SANS | Research Program

Survey

SANS 2024 Multicloud Survey: Securing Multiple Clouds Amid Constant Changes

Written by Kenneth G. Hartman

August 2024

Microsoft

Executive Summary

The rapid evolution of cloud services and the increasing complexity of multicloud environments present significant challenges for organizations. This survey delves into the trends and challenges faced by organizations in their multicloud journey, with a specific focus on security.

Key findings include:

- **Cloud adoption—**AWS and Azure dominate the market, with Google Cloud experiencing slower growth. However, there's a lack of visibility into cloud usage in some organizations, indicating potential shadow IT concerns.
- **Cloud storage—**Cloud storage is widely adopted and growing rapidly, with AWS and Azure leading the charge. The diverse usage patterns and fluctuations in growth highlight the dynamic nature of cloud storage demands.
- **Cloud security—**Although most organizations express confidence in their cloud security teams' skills and resources, many report gaps, especially with AWS and Azure. This underscores the need for continuous investment in training, resource allocation, and leadership education.
- **Security tools—**Organizations are actively adopting various cloud security tools, including cloud-native application protection platform (CNAPP), cloud access security broker (CASB), secure access service edge (SASE), cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), and infrastructure-as-code (IaC) scanning solutions. However, adoption rates vary, indicating opportunities for providers to increase awareness and usability.
- **Incident response—**Azure Sentinel leads in adoption, followed by AWS Detective and various third-party SIEM-as-a-service options. The underutilization of Google Chronicle and the diverse range of third-party solutions reflect the evolving nature of incident response strategies.
- **DNS security—**Although most organizations have implemented DNS security solutions, a significant portion remain unprotected or uncertain, highlighting the need for increased awareness and education.
- **Artificial intelligence—**AI is gaining traction in multicloud security, with diverse use cases emerging. Although interest is high, implementation levels vary, and organizations face challenges such as lack of expertise and concerns about effectiveness.

This survey focused on professionals in various roles (management, design/development, operations, security/compliance) who utilize multiple cloud providers in their work. The survey population is 653 multicloud users who work in a variety of roles across a variety of industries and company sizes, as indicated in Figure 1.

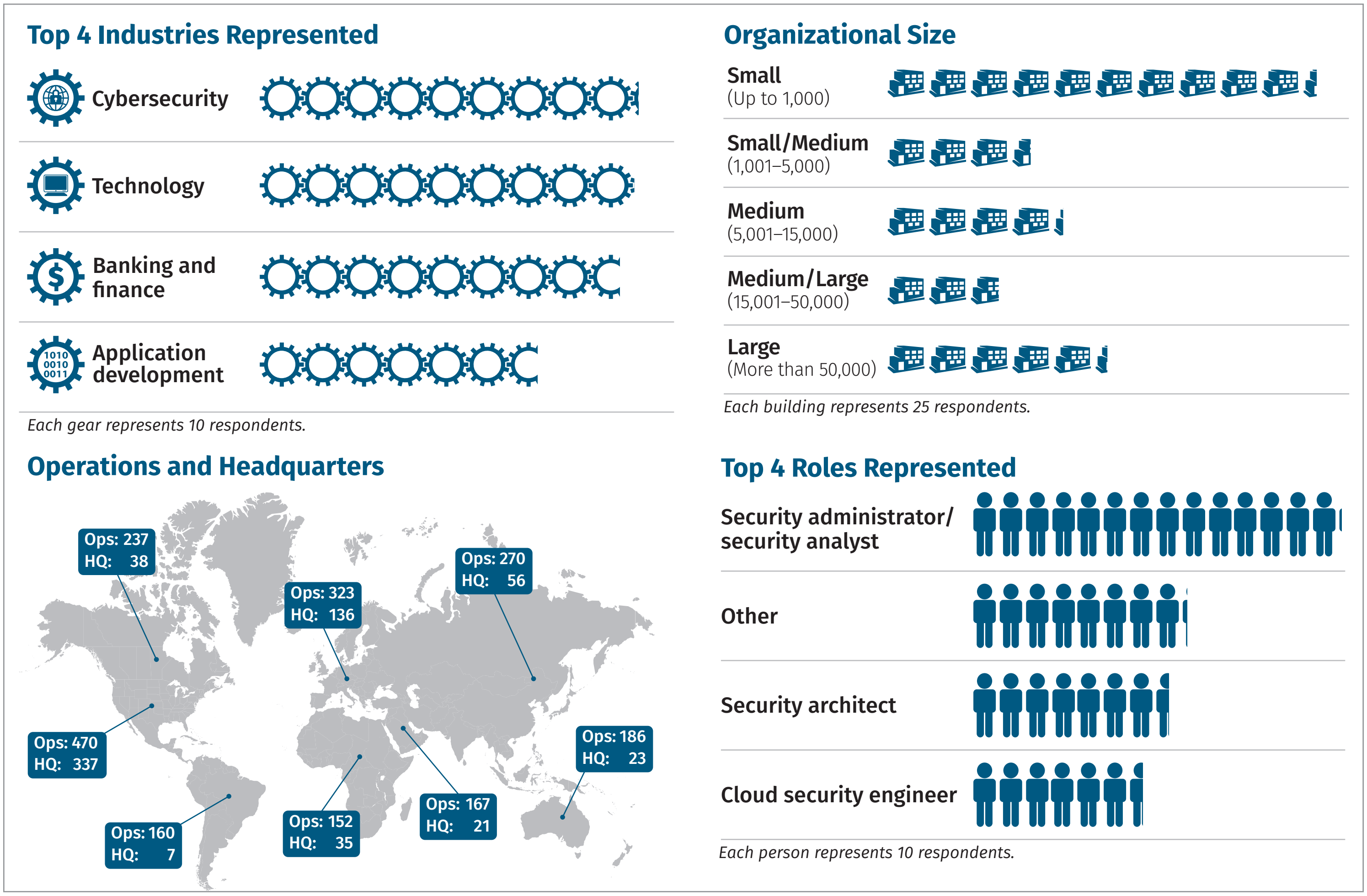


Figure 1. Survey Demographic Data

Multicloud Operations

Azure and AWS show a distinct lead in market share compared with other cloud service providers, with more than 80% of respondents indicating that their organizations use them. Google Cloud comes in at 55% of respondents. Oracle Cloud, Alibaba, and IBM are the remainder of the Top 6, coming in at 16%, 9%, and 9%, respectively. Hetzner, Huawei, and Digital Ocean were the top write-in responses. See Figure 2.

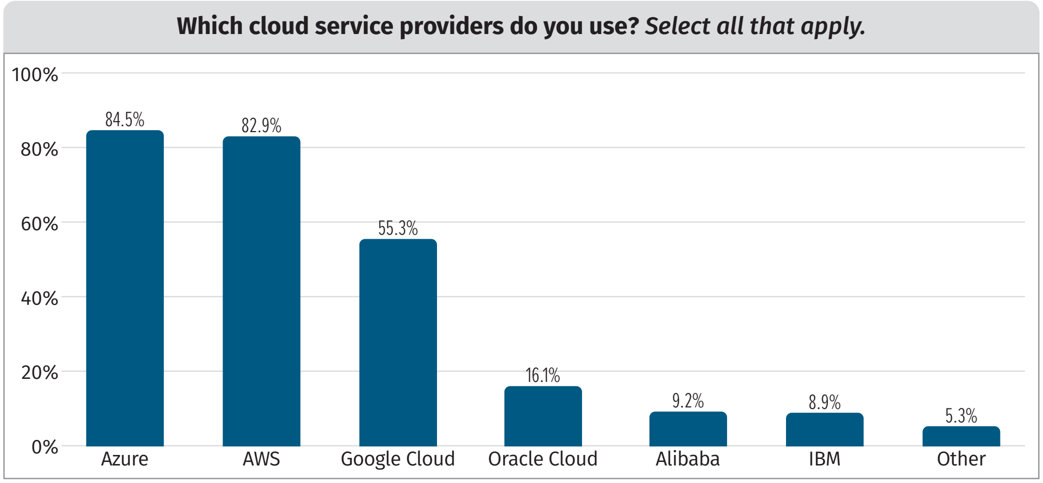


Figure 2. Cloud Service Providers Used by Survey Participants

Key Takeaway: Companies that use multiple cloud service providers are most likely to use both AWS and Azure, and a majority will use Google Cloud as well. Cloud security practitioners must be adept on all platforms that their organization uses.

Identity Federation and Single Sign-On

Managing user identities and access across a multitude of applications and cloud platforms has become a critical challenge for organizations. The proliferation of cloud services, coupled with the growing complexity of IT environments, has amplified the need for streamlined and secure authentication mechanisms.

Just over 90% of the respondents indicated that their organization uses SSO. Of that group, 44% stated that their organization uses multiple SSO providers. This was an astounding observation that we first identified during last year's survey. This year, we asked why those organizations that use multiple SSO services did so. Table 1 shows the responses. Two major factors seem to be at play: many organizations are in a state of flux, and the organizations do not utilize a single team that owns identity and access management, at least not yet.

