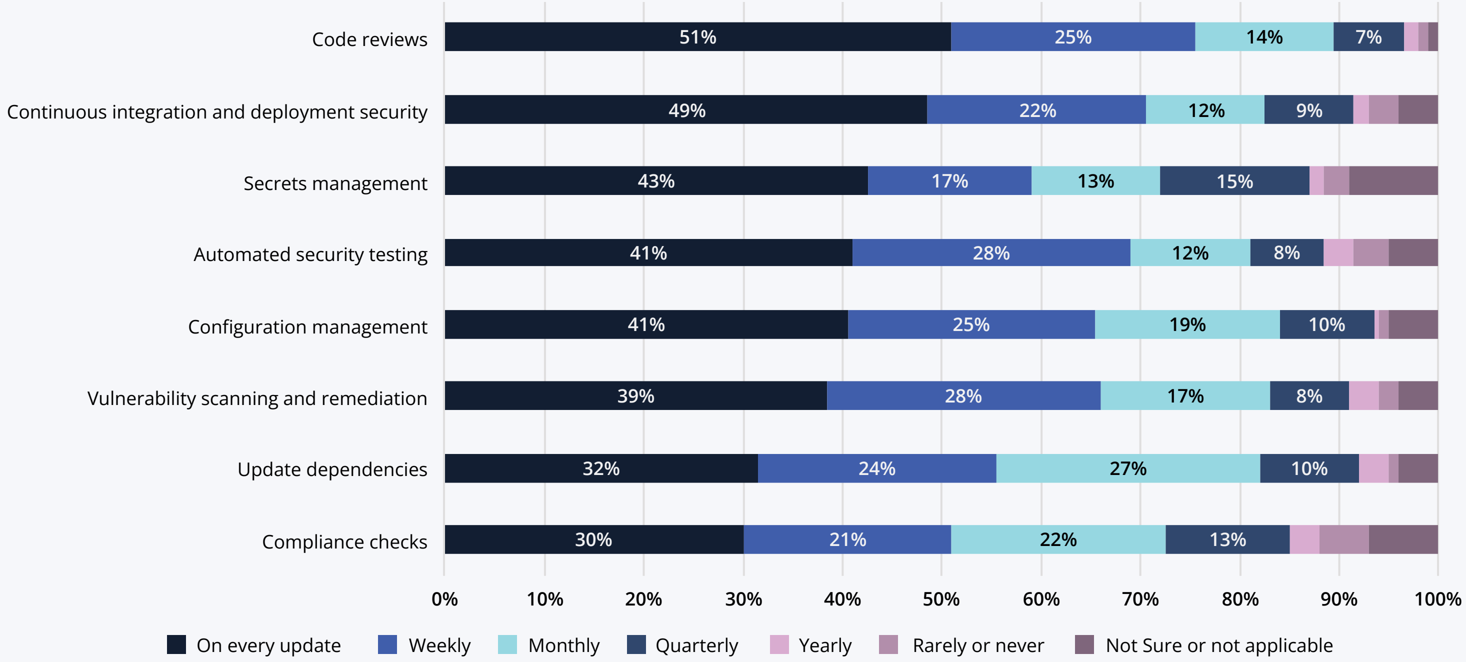
Key security strategies include code reviews and CI/CD security

FIGURE 9 shows that manual code reviews are an effective tool for improving cloud native security, offering deep insights into business logic, architectural patterns, and complex security issues that automated tools may miss. When combined with automated security testing tools like SAST and SCA, manual reviews can significantly enhance the security posture of cloud native applications by addressing both technical vulnerabilities and context-specific threats.

FIGURE 9

USAGE CHARACTERISTICS OF COMMON SECURITY STRATEGIES FOR CLOUD NATIVE APPLICATION DEVELOPMENT

How often does your organization practice the following security strategies within cloud native ecosystems? (one response per row)



2024 Cloud Native Security Survey, Q17, Sample Size = 200

However, the effectiveness of manual reviews depends on the expertise of the reviewers, the thoroughness of the review process, and the ability to integrate the findings into the broader development and security workflows. In practice, you achieve the best results by using manual code reviews in conjunction with automated tools to create a comprehensive security strategy.

CI / CD security is essential for ensuring that the automation and efficiency benefits of CI / CD pipelines do not come at the expense of security. By embedding security practices throughout the pipeline—from code development and dependency management to deployment and monitoring—organizations can maintain a strong security posture while delivering software quickly and reliably.

One of the strategies shown in FIGURE 9 that could use improvement is automated security testing. Given the automated testing capabilities of many security tools and today's reality that only 41% of organizations use these tools on every update, there is clear room for improvement.

Vulnerability scanning, automated security testing, and CI / CD security are a fast path to improved security

Intersecting security strategies used in cloud native ecosystems (FIGURE 9) with organizational perceptions on how much cloud native security has improved over the last two years provides insight into strategies that perform best. In FIGURE 10, using "About the same" as a baseline again, the most significant improvements from the baseline are associated with the use of vulnerability scanning and remediation tools, automated security testing, and CI / CD security.

