Cybersecurity
INSIDERS

2024

Cloud Security Report

ISC2™

Introduction

In an era where cloud computing has become the backbone of IT infrastructure, cybersecurity professionals and organizations face a continuously evolving threat landscape. These challenges are diverse, encompassing everything from securing multi-cloud environments and ensuring data protection to mitigating cloud-specific vulnerabilities. But they also highlight a pronounced skills gap in the cybersecurity workforce. As the complexity of cloud ecosystems expands, so does the need for advanced, cloud-centric cybersecurity strategies and skills.

Against this backdrop, the 2024 Cloud Security Report, developed in partnership with ISC2 — a cybersecurity training and certification leader — provides an in-depth analysis of current cloud security trends, challenges, and organizational responses.

Key findings include:

- **Cloud Concerns:** 96% of organizations express apprehension about public cloud security, a clear indicator of the pervasive concern over cloud vulnerabilities.
- **Multi-Cloud Challenges:** Securing multi-cloud environments is identified as a primary challenge by 55% of respondents, emphasizing the critical need for skills in data protection and seamless cloud integration.
- **Simplification Strategy:** The survey underscores the need to reduce security solution complexity, with 69% of organizations depending on three or more separate security solutions to manage their cloud security.
- **Barriers to Adoption:** Key obstacles in cloud security adoption include budget constraints (48%), a lack of skilled staff (45%), and data privacy concerns (40%), highlighting the indispensable role of targeted training and certification.
- **Skills Gap:** The report underscores a significant cybersecurity skills gap, with 93% of participants concerned about the shortage of qualified professionals in the field.

We sincerely thank ISC2 for their support and partnership in this important research. Their dedication to fostering a highly skilled cybersecurity workforce through top-tier training and certification programs is crucial in addressing the sophisticated security challenges presented by modern cloud computing.

We hope that the insights and data presented in this report will prove valuable to cybersecurity professionals as you strive to protect your cloud environments against evolving threats.

Thank you,

Holger Schulze

Founder, Cybersecurity Insiders

Cybersecurity INSIDERS

Cloud Security Concerns

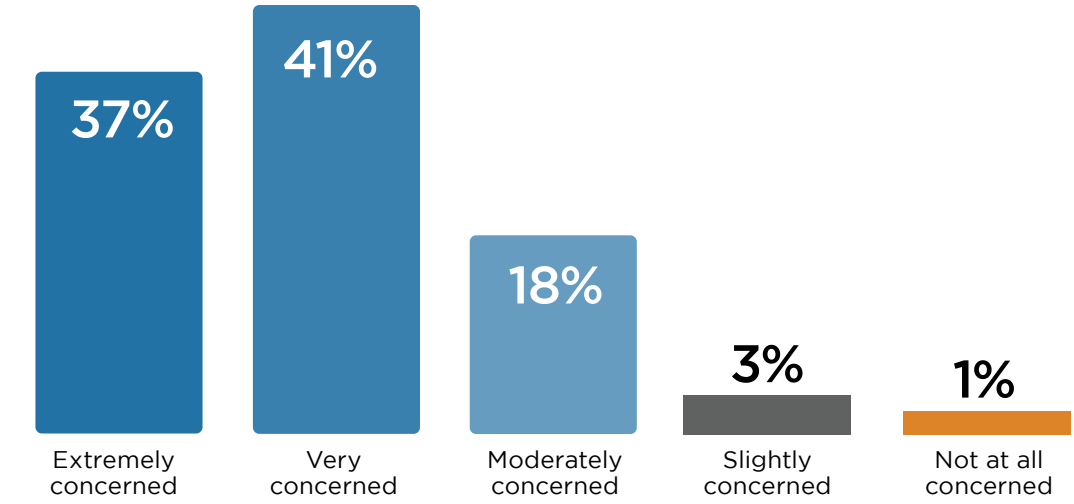
The prevailing concern among IT and cybersecurity professionals regarding cloud security highlights the significant vulnerabilities inherent in today's digital operations. Our survey reveals a notable 96% of respondents express significant concern for security within public clouds, a slight increase from 95% in 2023. This near-universal apprehension reflects an acute awareness of the complex threats facing cloud infrastructures.

In response, it's imperative for organizations to adopt advanced security measures and comprehensive risk management strategies. Prioritizing the deployment of innovative security technologies and enhancing monitoring capabilities are essential steps to fortify defenses against the nuanced challenges of public cloud ecosystems.

How concerned are you about the security of public clouds?

96%

of organizations are moderately to extremely concerned about cloud security



This sustained focus underscores the importance of continuous education in cloud security and the development of adaptive solutions capable of responding to the rapidly changing dynamics of multi-cloud environments and associated threats. Therefore, organizations must elevate cloud security as a strategic imperative, investing in robust protection mechanisms and ongoing training to ensure the integrity of their cloud operations.