Table 1. Reasons Organizations Use Multiple SSO Services

	Percent
We use multiple SSO services because different teams support different services.	55.2%
We use multiple SSO services because of mergers and acquisitions.	46.1%
We use multiple SSO providers, rather than a single SSO solution, because our organization lacks a central authority that is driving us toward a single solution.	23.3%
We are in transition toward a single SSO solution, but currently use more than one.	16.8%
Other	1.7%

Different departments or teams within a company may have varying preferences for SSO solutions based on their specific workflows and needs. Using multiple SSO solutions can cater to these diverse preferences and ensure a smoother user experience. Furthermore, companies often have a mix of legacy systems and applications acquired through mergers or acquisitions. These systems may be tied to specific SSO solutions that predate multicloud adoption. Replacing or integrating these legacy SSO solutions can be complex and costly, leading companies to maintain multiple SSO systems.

Key Takeaway: Using multiple SSO solutions introduces challenges in terms of complexity, maintenance, and potential user confusion. Companies need to carefully weigh the benefits and drawbacks before deciding on the most suitable approach for their multicloud environment.

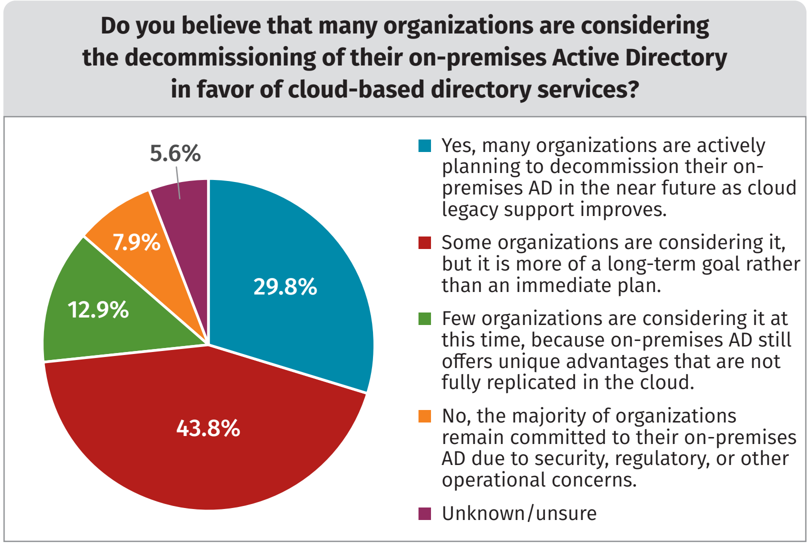


Figure 3. Perspectives on Decommissioning On-Premises Active Directory

The results illustrated in Figure 3 suggest a gradual shift toward cloud-based directory services; however, a significant portion of organizations still value the benefits of on-premises Active Directory (AD).

Workload Identity Federation

The survey results indicate that workload identity federation is gaining traction, with nearly 44% of organizations already using it. (See Figure 4.) However, there is still a significant portion (29.9%) that are either unaware of it or unsure if they are utilizing it. This suggests a potential opportunity for education and awareness-raising within organizations about workload identity federation's benefits and security advantages.

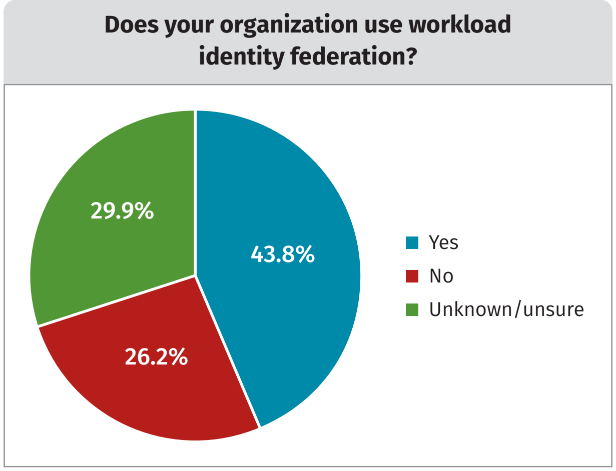


Figure 4. Use of Workload Identity Federation

Workload identity federation is gaining momentum, however, with most organizations either embracing it fully or in the process of doing so. Refer to Figure 5.

Key Takeaway: Workload identity federation is experiencing rapid adoption, but legacy systems and lack of coordination present challenges. Addressing technical debt and establishing centralized strategies are crucial for maximizing the benefits of this technology.

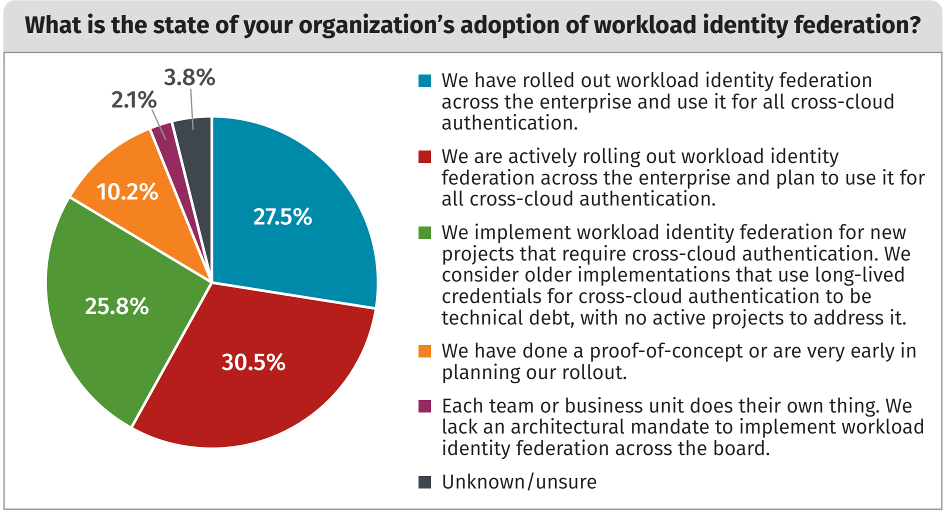


Figure 5. Adoption of Workload Identity Federation

CASB and SASE

The survey results indicate that CASB and SASE technologies are gaining significant traction in the cloud security landscape. Although some organizations have not yet adopted these solutions, a substantial group is actively evaluating or already implementing them (see Figure 6). This trend reflects the growing recognition of the need for enhanced security measures in cloud environments.

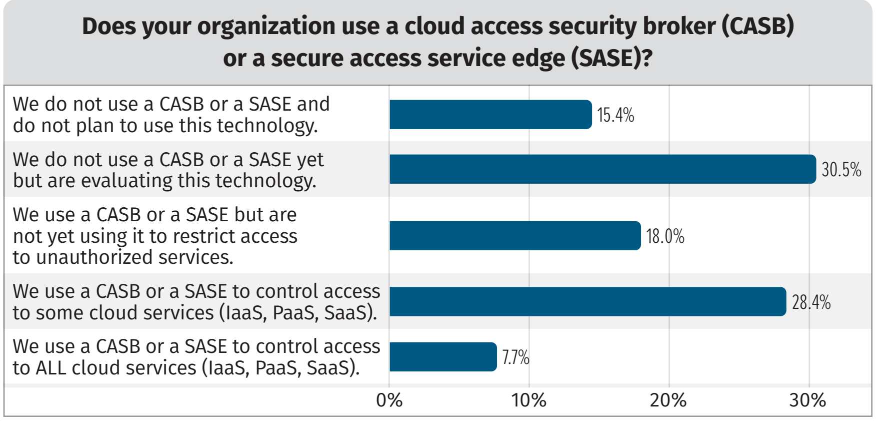


Figure 6. Use of CASB or SASE

The data also reveals that many organizations are still in the early stages of utilizing CASB/SASE capabilities. This presents an opportunity for these organizations to explore further and leverage the full potential of these solutions to enhance their cloud security posture.

Key Takeaway: CASB and SASE are emerging as vital components of cloud security strategies, with significant adoption and untapped potential for further enhancing the protection of cloud resources and data.

The most common reason for not using CASB or SASE is a *lack of awareness or understanding* of these technologies. This highlights the need for educational efforts and awareness campaigns by CASB/SASE providers to effectively communicate the value proposition of these solutions to potential customers.

The second most common reason is the perception that *current solutions are sufficient* or that there is *no immediate need* for CASB/SASE. This suggests that CASB/SASE providers need to articulate the specific benefits better and use cases where these technologies can add value beyond existing security measures.

Cost concerns also significantly influence the decision not to adopt CASB/SASE. This indicates the need for providers to offer flexible pricing models and demonstrate a clear return on investment (ROI) to justify the costs.

Technical and implementation challenges are also a barrier for some organizations. This emphasizes the importance of providing robust documentation, support, and training resources to facilitate the smooth adoption and integration of CASB/SASE.

This analysis provides valuable insights for CASB/SASE providers to address potential customers' concerns and challenges, tailor their messaging and marketing strategies, and ultimately drive greater adoption of these technologies.

Key Takeaway: Increased awareness, clearer ROI demonstration, flexible pricing models, and streamlined implementation support are crucial for the broader adoption of CASB/SASE technologies.

Cloud-Native Application Protection

The survey results in Figure 7 indicate that CNAPP is gaining traction in the cloud security landscape, with a combined 65.8% of organizations either using it or actively considering it. This suggests a growing recognition of the unique security challenges in the cloud and the need for specialized solutions to address them.

The significant portion of respondents who are "unknown/unsure" suggests a potential opportunity for CNAPP providers to increase awareness and education about their offerings. By highlighting the benefits and value proposition of CNAPP, providers can potentially tap into this untapped market and drive further adoption.