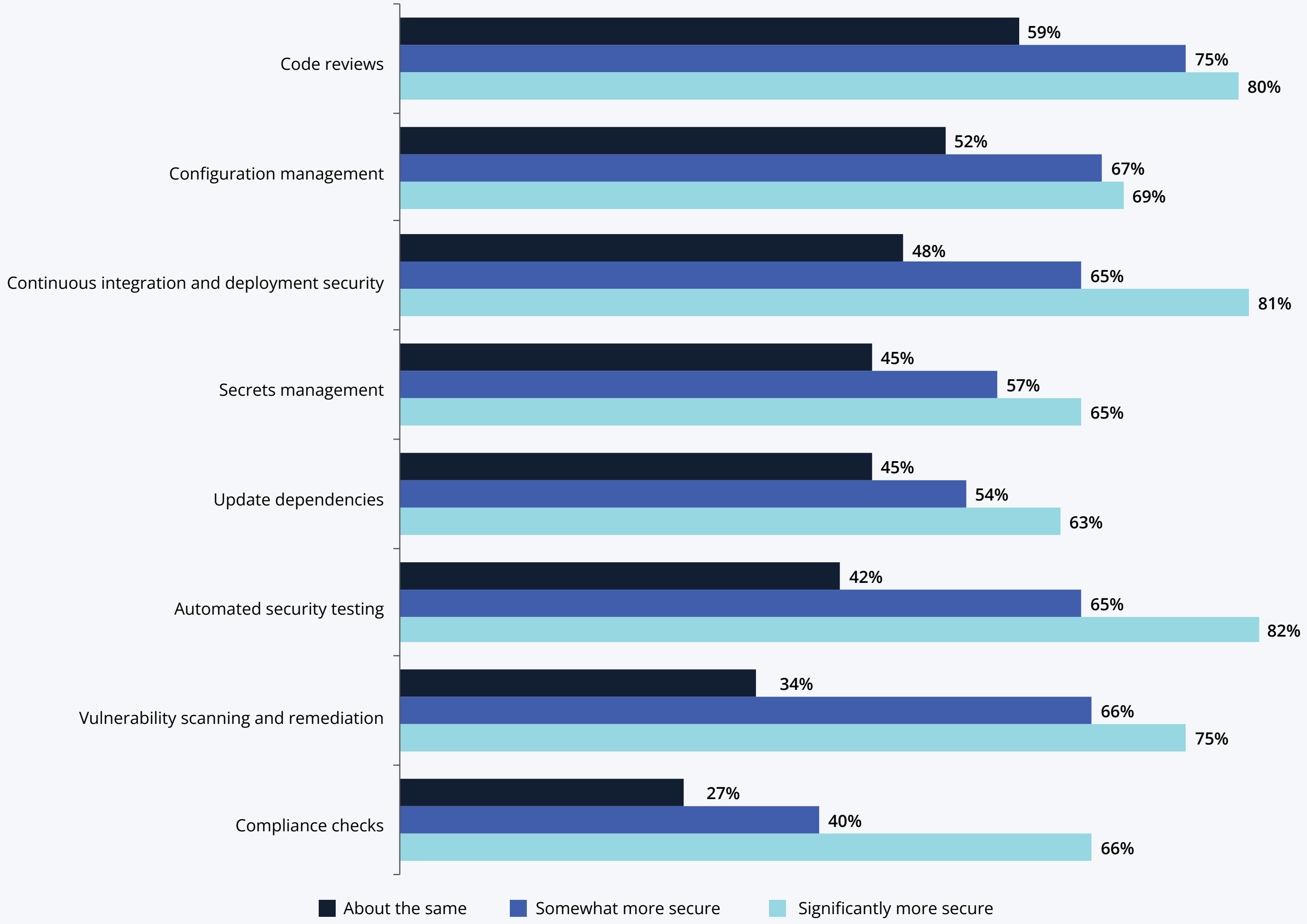
By embedding security practices throughout the pipeline—from code development and dependency management to deployment and monitoring—organizations can maintain a strong security posture while delivering software quickly and reliably.

There is a clear trend where organizations that perceive their cloud native applications as "Significantly more secure" tend to practice security strategies more frequently. This suggests a correlation between frequent, proactive security measures and improved security perceptions. As organizations increase their commitment to frequent security practices like automated testing, continuous integration, and vulnerability scanning, they tend to perceive their environments as more secure. Code reviews are again the gold standard for addressing security concerns.