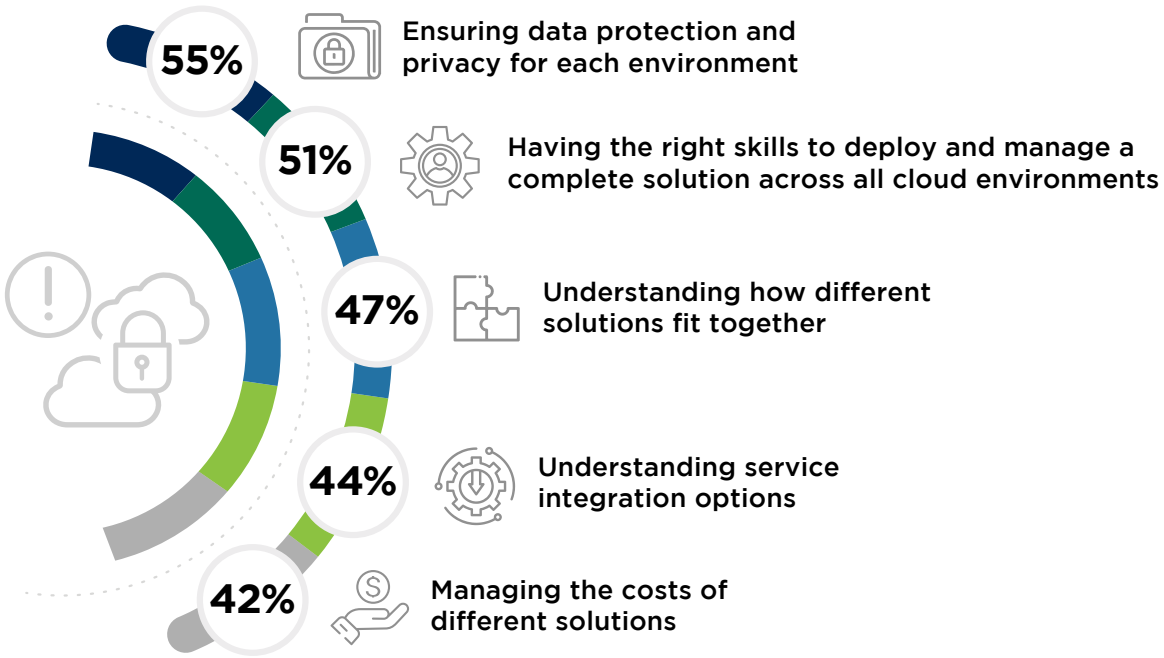
Tackling Multi-Cloud Hurdles

As companies increasingly leverage multiple cloud services, the challenge of maintaining security across diverse platforms becomes more acute. In 2024, securing multi-cloud environments remains a complex task, with data protection and privacy leading as the primary concern, highlighted by 55% of survey participants. This represents a slight increase from 52% observed in 2023, signaling a growing awareness and concern for safeguarding information across disparate cloud platforms.

The challenge of possessing the right skills for deploying and managing solutions across all cloud environments follows closely, although it has seen a decrease from 58% in 2023 to 51% in 2024. This drop could indicate an improvement in training or a shift in focus towards other emerging issues.

Understanding how different solutions integrate (47%) remains at the number three spot, suggesting a continued emphasis on the cohesion of cloud services. Similarly, the challenge of understanding service integration options (44%) reflects the complexities of ensuring seamless operation across cloud environments. The management of costs associated with different cloud security solutions has seen a significant rise in concern, from 37% in 2023 to 42% in 2024, likely reflecting both budget constraints and the increasing financial implications of multi-cloud strategies.

What are your biggest challenges securing multi-cloud environments?



Addressing these challenges starts with enhancing professional skills through targeted education and certifications. It's crucial for companies to develop integrated security strategies that focus on data protection and the seamless interplay of cloud services. By equipping teams with the right expertise and frameworks, organizations can ensure a more secure, efficient multi-cloud ecosystem.

Simplifying Cloud Security Solutions

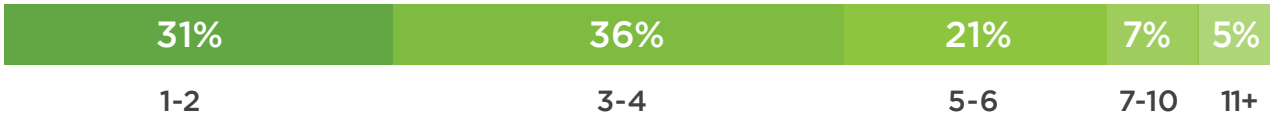
The integration and management of security solutions within cloud infrastructures are pivotal for maintaining organizational agility and safeguarding assets. This survey question sheds light on the operational complexity of handling multiple security solutions, which is a key concern for IT and cybersecurity professionals navigating the multi-cloud environments discussed previously.

About two thirds of users (69%) must access three or more separate security solutions to configure their enterprise's cloud policies. More than a third of respondents (36%), report utilizing 3-4 separate security solutions in their operations.

The data also shows a significant portion (31%) using only 1-2 solutions, up from 28% in 2023, confirming the consolidation trend. This is down from 41% in 2023, suggesting a trend towards simplification and integration of security functionalities to reduce the complexity and potential for inefficiency in managing a diverse set of tools. However, a notable 21% are managing 5-6 solutions (up from 20% in 2023), indicating a high complexity and potential challenges in ensuring seamless security operations.

How many separate security solutions do your users have to access to configure the policies that secure your enterprise's entire cloud footprint?

69% **of organizations depend on at least 3 separate security solutions to manage cloud security across their enterprise**