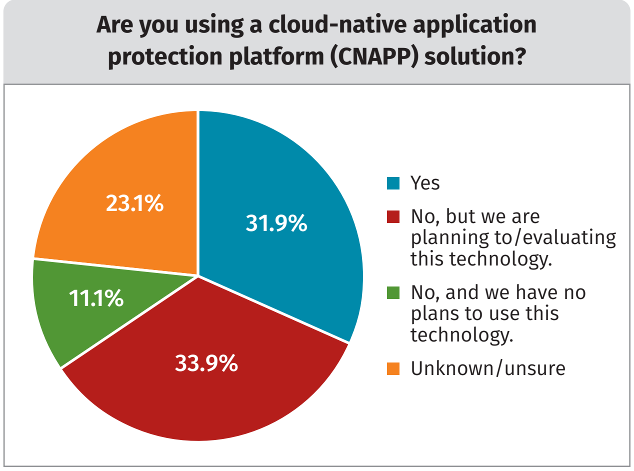


Figure 7. Adoption of CNAPP Solutions

Overall, the survey findings point toward a positive outlook for the CNAPP market. Continued growth and adoption are expected in the coming years as organizations increasingly embrace cloud-native architectures and seek to secure their applications in these dynamic environments. See Figure 8.

Key Takeaway: CNAPP adoption is gaining momentum, but most organizations are still in the early or intermediate stages of implementation. This highlights a significant growth opportunity for CNAPP providers and the need for continued support and guidance throughout the adoption process.

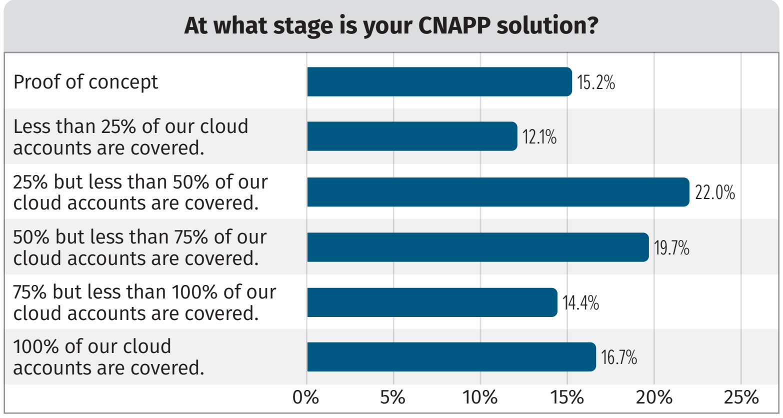


Figure 8. Adoption Stage of CNAPP Solutions

Cloud-native application protection platforms are the convergence of cloud security posture management (CSPM), cloud workload protection platforms (CWPPs), cloud infrastructure entitlement management (CIEM), and infrastructure-as-code (IaC) scanning. This has created some market confusion. An organization that may not be using a CNAPP solution may be using a CSPM solution or a CWPP solution, or both solutions but from different vendors. See Figure 9.

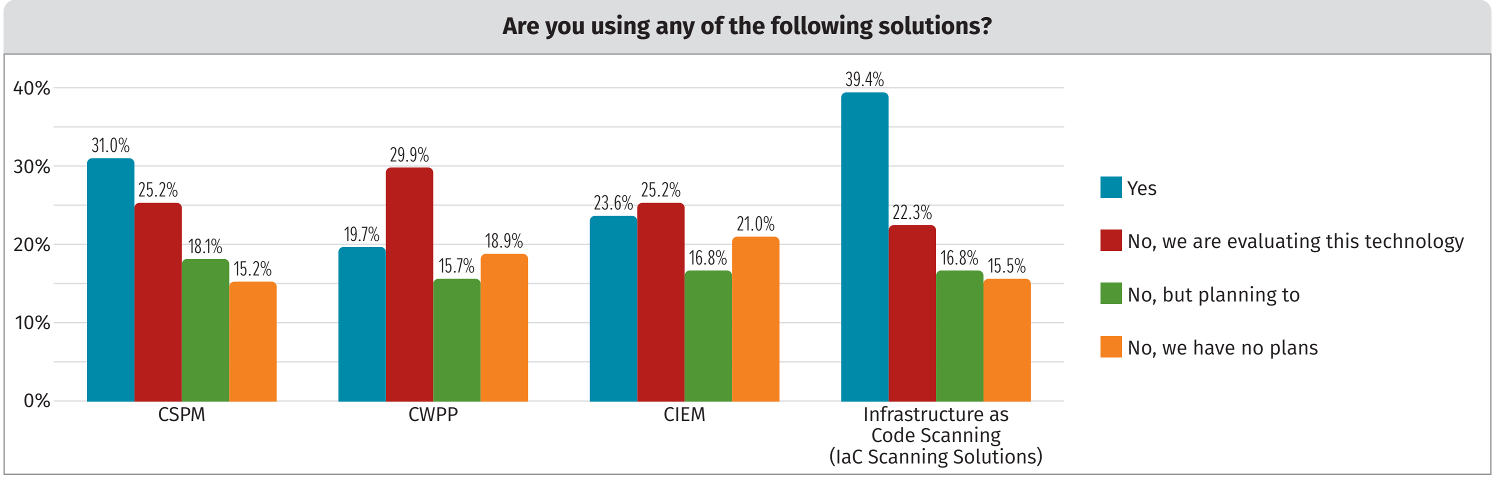


Figure 9. Usage of Various CNAPP Component Solutions

Key Takeaway: Organizations are actively adopting cloud security solutions, with IaC scanning and CSPM leading the way. The growing interest in CIEM and CWPP highlights a shift toward comprehensive, multilayered cloud security strategies.

Most organizations adopt cloud security solutions on a progressive journey. The findings illustrated in Figure 10 emphasize that cloud users start with solutions that address the most critical risks and gradually expand coverage as the organization's cloud security maturity grows.

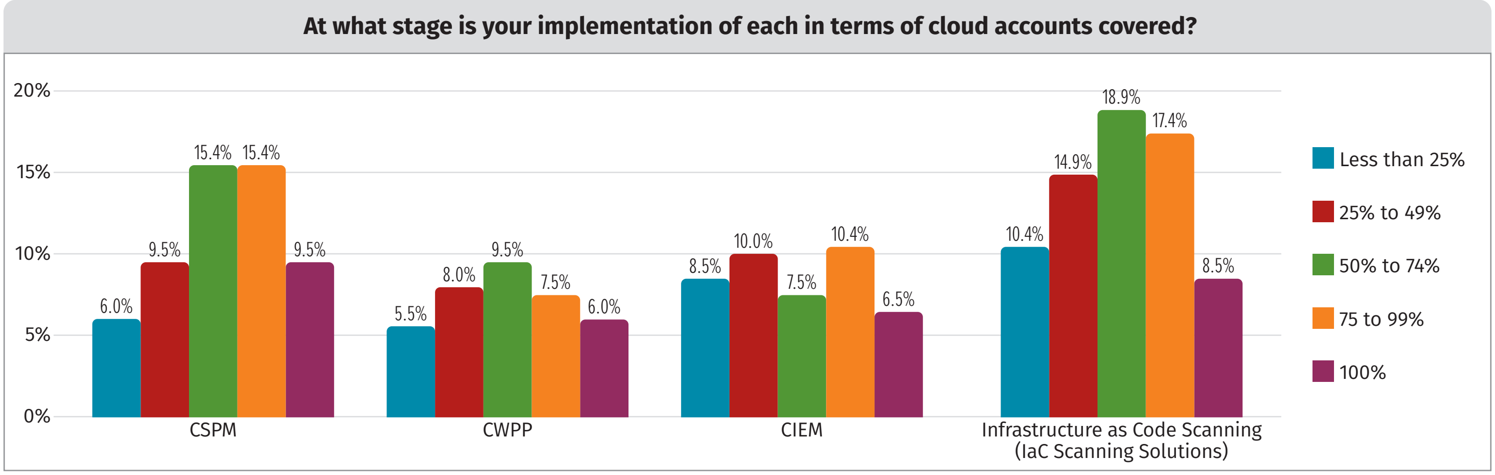

At what stage is your implementation of each in terms of cloud accounts covered?

Figure 10. The Adoption Patterns of Various CNAPP Component Solutions

Key Takeaway: Cloud security solution adoption is a phased process, with IaC scanning leading in full coverage. This highlights a strategic, risk-based approach by organizations and emphasizes the need for tailored vendor support throughout the implementation journey.

Security Information and Event Management

Cloud-hosted SIEM solutions are the dominant choice for organizations with a preference for single-vendor offerings. The rise of hybrid deployments and the persistent non-adoption by some organizations present opportunities and challenges for SIEM providers to address through tailored solutions, education, and flexible pricing models. See Figure 11.

Key Takeaway: The survey results reveal a growing preference for cloud-hosted and single-vendor solutions, along with the emergence of hybrid deployments, which indicates a shift toward more integrated and cloud-centric security strategies.