FIGURE 10

SECURITY STRATEGIES THAT RESULT IN SIGNIFICANT IMPROVEMENTS TO CLOUD NATIVE APPLICATION SECURITY

What types of security assessments do you perform? (select all that apply) segmented by: How secure are you cloud native apps compared to 2 years ago? (select one)



2024 Cloud Native Security Survey Q17 x Q21a, Sample Size = 197, respondents who answered “On every update” or “Weekly”.

Verification of the leading cloud native security strategies

In FIGURE 9, we asked how frequently organizations employ various security strategies. FIGURE 11 employs the same list of strategies but instead asks how important each of these strategies is to the organization. Code reviews once again reside at the top of the list with 84% identifying the strategy as either extremely important or very important. Manual reviews are the gold standard when evaluating security concerns and excel at identifying business logic flaws, architectural flaws, code smells, anti-patterns, logic errors, edge cases, and verification of security tool findings.

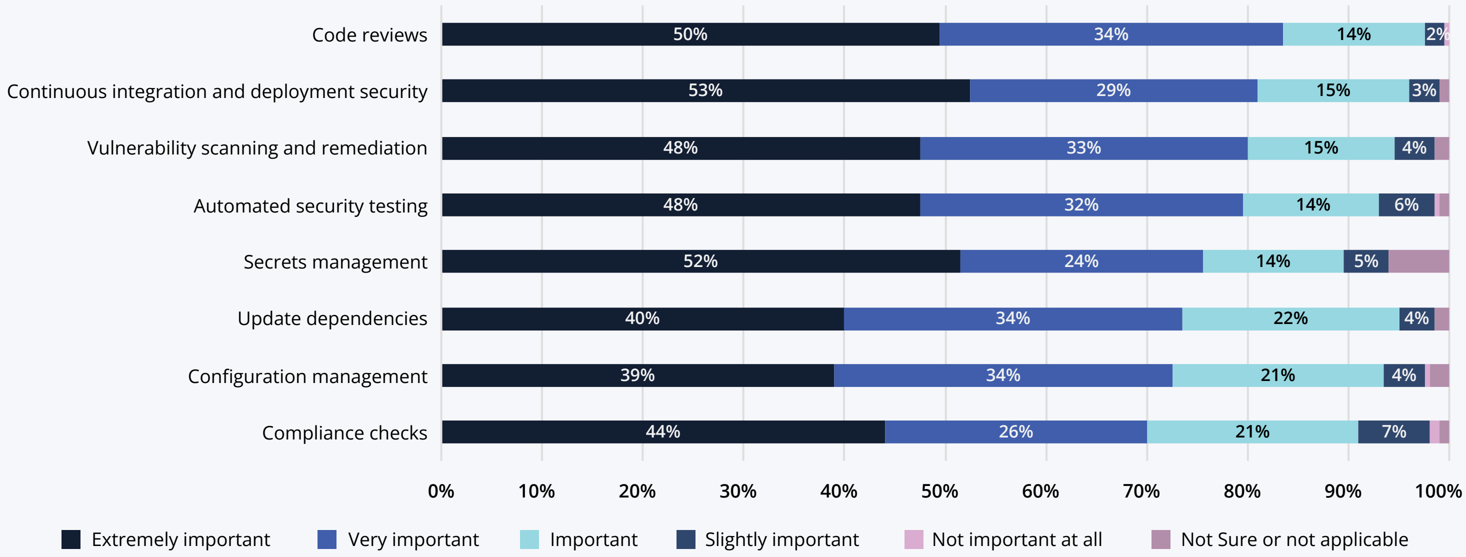
Manual code reviews can be highly effective in improving cloud native security, provided knowledgeable reviewers conduct them systematically. While automated tools like SAST and SCA play crucial roles in detecting vulnerabilities, manual code reviews offer unique advantages that complement these tools, particularly in the context of cloud native environments.

The importance of CI / CD security (82%), vulnerability scanning and remediation (81%), and automated security testing (80%) aligns with the variance findings in FIGURE 9 confirming the importance of employing these tool categories as part of an organization's security tool portfolio and tool chain.

FIGURE 11

THE IMPORTANCE OF SELECTED CLOUD NATIVE SECURITY STRATEGIES

How important are each of these security strategies? (one response per row)



2024 Cloud Native Security Survey, Q18, Sample Size = 200, sorted by percentage of respondents who selected "Extremely important" or "Very important"