Security solutions to configure policies

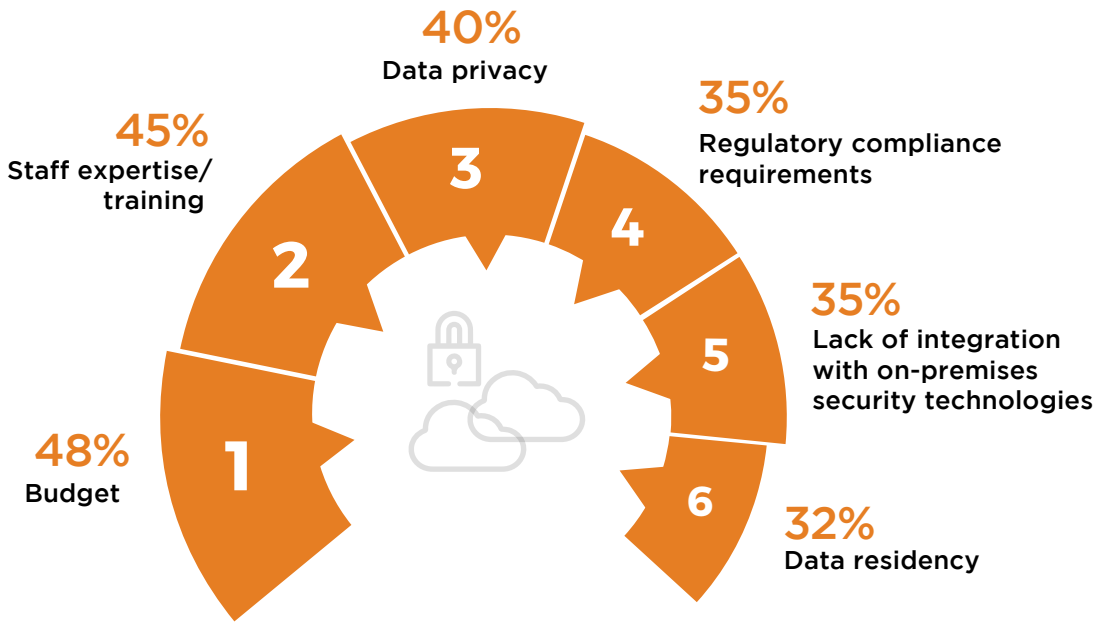
Fragmentation in security tools can lead to increased complexity and potential gaps in cloud protection. Security professionals also struggle to keep up with requirements and alerts, making it harder for security to be more proactive. This challenge underscores the importance of strategic consolidation and optimization of security tools to enhance efficiency and efficacy. For organizations, this means prioritizing the adoption of integrated security platforms that can provide comprehensive protection without the overhead of managing numerous disparate solutions. Such a shift can not only streamline security operations but also improve response times and reduce potential gaps in defense strategies, aligning with the need for robust data protection and skilled management in multi-cloud environments.

Transitioning to Cloud-Based Security Solutions

As organizations deepen their engagement and investment in cloud computing, transitioning to cloud-based security solutions introduces a distinct set of challenges. Leading the list of barriers is budget constraints, cited by 48% of respondents as a main hurdle, up from the second ranked barrier in 2023 (44%). This underscores the heightened scrutiny for technology investments and the need for performing detailed cost-benefit analysis to justify additional cloud security investments.

Close behind, 45% indicate a lack of staff expertise and training as a significant barrier. This points to the critical need for organizations to invest in ongoing education and professional development to equip their teams with the necessary cloud security skills. Data privacy concerns, highlighted by 40%, remains a pressing issue (up from 38% in 2023), reflecting ongoing apprehensions about securing sensitive information within cloud environments. This concern necessitates robust data protection measures and privacy-centric cloud security solutions. Compliance with regulatory requirements, cited by 35%, emphasizes the importance of navigating legal and industry standards in cloud security practices, pointing to the need for solutions that can adapt to diverse regulatory landscapes.

What are the main barriers to migrating to cloud-based security solutions?



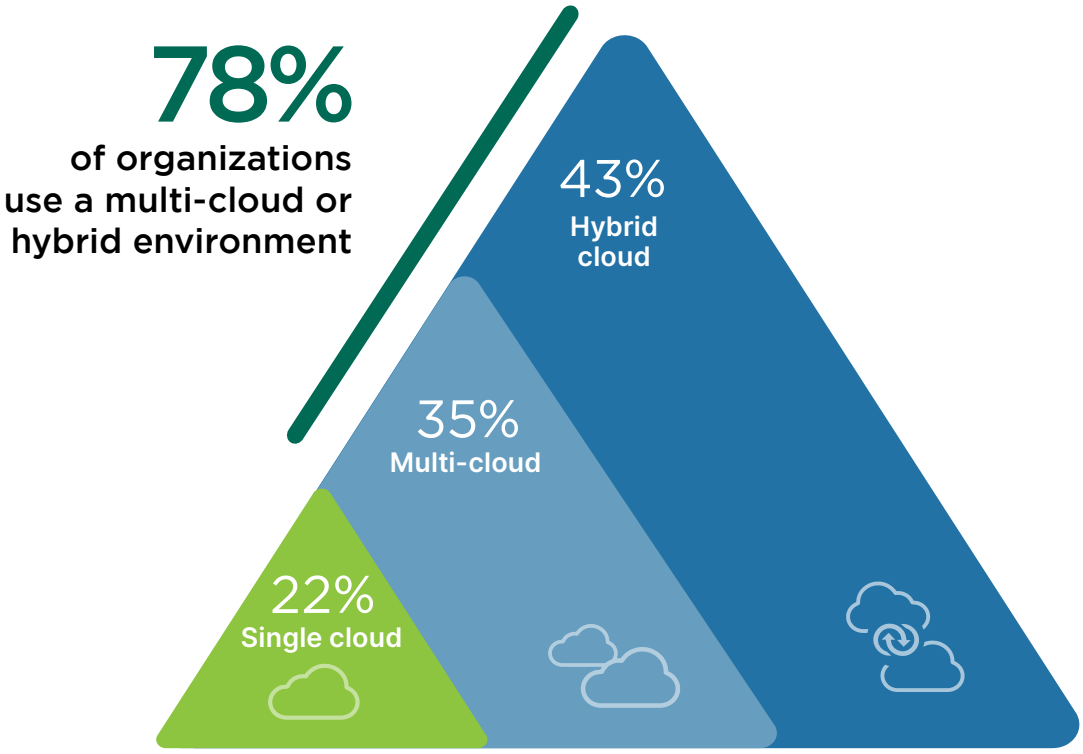
These findings suggest that overcoming barriers to cloud security adoption requires a multifaceted strategy encompassing financial, technical, educational, and strategic dimensions. Organizations must prioritize investments in staff training, select adaptable and compliant cloud security solutions, and navigate financial and operational considerations to ensure a secure, efficient transition to cloud-based security technologies. Emphasizing the development of a skilled workforce capable of managing modern security architectures can significantly smooth the transition, ensuring that cloud migrations enhance, rather than endanger, organizational security.