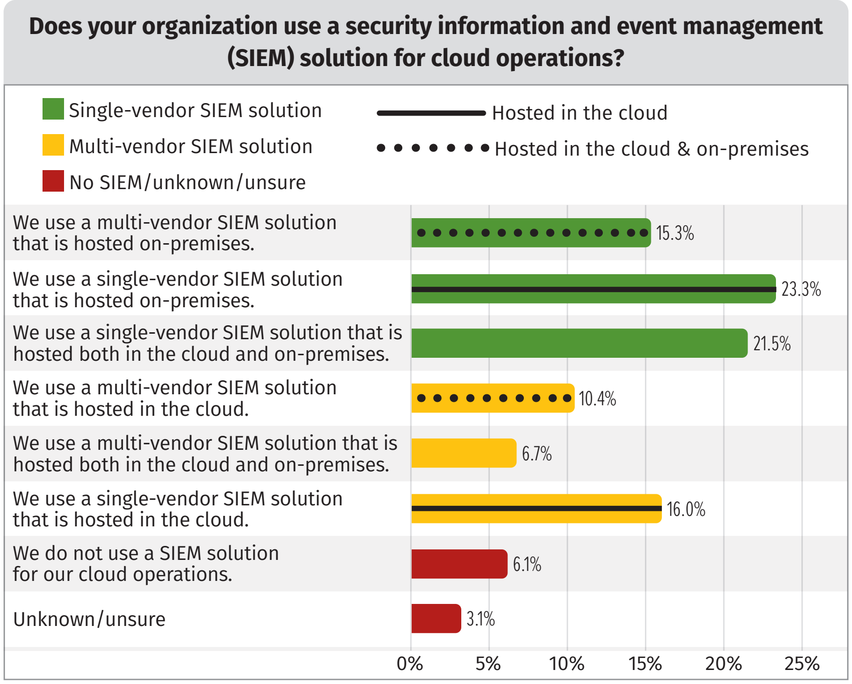

Does your organization use a security information and event management (SIEM) solution for cloud operations?

Figure 11. SIEM Deployment Models

DNS Security Solutions

The survey results in Figure 12 demonstrate that although DNS security is gaining traction in multicloud environments, there is still significant room for growth. By addressing the lack of awareness and offering solutions that meet the diverse needs of organizations, DNS security providers can unlock a vast defensive potential and help organizations strengthen their overall cloud security posture.

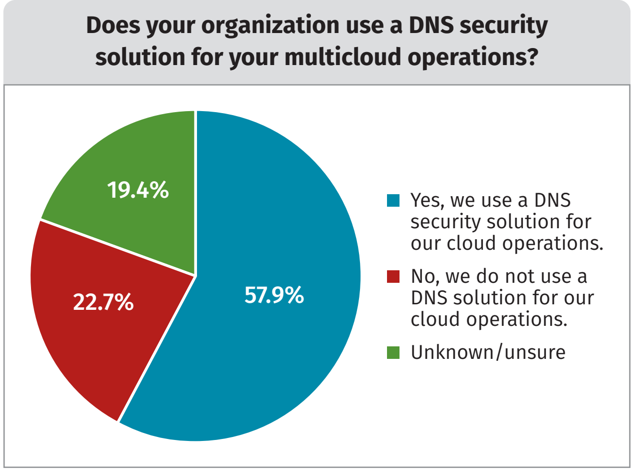


Figure 12. Adoption of DNS Security Solutions

Key Takeaway: Although the majority of organizations recognize the importance of DNS security in multicloud environments and have adopted solutions, a significant portion remains unaware or unconvinced. This presents a substantial opportunity for DNS security providers to educate potential customers and expand their market share by addressing the unique needs of different organizations.

Usage of DNS Security Solutions

The role of DNS security in safeguarding multicloud environments has become increasingly critical, prompting organizations to adopt various approaches to mitigate potential threats. Our survey data reveals diverse patterns of DNS security adoption, with a clear preference for cloud service provider solutions and a growing interest in specialized tools and add-ons. See Figure 13.

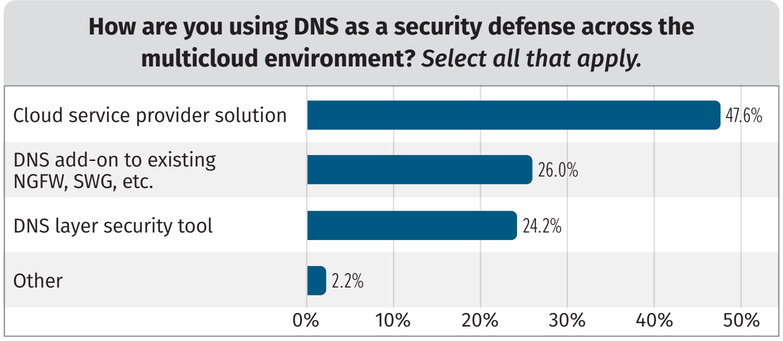


Figure 13. Usage of DNS Security Solutions

Usage of DNS for Visibility and Detection

The increasing complexity of multicloud environments has amplified the need for robust DNS security, a reality reflected in our survey findings. Although a majority of organizations acknowledge this need and have implemented DNS security solutions, a significant portion remains unprotected or uncertain about their current measures. See Figure 14.

Key Takeaway: Cloud-based DNS security solutions are favored by organizations, with many opting for either integrated offerings or specialized tools. However, a sizable portion of organizations remains unprotected, highlighting the need for increased awareness and education about the importance of DNS security.

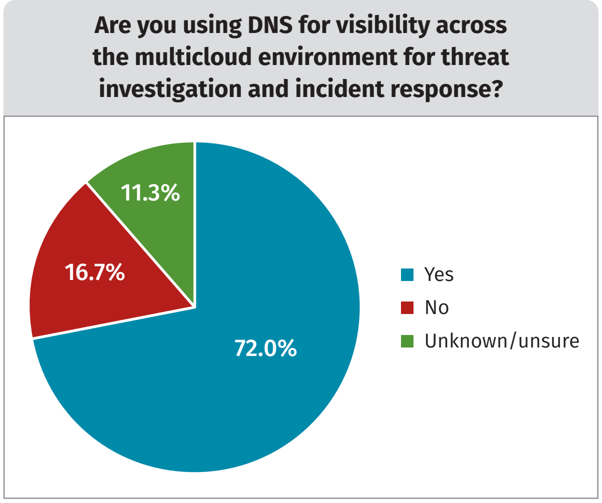


Figure 14. Usage of DNS for Visibility

How Organizations Use DNS Visibility

Organizations are actively leveraging DNS data for threat investigation and incident response in their multicloud environments. (See Figure 15.) The strong preference for SIEM integration and cloud-native solutions underscores the need for integrated and comprehensive approaches to DNS security.

Key Takeaway: Integrating DNS data with SIEM solutions is the dominant approach for gaining threat visibility in multicloud environments. Although cloud-native and add-on solutions are popular, the continued use of specialized tools highlights the need for diverse DNS security offerings to cater to various organizational needs.

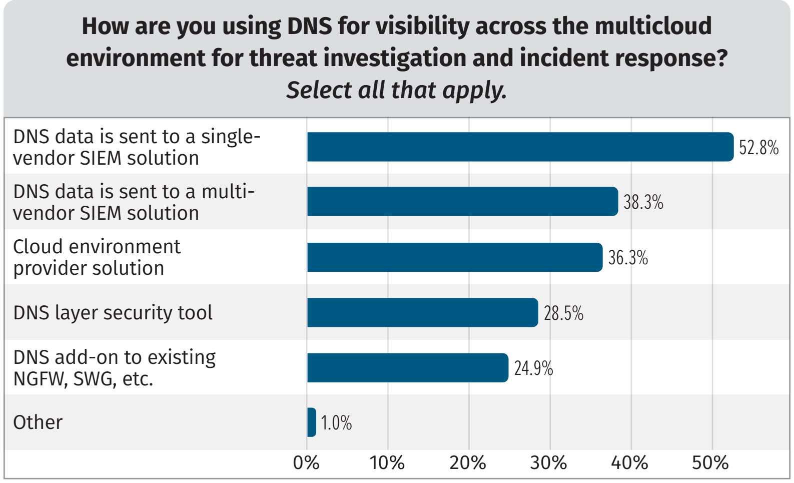


Figure 15. How Organizations Use DNS Visibility

Cloud Security Training, Resources, and Staffing

Although most organizations express confidence in their security teams' abilities and resources, a significant portion acknowledge a gap in skills, staffing, and leadership understanding, particularly among AWS and Azure users.

Cloud Security Skills and Training

The survey data indicates that most organizations using major cloud service providers (CSPs) believe their security teams have the necessary skills and training to ensure secure usage. However, a significant percentage still report lacking these capabilities, especially among AWS and Azure users. See Figure 16.

Important Note: The data reflects only the perceptions of the survey respondents and may not represent the organizations' actual security posture.