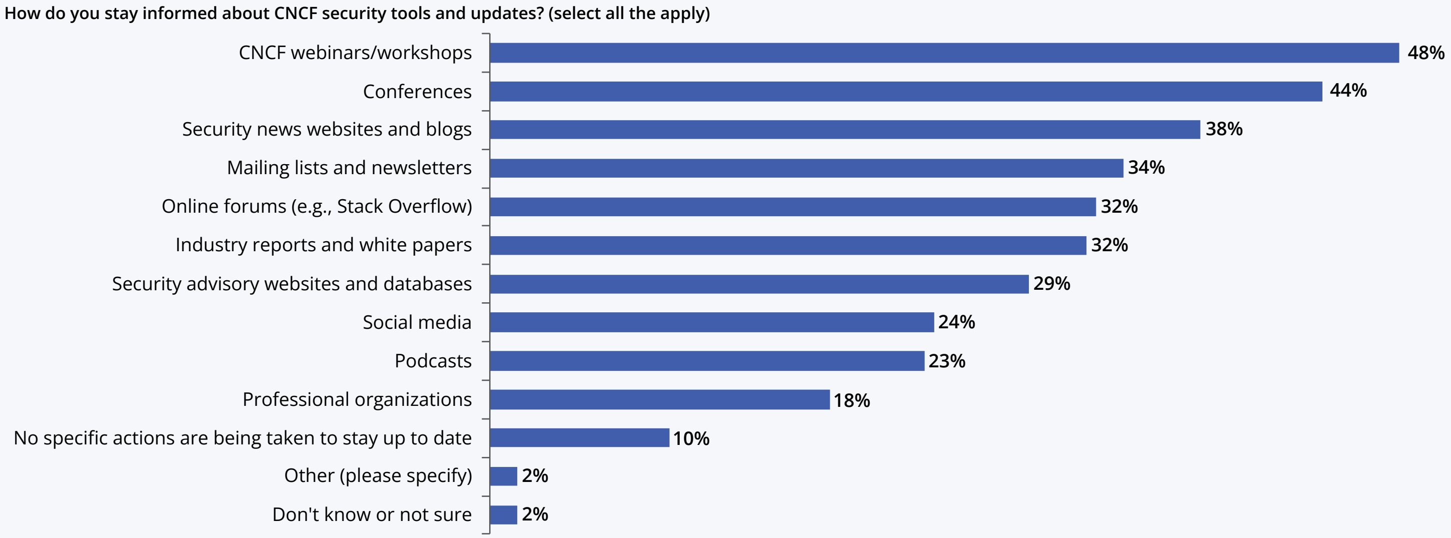
Webinars and conferences are the primary sources for staying informed about CNCF security tools and updates

The cybersecurity domain is continually changing. New vulnerabilities, threats, exploits, patches, tools, components, and best practices are always surfacing. Even if a component doesn't change, a new vulnerability can be found leading to a race between those seeking to exploit the vulnerability and those seeking to remediate it.

FIGURE 12 shows that CNCF webinars and workshops are the leading approach that 48% of respondents use for staying informed about CNCF security tools and updates. Other leading approaches to stay up to date include conferences (44%), security news websites and blogs (38%), and mailing lists and newsletters (34%). Since the majority of respondents used no single approach, is there a combination of approaches preferred by a significant majority of respondents? There is a combined use of CNCF webinars and conferences by 67% of the sample. Adding mailing lists and newsletters increases the total to 76% of the sample, adding security news websites and blogs increases the total to 82% of the sample, and adding security advisory websites and databases increases the total to 84% of the sample. We recommend that it is best to adopt a portfolio of approaches to identify important events as well as corner cases.

FIGURE 12

HOW RESPONDENTS STAY INFORMED ABOUT CLOUD NATIVE SECURITY PROJECTS, TOOLS, AND ISSUES



2024 Cloud Native Security Survey, Q44, Sample Size = 200, Valid Cases = 200, Total Mentions = 664

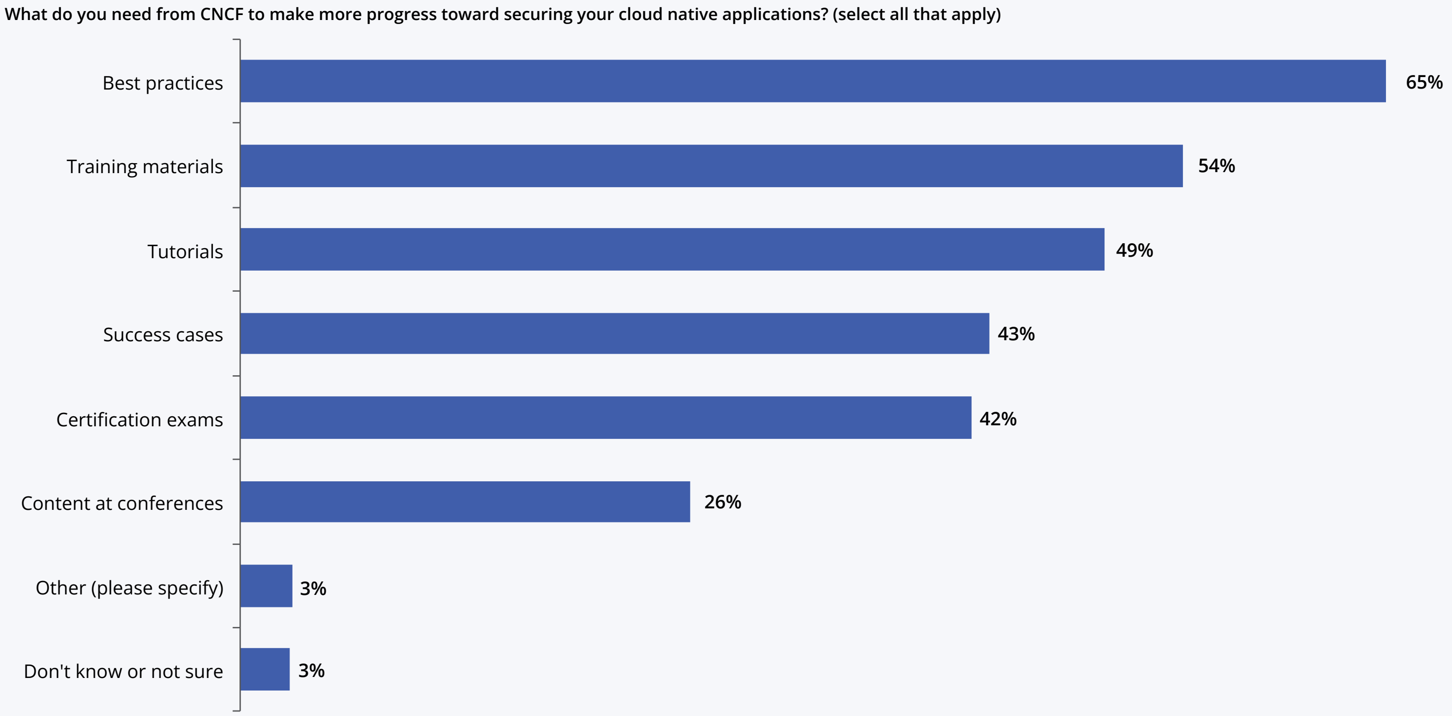
Best practices and training materials are the most desired content to improve the security of cloud native applications