Cloud Strategy Preferences

The strategic selection of cloud deployment models is a pivotal decision for organizations, influencing operational flexibility, data security, and technology integration. This decision ties back to the challenges of cloud migration, where considerations around data privacy, budget, and expertise play significant roles in shaping cloud strategies.

The survey reveals a preference for hybrid cloud models, with 43% of respondents adopting this approach, indicating its appeal in offering both the scalability of public clouds and the control of private clouds. Following this, 35% of organizations favor a multi-cloud strategy, leveraging the strengths of various cloud providers to optimize performance and reduce dependency on a single vendor. A smaller segment, 22%, opts for a single cloud service, highlighting a streamlined approach that may offer simplicity and ease of management but potentially limits flexibility and redundancy.

What is your organization's primary strategy for cloud deployment?



These preferences underscore the need for organizations to carefully consider their cloud strategies based on their specific operational needs, security requirements, and technological landscapes. Embracing a hybrid or multi-cloud strategy requires a robust framework for managing complexity, ensuring data protection across environments, and a broader skill within security teams. It also suggests a move towards embracing cloud diversity, driven by the need for agility, resilience, and cost optimization in digital transformation efforts.

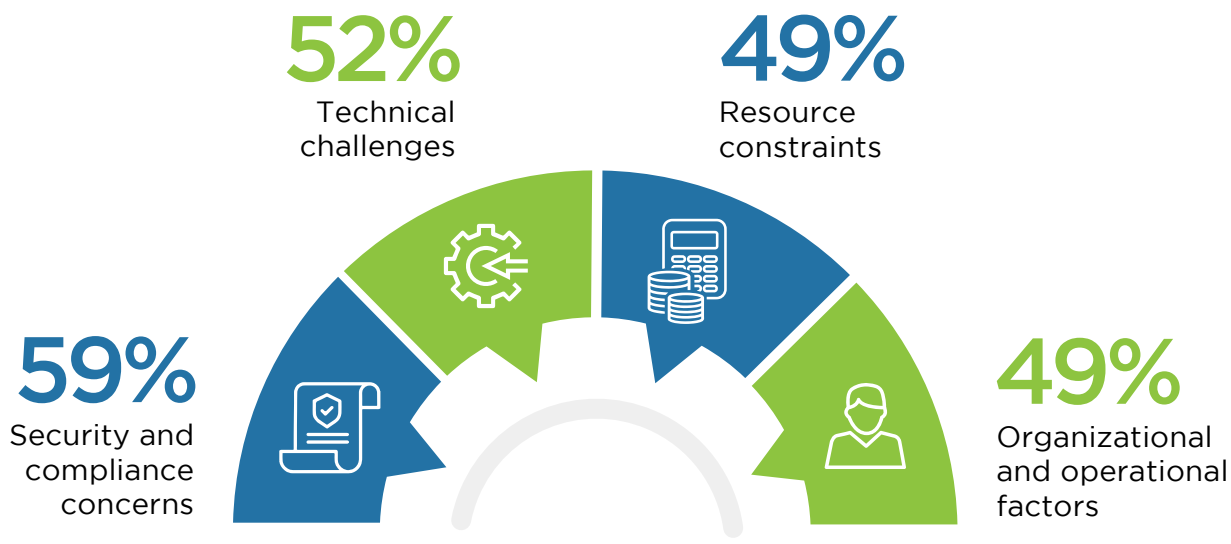
Barriers to Advancing Cloud Maturity

For organizations already utilizing cloud computing, the journey towards deepening and optimizing their cloud strategies presents unique challenges. This shift from initial adoption to continued enhancement and integration of additional cloud services underscores a maturation process that requires a strategic approach to overcome inherent barriers.

Security and compliance concerns remain paramount, identified by 59% of respondents, as growing cloud footprints magnify the complexity of maintaining a robust security posture across increasingly diverse environments.

Technical challenges related to integration with existing infrastructure, noted by 52%, points to the necessity for more sophisticated approaches to system interoperability and data management as cloud utilization scales. Additionally, the resource constraint of finding adequately skilled staff, a challenge for 49% of organizations, signals a critical need for focused investment in talent development and expertise in advanced cloud technologies.

What are the primary barriers to cloud adoption in your organization?



To successfully navigate these challenges, organizations with established cloud operations should prioritize fostering a culture of continuous learning and improvement, investing in advanced training and certification programs for their teams. Embracing cutting-edge cloud security and management tools that offer greater flexibility, automation, and integration capabilities can address technical and security challenges as well as compensate for the continued skill shortage.

Moreover, developing a strategic roadmap that includes regular evaluations of cloud services and vendors will ensure that cloud strategies remain aligned with organizational goals and industry best practices, thereby facilitating a seamless evolution in the cloud maturity journey.