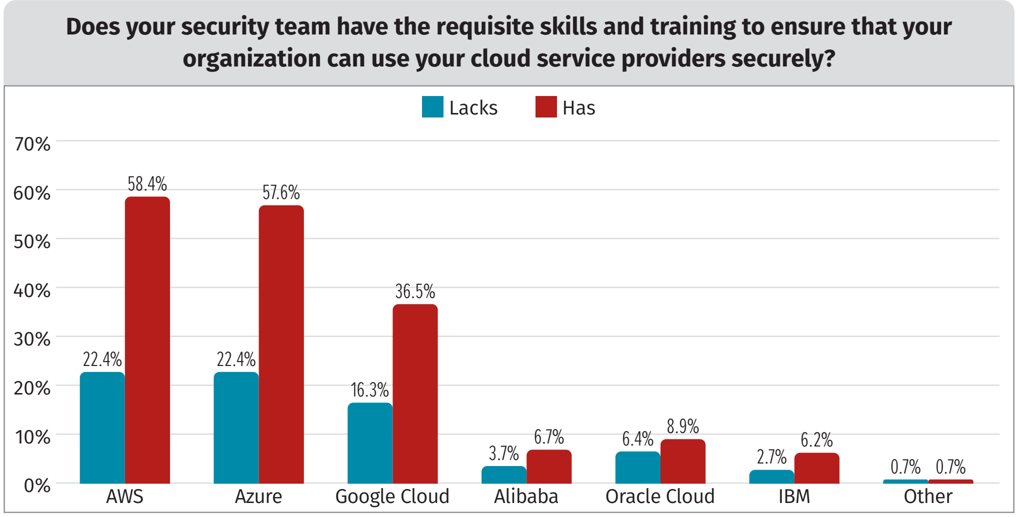


Figure 16. Perception of the Security Team's Skills and Training

Key Takeaway: Although most organizations feel confident in their cloud security team's skills, a notable gap exists. This highlights the need for continued investment in training and development to ensure security teams can effectively navigate the complexities of these cloud environments.

Cloud Security Resources and Staffing

The survey reveals a mixed perspective on cloud security resources and staffing. (See Figure 17.) Although the majority of organizations believe their teams are adequately equipped, a notable portion report lacking the necessary resources and personnel to maintain robust security measures in their cloud environments.

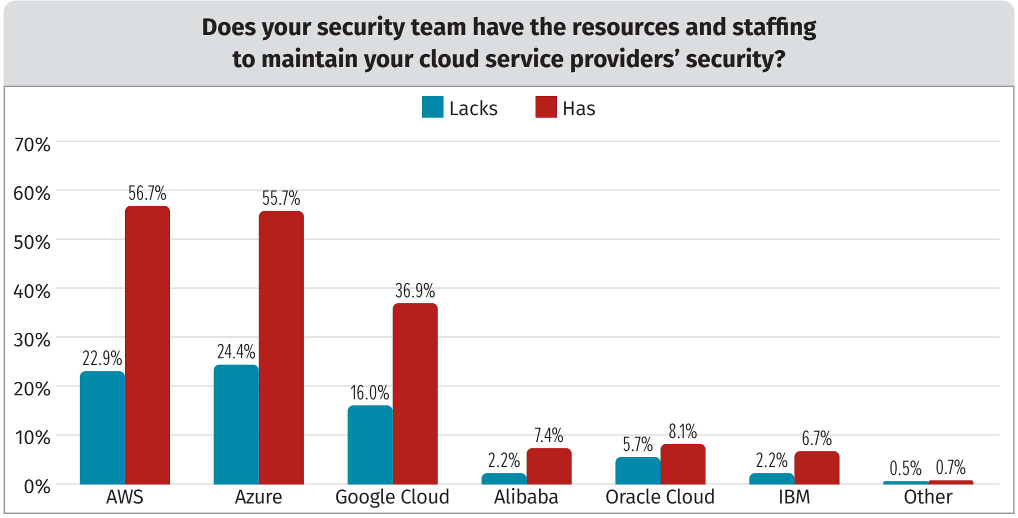
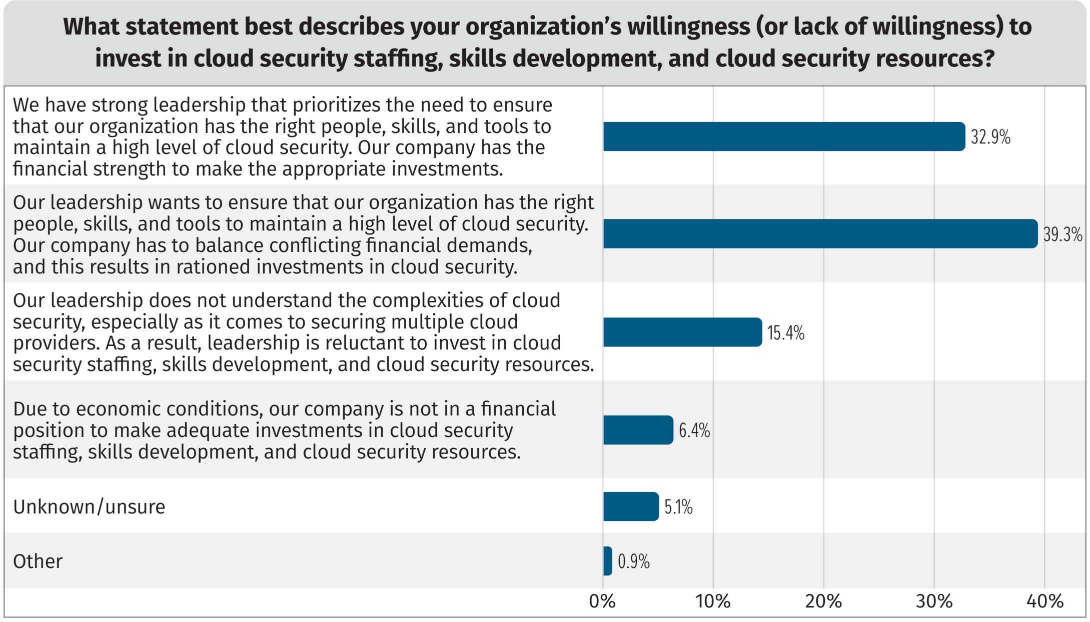

Does your security team have the resources and staffing to maintain your cloud service providers' security?

Figure 17. Perception of the Security Team's Resources and Staffing

Key Takeaway: **Despite general confidence in cloud security staffing, a significant portion of organizations report resource constraints, indicating a need for increased investment to address the growing complexities of securing cloud environments.**

Cloud Security Investment

Allocating resources for cloud security is a multifaceted challenge for organizations, often influenced by leadership priorities, financial constraints, and the evolving nature of cloud environments. Our survey reveals a variety of investment strategies, ranging from proactive prioritization to cautious rationing, and even a lack of understanding among some leadership teams. See Figure 18.


What statement best describes your organization's willingness (or lack of willingness) to invest in cloud security staffing, skills development, and cloud security resources?

We have strong leadership that prioritizes the need to ensure that our organization has the right people, skills, and tools to maintain a high level of cloud security. Our company has the financial strength to make the appropriate investments.	32.9%
Our leadership wants to ensure that our organization has the right people, skills, and tools to maintain a high level of cloud security. Our company has to balance conflicting financial demands, and this results in rationed investments in cloud security.	39.3%
Our leadership does not understand the complexities of cloud security, especially as it comes to securing multiple cloud providers. As a result, leadership is reluctant to invest in cloud security staffing, skills development, and cloud security resources.	15.4%
Due to economic conditions, our company is not in a financial position to make adequate investments in cloud security staffing, skills development, and cloud security resources.	6.4%
Unknown/unsure	5.1%
Other	0.9%

Figure 18. Perception of Cloud Security Investment

Although many organizations express confidence in their security teams, significant gaps in skills and resources persist. To address these challenges, organizations must invest in continuous learning, robust governance frameworks, and a combination of cloud-native and third-party solutions to ensure comprehensive security in their multicloud environments.

Key Takeaway: **Cloud security investment is a balancing act between competing priorities and resource constraints. Organizations must prioritize leadership education, financial planning, skills development, and comprehensive governance frameworks to secure their cloud environments effectively.**

Cloud Scale

The rapid expansion of cloud computing has led to a surge in both the adoption of cloud services and the volume of data stored within them. This section explores the current state of cloud scale, delving into the adoption trends of major cloud providers and the utilization patterns of their storage offerings.

Growth in Cloud Accounts

The data displayed in Figures 19, 20, and 21 demonstrate a clear trend of increasing cloud adoption across all three major providers (AWS, Azure, and Google Cloud) over the past three years.

Eleven percent of the respondents indicated that they have more than 1,000 AWS accounts and more than 1,000 Azure subscriptions, while 8% indicated that they have over 1,000 Google projects.

Key Takeaway: Based on the number of accounts, cloud adoption is accelerating, with AWS and Azure leading the charge. Although Google Cloud also shows growth, its pace lags behind its competitors. Notably, a lack of visibility into cloud usage persists within some organizations, indicating a need for greater transparency and governance.