FIGURE 13 shows that cloud native security best practices followed closely by training materials are the most desired content that respondents want from the CNCF. This confirms once again the findings in earlier CNCF and OpenSSF surveys.

The Linux Foundation provides a large variety of training and certification courses, tutorials, and exams focusing on secure software development, Kubernetes, service meshes, and APIs. Some of these courses are free, and others are fee-based. Most of these courses include best practices distributed across the content. Cybersecurity is a key focal point of established uber-projects including CNCF and OpenSSF. For more information see: **training.linuxfoundation.org/resources.**

FIGURE 13

PREFERRED CONTENT FROM CNCF TO SUPPORT CLOUD NATIVE APPLICATION SECURITY



2024 Cloud Native Security Survey, Q42, Sample Size = 200, Valid Cases = 200, Total Mentions = 565

Methodology

About the survey

This study is based on a web survey conducted by Linux Foundation Research and the CNCF from March 2024 through May 2024. The survey's goal was to understand how organizations are addressing cloud native security. In this section, we present the study methodology and context regarding how we analyzed the data followed by the demographics of the respondents.

From a research perspective, it was important to eliminate any perception of sample bias and ensure high data quality. We handled the elimination of sample bias by sourcing our usable sample from Linux Foundation subscribers, members, partner communities, and social media. We addressed data quality through extensive prescreening, survey screening questions, and data quality checks to ensure that respondents had sufficient professional experience to answer questions accurately on behalf of the organization they worked for.

We collected survey data from industry-specific companies, IT vendors and service providers, nonprofit, academic, and government organizations. Respondents spanned many vertical industries and companies of all sizes, and we collected data from several geographies, although primarily from North America (76%).

The 2024 Cloud Native Security Survey comprised 45 questions that addressed screening, respondent demographics, supply chain security for cloud native applications, open source security tool use, and how the CNCF can better support your needs. We have not published open source security tool use in this report, but you can find it in the dataset and survey frequencies on Data.World. For information about access to the 2024 Cloud Native Security Survey, its dataset, and survey frequencies, see the Data.World access information below.

The high-level design of the survey is outlined in FIGURE 14.

The target audience included respondents who met the following criteria:

- Must be involved in the development of cloud native applications
- Must be familiar with how the organization they work for deals with the security of its cloud native applications
- The organization must be using cloud native technologies and techniques
- Must be employed

Survey development by Linux Foundation Research occurred in March 2024, and the survey was fielded in April 2024. A total of 200 respondents completed the survey. The margin of error for this sample size was + / - 5.8% at a 90% confidence level and + / - 6.9% at a 95% confidence level.

We stratified the data collection by company size, geographic region, and organization type. The data was primarily segmented by geographic region, company size, and type of organization.

FIGURE 14

SURVEY DESIGN

Pages	Questions	Question categories	Who answers the questions
P1		Introduction	All respondents
P2	Q1 – Q7	Introductory questions	All respondents (N=200)
P3	Q8 – Q9	Tell us about yourself	All respondents (N=200)
P4	Q10 – Q11	Tell us about your involvement in open source	Open source contributors (N=153)
P5	Q12 – Q16	Tell us about the company you work for	All respondents (N=200)
P6	Q17 – Q23	Supply chain security of cloud native applications	All respondents (N=200)
P7 – 15	Q24 – Q41	Open source security tool use (nine categories)	Respondents with tool use experience (N=54 to 87)
P16	Q42 – Q45	Closing questions	All respondents (N=200)

2024 Cloud Native Security Survey

Although respondents needed to answer nearly all questions in the survey, we included a provision when a respondent was unable to answer a question by adding a “Don’t know or not sure” (DKNS) response to the list of responses for every question. However, this created a variety of analytical challenges.