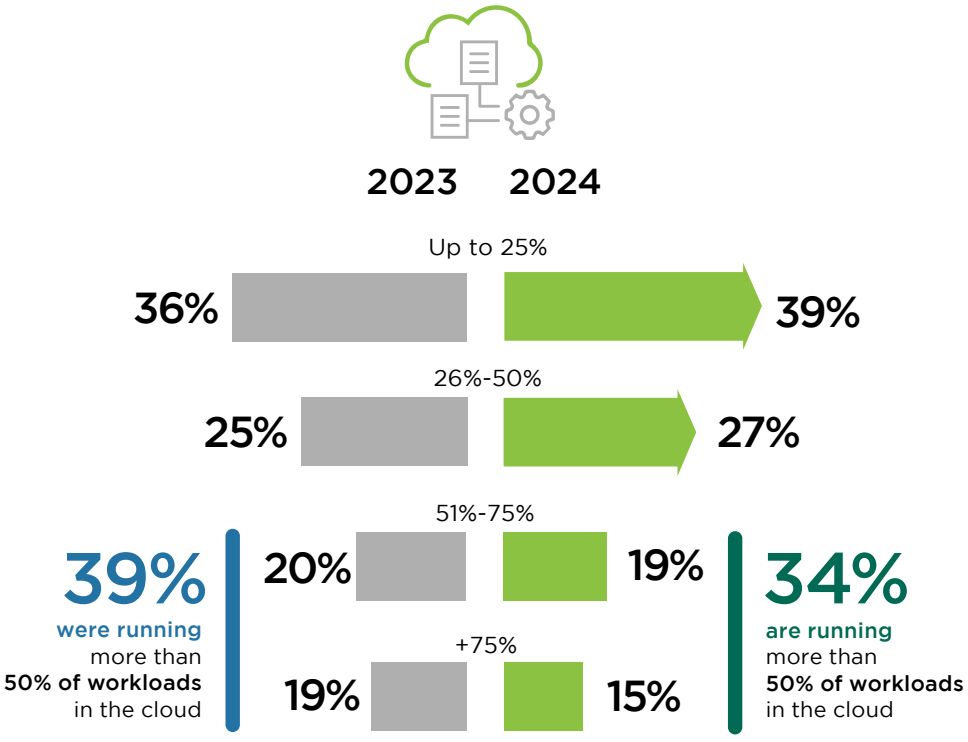
Cloud service concerns 28% | Provider related issues and legalities 27%

Expanding Cloud Footprints

As organizations continue to evolve their cloud strategies, understanding the distribution of workloads across cloud environments offers key insights into their operational and security postures. In our survey, 34% of organizations are operating more than half of their workloads in the cloud, indicating an increasing maturity in the use of cloud computing. A significant portion of respondents (39%) only host up to 25% of their workloads in the cloud, suggesting a cautious or early-stage approach to cloud migration.

Meanwhile, 27% of participants have moved a more considerable portion, 26-50% of their workloads, to the cloud (up from 25% in 2023), reflecting a deeper commitment to cloud computing. 19% of organizations operate 51-75% of their workloads in cloud environments, and 15% exceed the 75% mark.

What percentage of your workloads are in the cloud today vs last year?



Share of workloads in the cloud

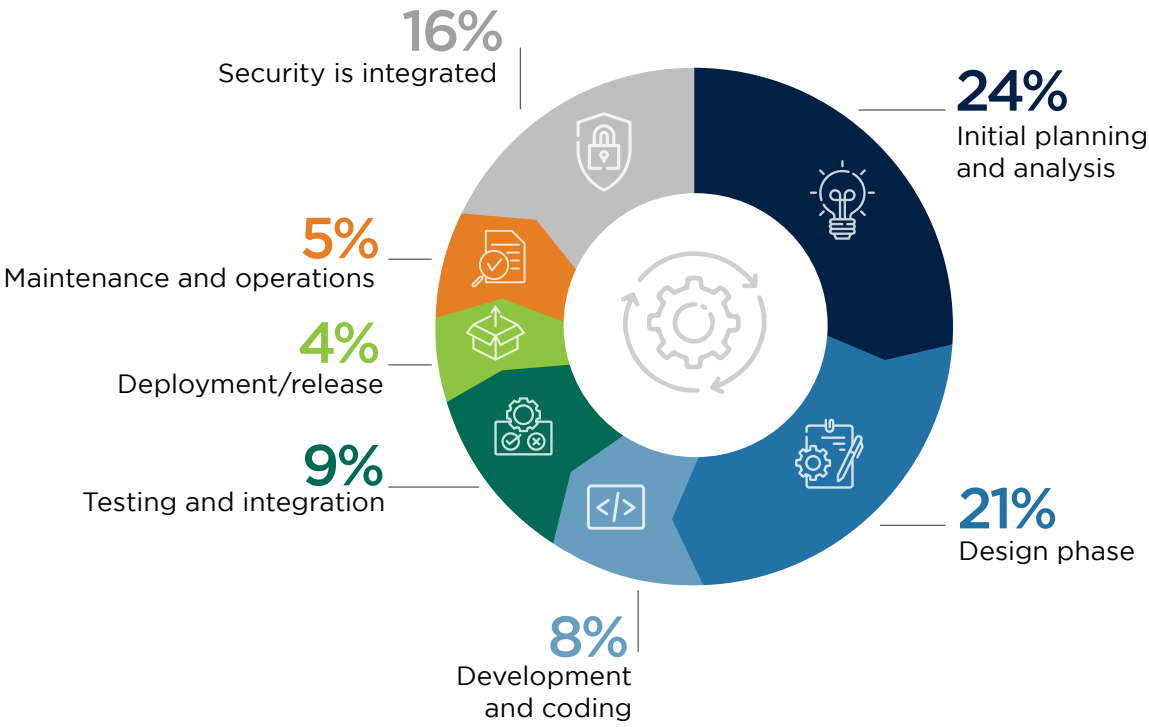
This progression towards higher cloud workload percentages underscores the need for ongoing transition within the cybersecurity landscape, necessitating advanced security strategies and solutions that can adapt to the complexities of cloud environments. It also highlights the need for robust skill development programs and strategic planning to manage the growing reliance on cloud services effectively.