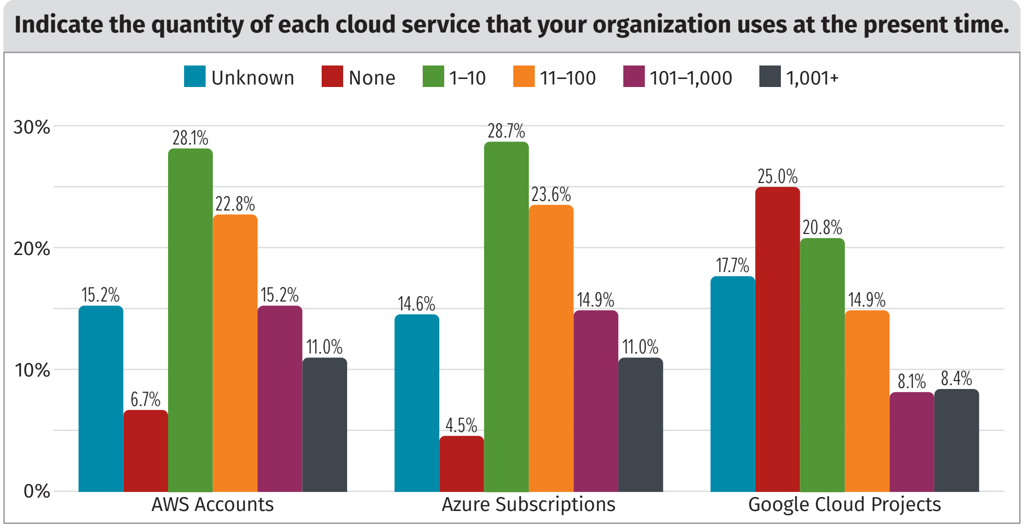


Figure 19. Quantity of AWS Accounts, Azure Subscriptions, and Google Cloud Projects at Present

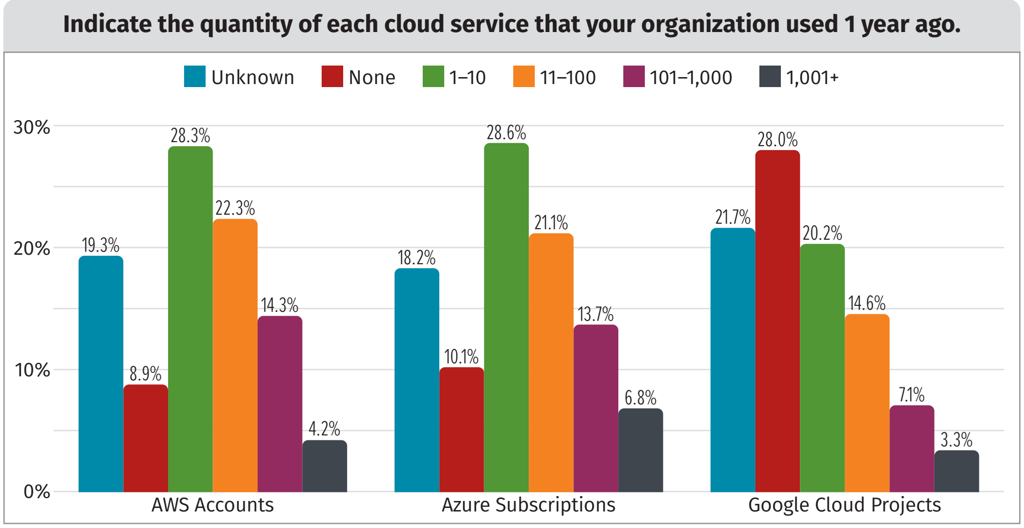


Figure 20. Quantity of AWS Accounts, Azure Subscriptions, and Google Cloud Projects—1 Year Ago

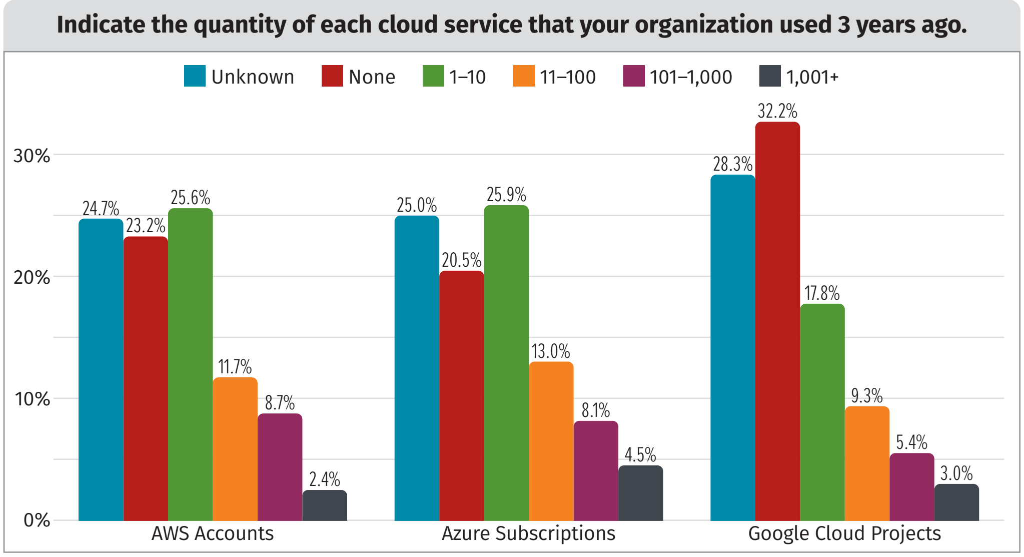


Figure 21. Quantity of AWS Accounts, Azure Subscriptions, and Google Cloud Projects—3 Years Ago

Growth in Cloud Storage Containers

The data indicates a significant usage of buckets and storage containers across all three major cloud providers (AWS, Azure, and Google Cloud), with a notable growth trend in the past three years. See Figures 22 and 23.

Key Takeaway: Cloud storage container usage is widespread and growing across all major providers, with AWS and Azure leading the market. Although most organizations are increasing their cloud storage footprint, some are optimizing their usage, as evidenced by a reported decrease in Google Cloud bucket usage for certain organizations.

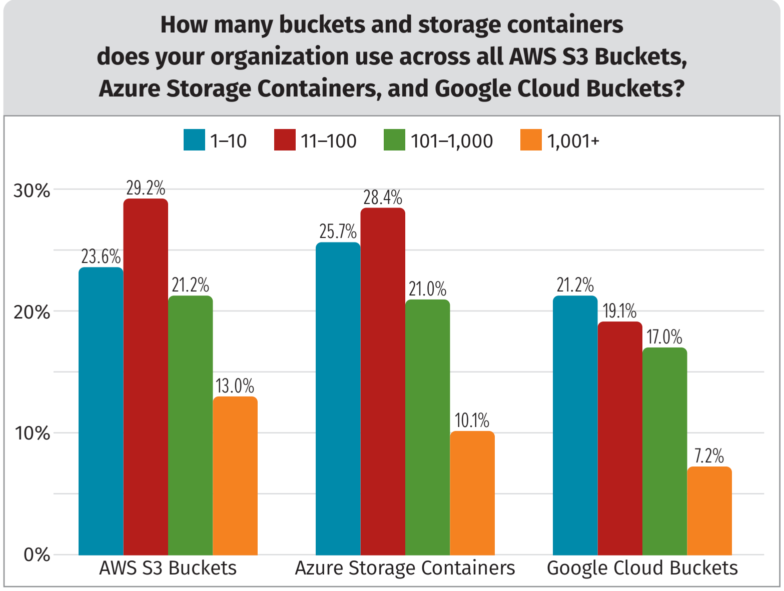


Figure 22. Quantity of AWS S3 Buckets, Azure Storage Containers, and Google Cloud Buckets

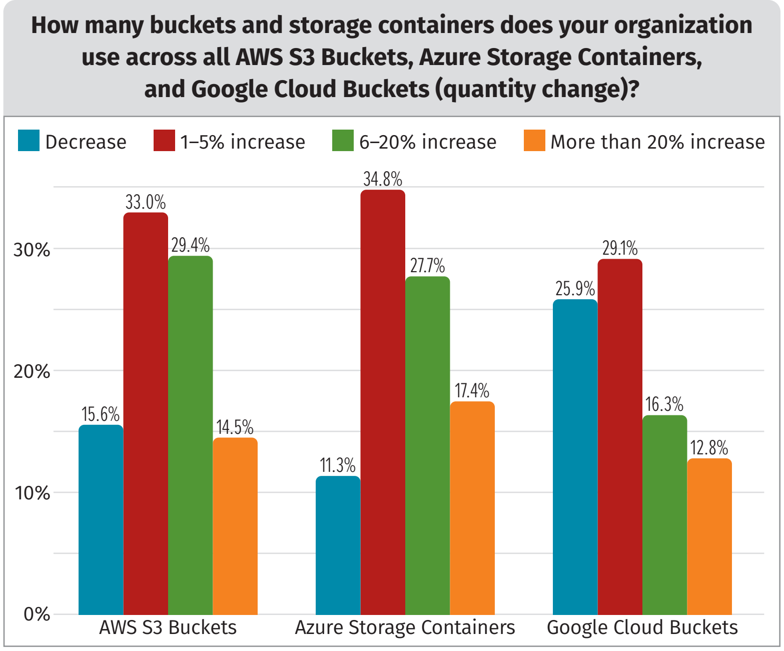


Figure 23. Change in the Quantity of AWS S3 Buckets, Azure Storage Containers, and Google Cloud Buckets in Past 3 Years

Growth in Cloud Storage Volume

The data paints a picture of widespread data storage across AWS, Azure, and Google Cloud, with varying degrees of growth over the past three years. See Figures 24 and 25.

Key Takeaway: Cloud storage volume is experiencing significant growth across the major providers. Although data volumes continue to rise for most, the diverse distribution of storage sizes and the fluctuations in usage demonstrate the dynamic and evolving nature of cloud storage demands.