One approach was to treat a DKNS just like any other response to determine the percentage of respondents that answered DKNS. The advantage of this approach is that it shows the exact distribution of data collected. The challenge with this approach is that it can distort the distribution of valid responses, i.e., responses where respondents could answer the question.

Some of the analyses in this report exclude DKNS responses. This is because we can classify the missing data as either missing at random or missing completely at random. Excluding DKNS data from a question does not change the distribution of data (counts) for the other responses, but it does change the size of the denominator used to calculate the percent of responses across the remaining responses. This has the effect of proportionally increasing the percentage values of the remaining responses. Where we have elected to exclude DKNS data, the footnote for the figure includes the phrase “DKNS responses excluded.”

The percentage values in this report may not total to exactly 100% due to rounding.

Data.World access

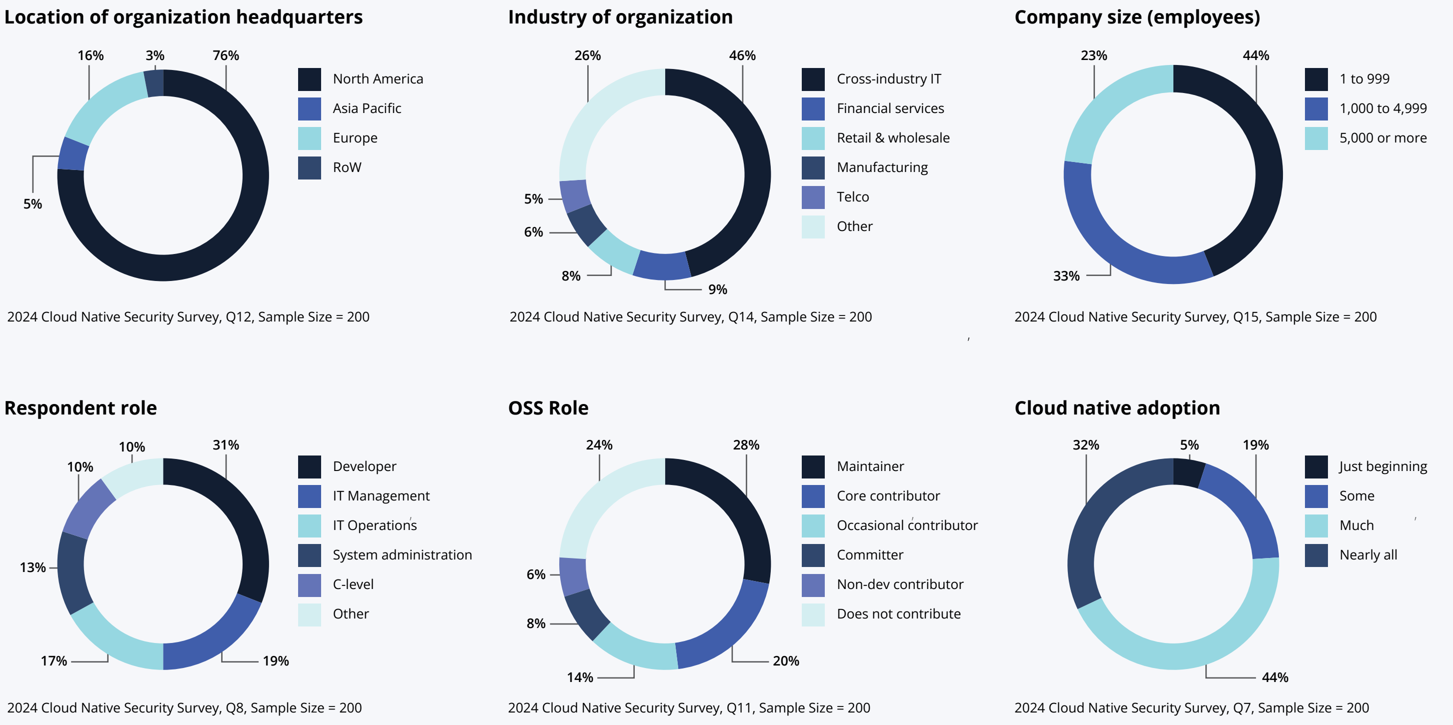
LF Research makes each of its empirical project datasets available on Data.World. Included in this dataset are the survey instrument, raw survey data, screening and filtering criteria, and frequency charts for each question in the survey. You can find LF Research datasets, including this project, at data.world/thelinuxfoundation. Access to Linux Foundation datasets is free but does require you to create a data.world account.

Respondent demographics

These demographics provide you with a profile of the 2024 Cloud Native Security Survey respondents. We have regrouped all of the demographics in FIGURE 15 to facilitate a more insightful analysis. For the original source data and study frequencies, please see the data.world access described above.