Securing Software from Conception to Deployment

As organizations mature in their cloud computing journey, the focus on securing software development processes intensifies, an aspect that's crucial for maintaining robust security postures in cloud-native and multi-cloud environments. This focus increasingly includes the integration of sound security practices within the Software Development Life Cycle (SDLC) and the adoption of robust DevSecOps principles, reflecting a holistic approach to embedding security into the fabric of software development and operations.

Our survey reveals a diverse application of security practices across different stages of the SDLC. Notably, 24% of respondents emphasize initial planning and analysis as the key phase for security integration, highlighting the trend towards "security by design." However, a significant portion (21%) focuses on the design phase for early integration of security measures in the SDLC. Aligning with best practices, 16% advocate for security integration throughout all stages, underscoring the importance of a comprehensive, end-to-end security mindset.

At which stage of the Software Development Life Cycle (SDLC) does your organization primarily begin to integrate security measures?



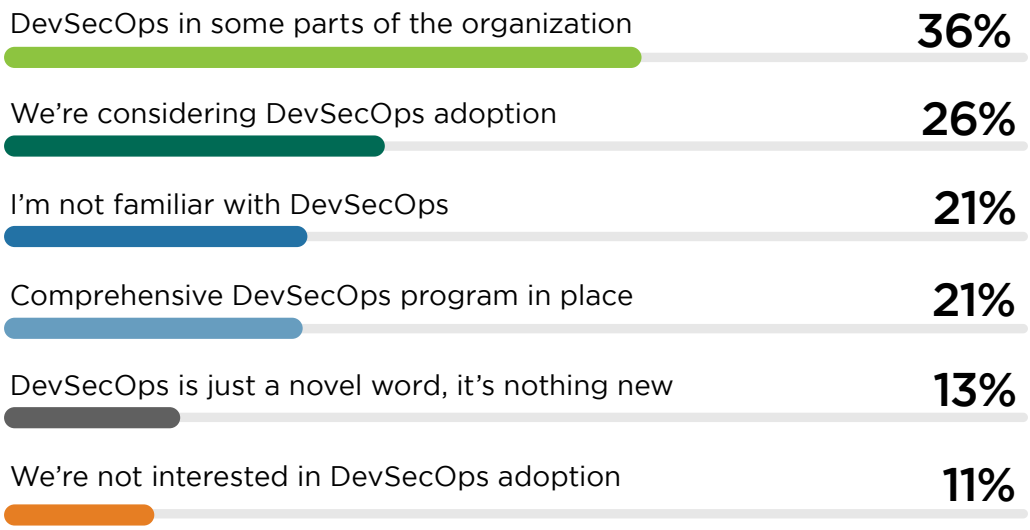
Unsure or lack of informtion about the stage 13%

DevSecOps Adoption

Parallel to the SDLC findings, the current position on DevSecOps adoption illustrates an evolving cybersecurity landscape. DevSecOps is an approach that integrates security practices within the DevOps process, aiming to build security into the software development lifecycle from inception to deployment. This systematic approach enables organizations to deliver secure software faster and more efficiently, reducing vulnerabilities and improving compliance, thereby aligning security with the rapid pace of modern software development and cloud deployment.

An encouraging 21% of organizations have a comprehensive DevSecOps program in place, signifying a mature approach to integrating security within development and operational workflows. Additionally, 36% are implementing DevSecOps in some parts of their organization, indicating growing recognition of its value. Yet, the journey is far from uniform, with 26% considering DevSecOps adoption and a combined 43% either uninterested, viewing DevSecOps as merely a buzzword, or unfamiliar with the concept.

What is your organization's current position on DevSecOps? (select all that apply)



These insights suggest a pivotal shift in how organizations approach software security, moving from traditional, siloed practices to more integrated, proactive security frameworks. The trend towards DevSecOps and security integration across the SDLC not only enhances the security of cloud-based workloads but also aligns with the broader goals of agility, efficiency, and resilience in cloud computing strategies.

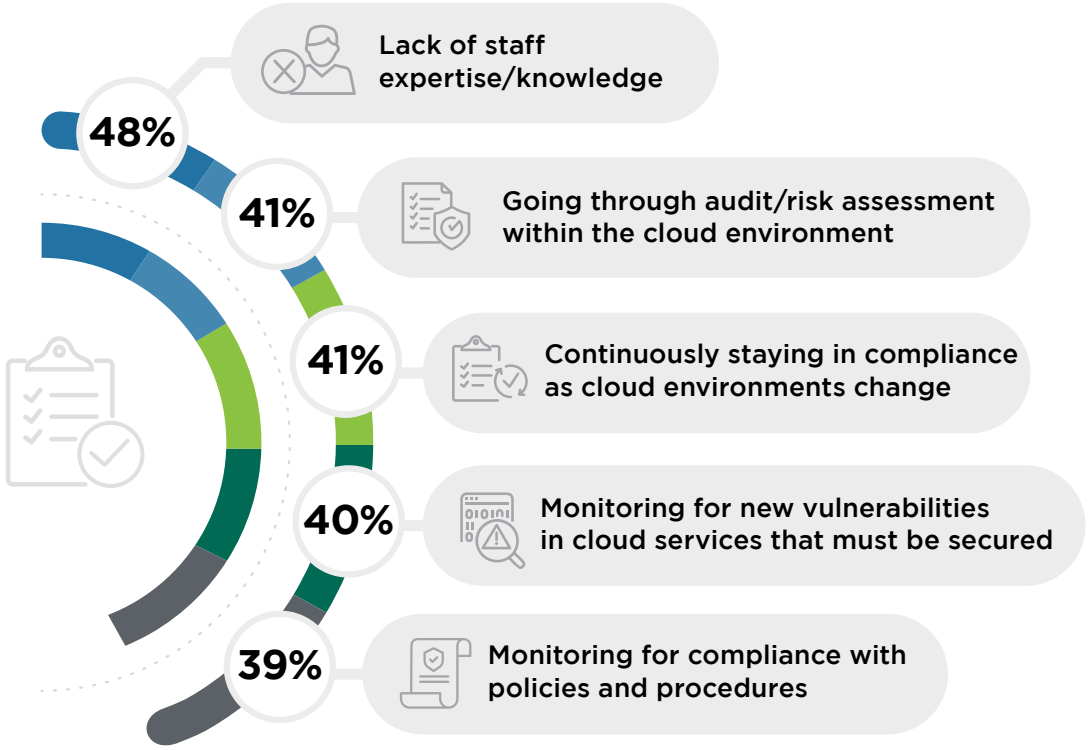
For organizations navigating the complexities of cloud security, the adoption of DevSecOps and the embedding of security at every stage of the SDLC emerge as key strategies for mitigating risks and fostering a culture of security-first thinking. This evolution in practice underscores the need for continuous education, skill development, and strategic investment in security technologies that support a more integrated and automated approach to securing software in the cloud era.