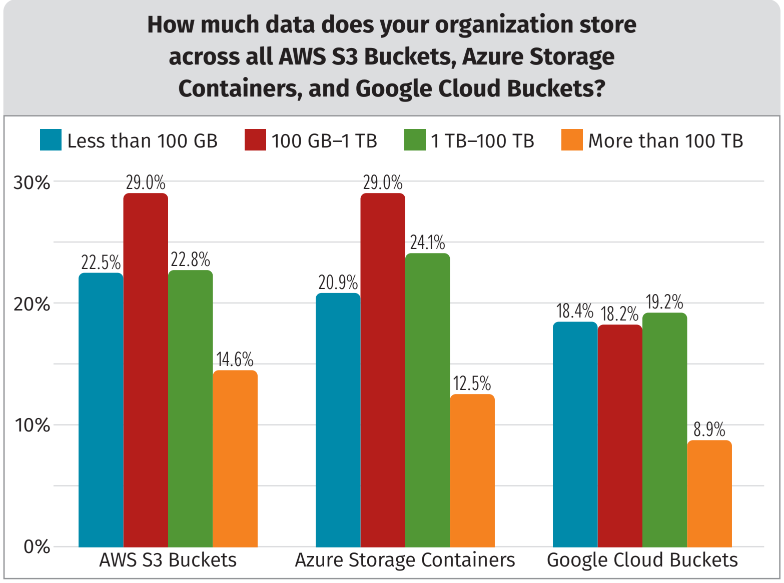

How much data does your organization store across all AWS S3 Buckets, Azure Storage Containers, and Google Cloud Buckets?

Figure 24. Volume of Data Stored in AWS S3 Buckets, Azure Storage Containers, and Google Cloud Buckets

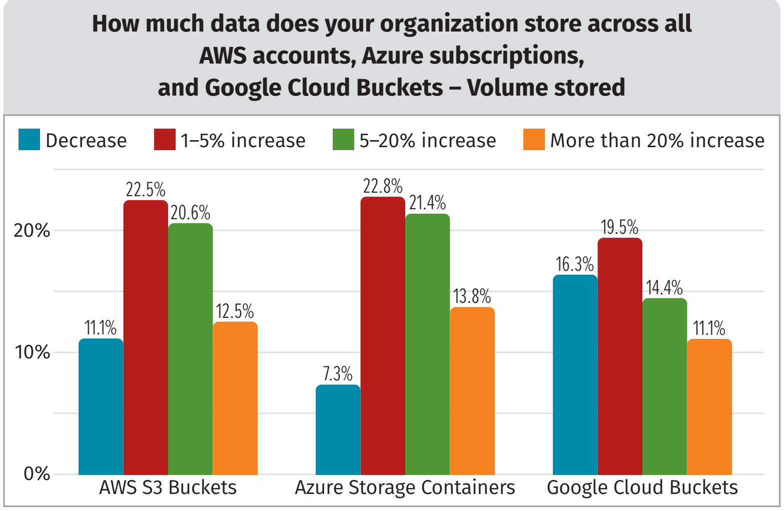

How much data does your organization store across all AWS accounts, Azure subscriptions, and Google Cloud Buckets – Volume stored

Figure 25. Change in the Volume of Data Stored in AWS S3 Buckets, Azure Storage Containers, and Google Cloud Buckets in the Past 3 Years

Artificial Intelligence

Artificial intelligence (AI) is set to transform multicloud security. Our survey explored how organizations are using or planning to use AI in this area, finding varied adoption levels, diverse applications, and mixed feelings.

Key findings:

- **Widespread interest but varying implementation—**Organizations show strong interest in using AI for multicloud security, but actual implementation varies. Some actively use AI tools, whereas others are still exploring or planning.
- **Diverse applications—**AI is being explored for threat detection (anomaly detection, malware analysis), security automation (incident response, vulnerability scanning), compliance (automated checks, policy enforcement), and more (log analysis, code generation).
- **Challenges and concerns—**Challenges include a lack of expertise, privacy and data security concerns, uncertainty about AI's effectiveness, and job displacement fears.

As AI technology develops, its use in multicloud security will likely increase. Organizations effectively leveraging AI will be better equipped to protect their cloud environments.

Key Takeaway: AI adoption for multicloud security is on the rise, with diverse use cases emerging. Although interest is high, implementation levels vary, and organizations face challenges such as lack of expertise and concerns about effectiveness. As AI matures, those who successfully leverage it will gain a significant advantage in securing their cloud environments.

Conclusion

The multicloud landscape is complex and dynamic, presenting both opportunities and challenges for organizations. Although cloud adoption is accelerating and security tools are evolving, organizations must actively address skill gaps, resource constraints, and leadership awareness to ensure the security of their cloud environments. By investing in education, adopting comprehensive governance frameworks, and leveraging a combination of cloud-native and third-party solutions, organizations can navigate this evolving space and build a robust and resilient cloud security posture.

The SANS Multicloud Survey findings highlight the importance of staying abreast of the latest trends and technologies in the multicloud space. As the cloud continues to evolve, so must organizations' security strategies. By proactively addressing the challenges and embracing the opportunities presented by multicloud environments, organizations can unlock the full potential of the cloud while safeguarding their critical assets and data.

Appendix

This section contains market data based on questions asked in the SANS 2024 Multicloud Survey and a follow-up "flash survey" that was performed to resolve some data discrepancies. Only respondents who provided their contact information in the first survey were asked to participate in the flash survey. Be advised that the data in this section is biased, because it only includes organizations that use multiple cloud providers. These charts are intended only to provide a high-level overview of the options that are available to multicloud customers. The companies listed in each software product category were identified using internet searches at the time the questions were written for the SANS 2024 Multicloud Survey. Therefore, rebranded and existing products that are only recently starting to be positioned in a software product category may be under-represented.

Single Sign-On (SSO) is an authentication method that allows users to access multiple applications or resources with a single set of credentials, eliminating the need to log in to each one individually. See Figure A1.

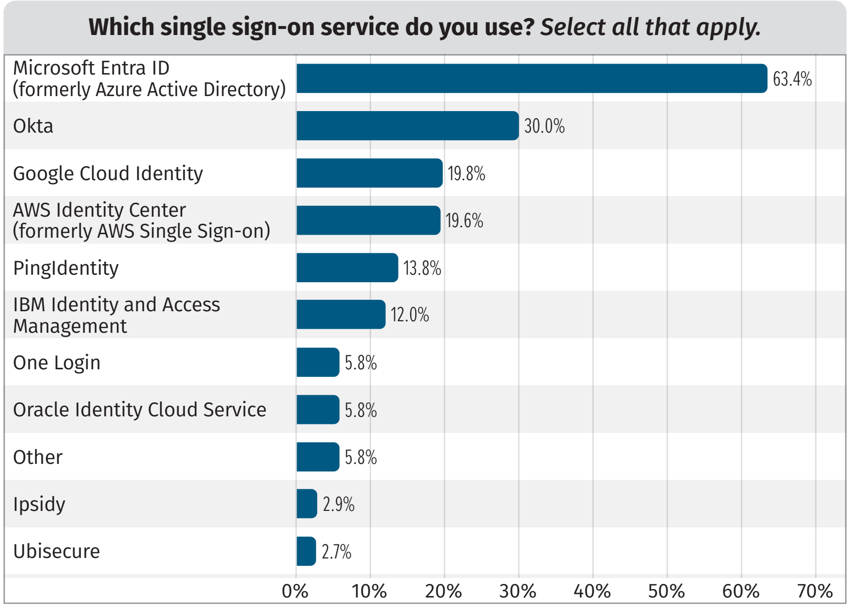


Figure A1. SSO Services Being Used

Cloud-Native Application Protection Platform (CNAPP) is a unified security solution designed to protect cloud-native applications throughout their entire lifecycle, from development to deployment and runtime, by combining multiple security capabilities such as CSPM, CWPP, CIEM, and IaC scanning into a single platform. See Figure A2.

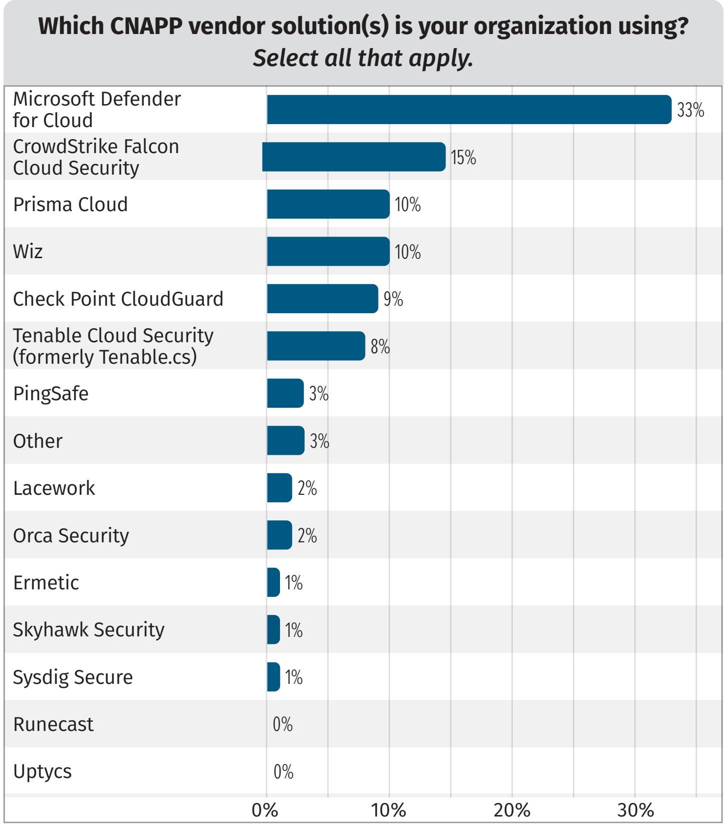


Figure A2. Usage of Various CNAPP Solutions

Cloud Security Posture Management (CSPM) is a security practice that focuses on identifying and remediating misconfigurations, vulnerabilities, and compliance risks within cloud environments, often leveraging automation to continuously monitor and enforce security policies across various cloud services and resources. Note: Vendors that offer CNAPP will typically offer CSPM capabilities and are not necessarily listed in this chart. See Figure A3.