FIGURE 15

RESPONDENT DEMOGRAPHICS



Location of organization headquarters

2024 Cloud Native Security Survey, Q12, Sample Size = 200

Industry of organization

2024 Cloud Native Security Survey, Q14, Sample Size = 200

Company size (employees)

2024 Cloud Native Security Survey, Q15, Sample Size = 200

Respondent role

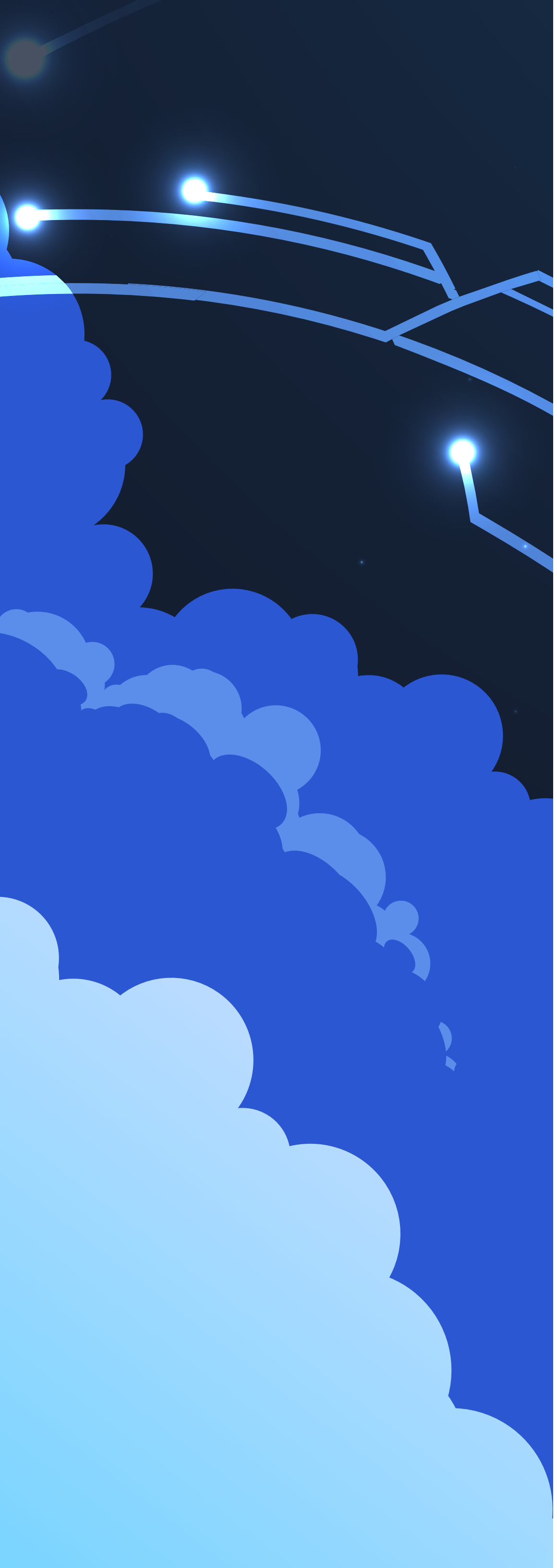
2024 Cloud Native Security Survey, Q8, Sample Size = 200