Streamlining Cloud Compliance

The task of maintaining regulatory and industry compliance in cloud environments underscores the critical need for skilled personnel, continuous adaptation, and strategic use of automation. A significant 48% of organizations pinpoint the lack of staff expertise as the primary hurdle, stressing the importance of targeted education and skill development in cloud compliance.

Challenges such as continuously adapting to evolving compliance requirements and conducting thorough audits resonate with 41% of respondents. These findings highlight the dynamic nature of cloud compliance and the necessity for organizations to integrate continuous compliance mechanisms throughout their cloud operations.

Which part of the cloud compliance process is the most challenging?
(select all that apply)



To navigate compliance, it's essential for organizations to foster a culture of continuous learning, automate compliance processes where possible, and ensure compliance practices are embedded within the cloud deployment lifecycle. This strategy not only mitigates the risk of non-compliance but also aligns with the broader objectives of agility and security in the cloud.

Staying up to date about new/changing compliance and regulatory requirements 38% | Data quality and integrity in regulatory reporting 28% | Scaling and automating compliance activities 28% | Applying/following the shared responsibility model 24%

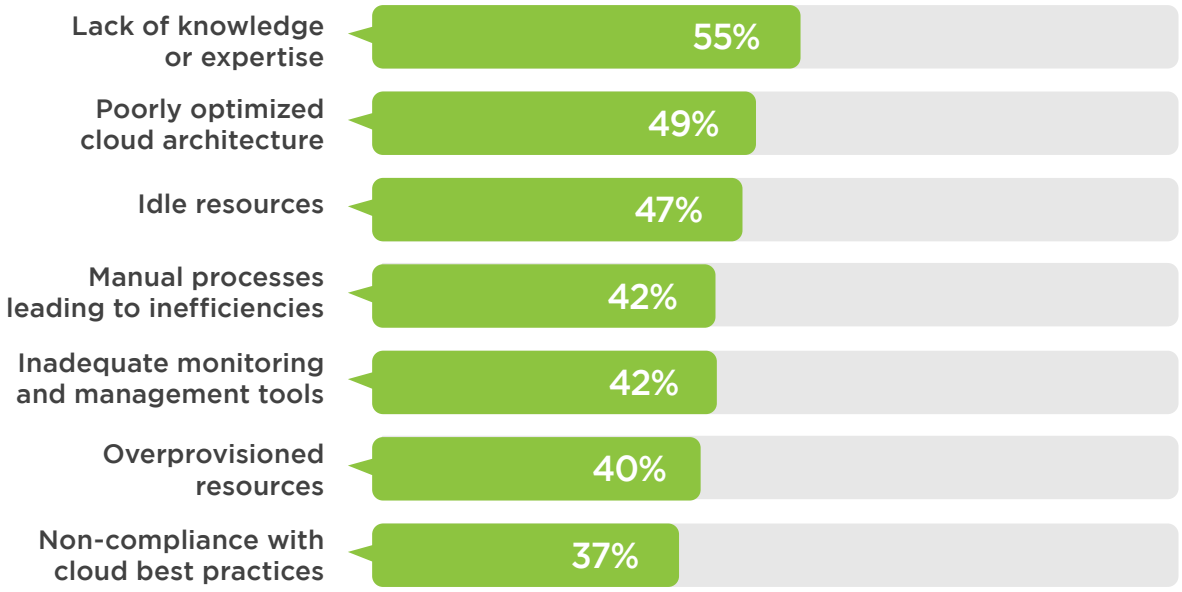
Increasing Cloud Efficiency

Successful cloud cost management involves identifying and reducing inefficiencies, a challenge that becomes increasingly complex as cloud environments grow.

Leading the factors contributing to cloud inefficiencies is the lack of knowledge or expertise in cloud resource management, highlighted by 55% of participants. This gap not only leads to suboptimal resource utilization but also underscores the importance of enhancing cloud literacy and operational skills.

Similarly, 49% highlight poorly optimized cloud architectures, which can lead to overprovisioning—another significant source of inefficiency noted by 40%. Related to this are idle resources, pointed out by 47% of respondents—spending resources on unused or underutilized computing capacity.