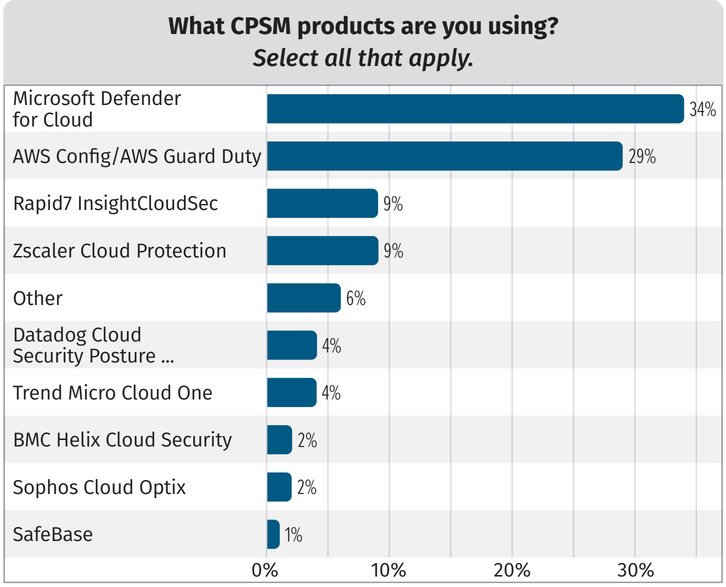


Figure A3. CSPM Product Usage

Cloud Workload Protection Platform (CWPP) is a security solution that protects workloads across various cloud environments (e.g., VMs, containers, serverless) by offering capabilities such as vulnerability management, threat detection, and runtime protection. Note: Vendors that offer CNAPP will typically offer CWPP capabilities and are not necessarily listed. See Figure A4.

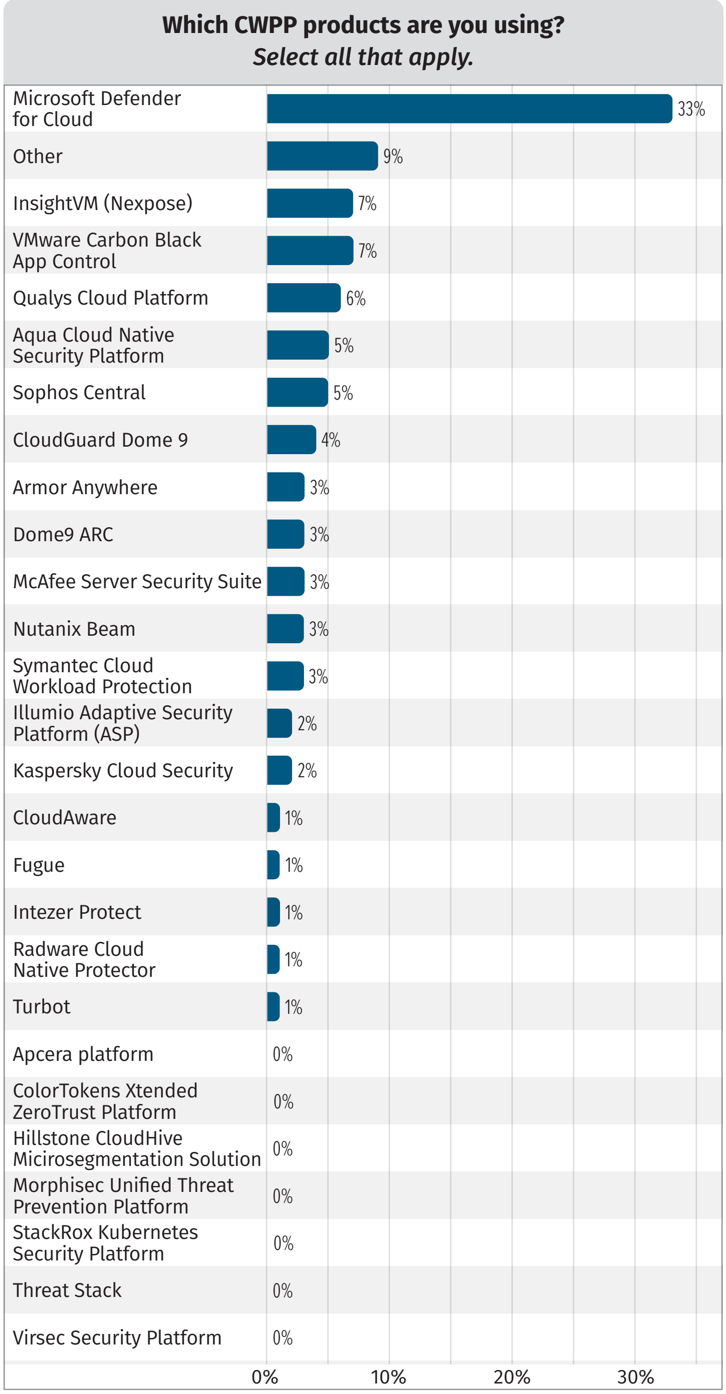


Figure A4. CWPP Product Usage

Cloud Infrastructure Entitlement Management (CIEM) is a security solution that helps manage and control access rights to cloud resources by providing visibility into entitlements, automating entitlement management, and enforcing least privilege principles across multicloud environments. Note: Vendors that offer CNAPP may offer CIEM capabilities and are not necessarily listed. See Figure A5.

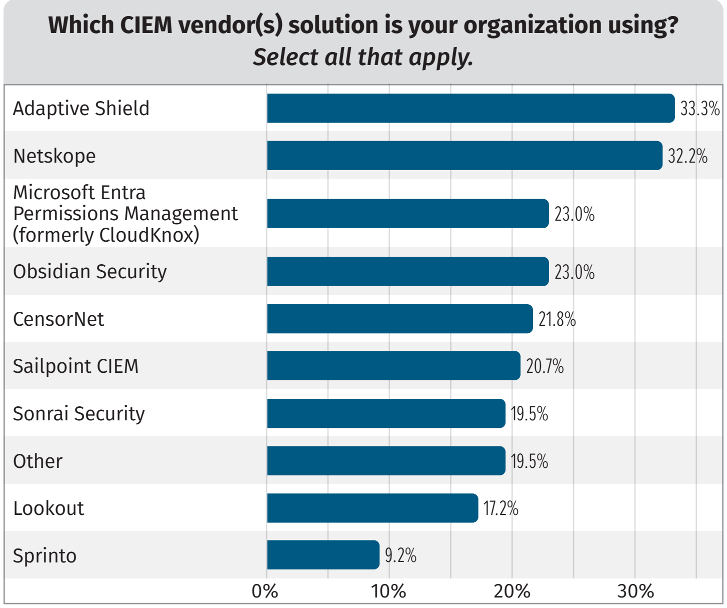


Figure A5. CIEM Product Usage

IaC Scanning is the automated process of analyzing Infrastructure as Code (IaC) templates and configurations to identify security vulnerabilities, misconfigurations, and compliance violations before they are deployed, helping organizations proactively secure their cloud infrastructure. Note: Vendors that offer CNAPP may offer IaC Scanning capabilities and are not necessarily listed. See Figure A6.

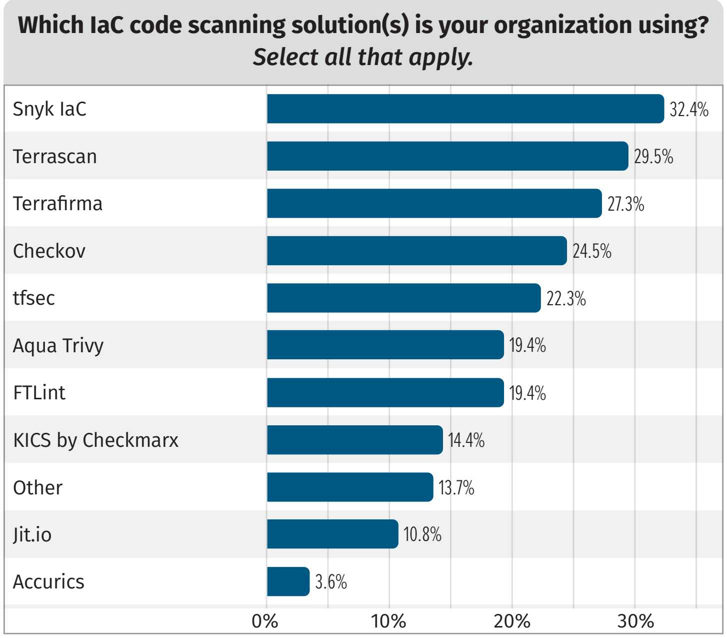


Figure A6. IaC Scanning Product Usage [1]

[1] Accurics, Inc. was acquired by Tenable in 2021.

Sponsor

SANS would like to thank this paper's sponsor:

Microsoft