OSS Role

2024 Cloud Native Security Survey, Q11, Sample Size = 200

Cloud native adoption

2024 Cloud Native Security Survey, Q7, Sample Size = 200

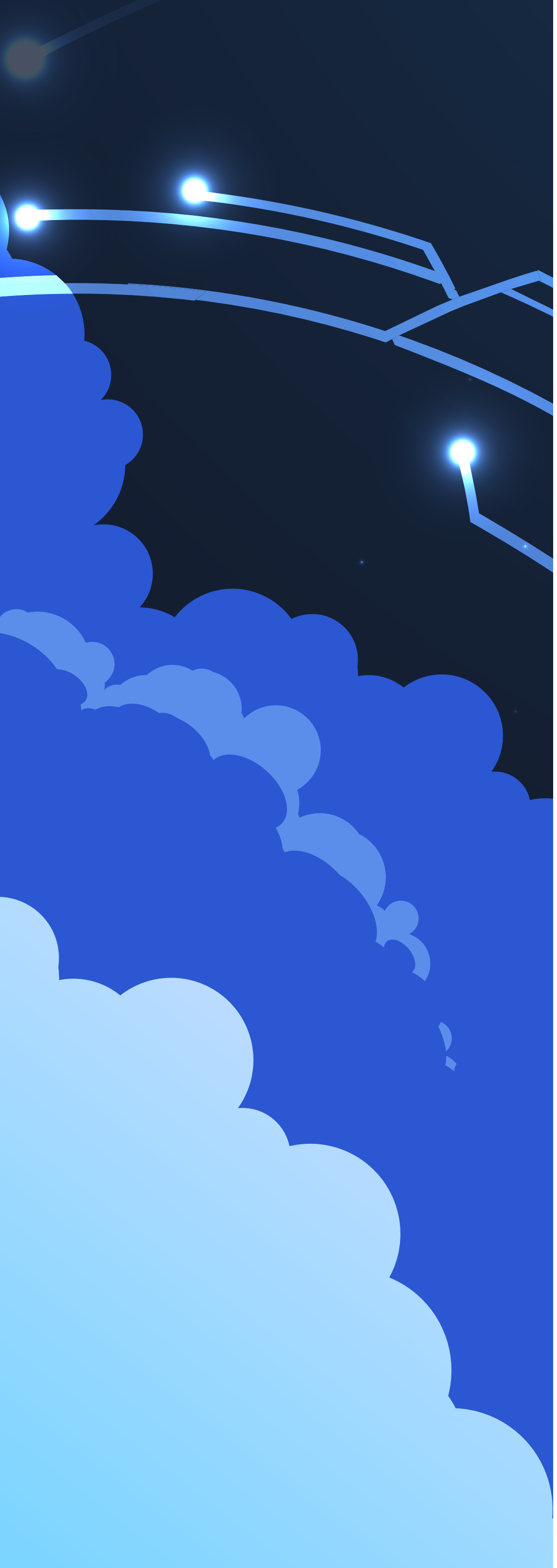


About the authors

STEPHEN HENDRICK is vice president of research at the Linux Foundation, where he is the principal investigator on a variety of research projects core to the Linux Foundation's understanding of how open source software is an engine of innovation for producers and consumers of IT. Steve specializes in primary research techniques developed over 30 years as a software industry analyst. Steve is a subject-matter expert in application development and deployment topics, including DevOps, application management, and decision analytics. Steve brings experience in a variety of quantitative and qualitative research techniques that enable deep insight into market dynamics and has pioneered research across many application development and deployment domains. Steve has authored over 1,000 publications and provided market guidance through syndicated research and custom consulting to the world's leading software vendors and high-profile start-ups.

ADRIENN LAWSON is a data analyst at the Linux Foundation. Adrienn obtained a master's degree in social data science from the University of Oxford. She is responsible for survey development, analysis, and report writing. Adrienn has previously conducted research at the University of Oxford, the Budapest Institute for Policy Analysis, and the U.K.'s Office for National Statistics. She is most fascinated by the collective power of open source collaboration within geographically dispersed communities. Additionally, she is most interested in researching trends and solutions for challenges related to OSS funding, sustainability, and supporting developers in their pursuit of responsible technological advancement.

JEFFREY SICA is Head of Projects at the CNCF, with a focus on improving maintainer experience, building communities, and project automation. Before that, he worked at Red Hat and the University of Michigan focusing on cloud native technologies and CICD patterns. Jeffrey has been a contributor to upstream Kubernetes, helping in SIG-Contribex, SIG-Release, and SIG-UI. He passionately advocates for open source development and recognizing and alleviating burnout.



Acknowledgments

We thank all the participants of the survey for kindly sharing their insights and experience in search and analytics. Special thanks to peer reviewers and LF colleagues for their involvement in the various stages of the research process, including:

- Chris Aniszczyk
- Elizabeth Bushard
- Hilary Carter
- Jorge Castro
- Mia Chaszeyka
- Anna Hermansen
- Christina Oliviero
- David Wheeler
- Katie Greenley

CLOUD NATIVE
COMPUTING FOUNDATION

Cloud native computing leverages an open-source software stack to deploy applications as microservices, where each component is packaged into its own container and orchestrated dynamically to optimize resource utilization. The Cloud Native Computing Foundation (CNCF) hosts key projects within the cloud native ecosystem, including Kubernetes, Envoy, Prometheus, and many others. CNCF serves as a neutral hub for collaboration, bringing together leading developers, end users, and vendors—from the world's largest public cloud providers and enterprise software companies to innovative startups. As part of The Linux Foundation, a nonprofit organization, CNCF fosters the growth and adoption of cloud-native technologies across industries. For more information, visit www.cncf.io.

x.com/cloudnativefdn

facebook.com/CloudNativeComputingFoundation

www.linkedin.com/cloud-native-computing

youtube.com/c/cloudnativefdn

github.com/cncf

THE LINUX FOUNDATION | Research

Founded in 2021, Linux Foundation Research explores the growing scale of open source collaboration, providing insight into emerging technology trends, best practices, and the global impact of open source projects. Through leveraging project databases and networks, and a commitment to best practices in quantitative and qualitative methodologies, Linux Foundation Research is creating the go-to library for open source insights for the benefit of organizations the world over.

x.com/linuxfoundation

facebook.com/TheLinuxFoundation

linkedin.com/company/the-linux-foundation

youtube.com/user/TheLinuxFoundation

github.com/LF-Engineering

To reference this work, please cite as follows: Stephen Hendrick, Adrienn Lawson, and Jeffrey Sica, "2024 Cloud Native Security Report: How Organizations Are Addressing Security for Cloud Native Application Development, foreword by Eddie Knight, " The Linux Foundation, October 2024.