Which factors contribute to cloud waste in your organization? (select all that apply)

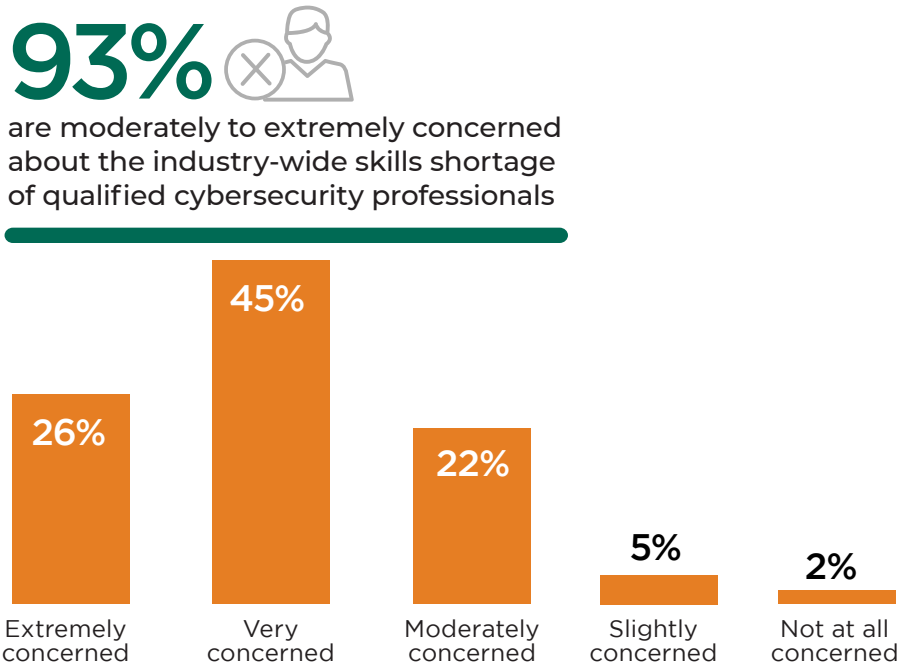


Mitigating cloud inefficiencies requires a strategic blend of education, precise monitoring, and architectural optimization. Organizations should prioritize comprehensive training programs to elevate their teams' understanding of cloud resource management. Leveraging advanced monitoring and management tools can also play a crucial role in identifying idle and overprovisioned resources, enabling proactive adjustments.

Bridging the Cloud Security Skills Gap

The ongoing concern about the industry-wide shortage of skilled cybersecurity professionals is evident among survey respondents, with a combined 93% of participants expressing high levels of concern. Addressing the cybersecurity skills gap is vital to ensure robust cloud security and provide robust defenses against evolving threats.

How concerned are you about the industry-wide skills shortage of qualified cybersecurity professionals?



The security skills shortage not only impacts the ability to defend against cyber threats effectively but also constrains organizations' capacity to innovate and leverage cloud technologies fully. This challenge is particularly critical given the nuances of cloud computing, which demands a unique blend of skills encompassing security, architecture, and operations.

Is your organization experiencing a shortage in cybersecurity talent?

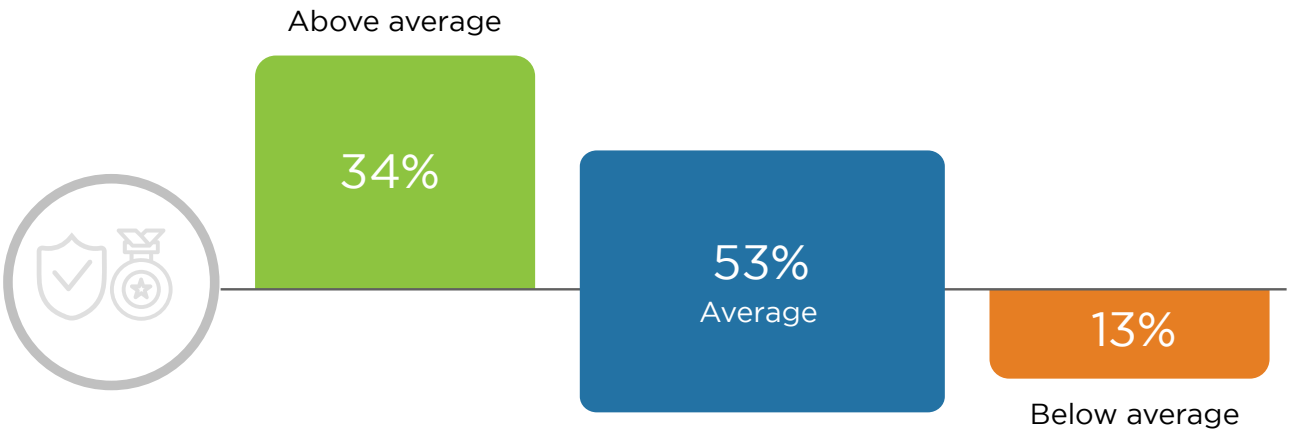
To combat this issue, a strategic approach focused on education, certification, and continuous professional development is essential. Emphasizing certification in cloud security disciplines, creating mentorship opportunities, and fostering a culture that values continuous learning can help mitigate the skills gap. Moreover, organizations might consider more flexible staffing models, such as leveraging external experts or adopting a managed security service approach, to bridge the immediate skills gap while developing internal capabilities over the long term.

Cloud Competence: Perception Vs. Reality

The discrepancy between self-assessed cloud security competencies and market realities suggests an optimistic view within many organizations. While a commendable 34% consider their capabilities above average, this perspective may not fully align with the complex and evolving nature of cloud security challenges. Recognizing the potential for overconfidence, it's essential to approach capability assessments with a blend of humility and strategic foresight. Education and certification emerge as key tools in this context, offering a structured way to accurately evaluate, benchmark, and expand cybersecurity competencies.

By aligning team skills with recognized standards and industry best practices, organizations can ensure their self-assessments are rooted in reality. Furthermore, these pathways provide a clear framework for continuous improvement, enabling teams to systematically address gaps and fortify their cloud security posture with confidence and precision.

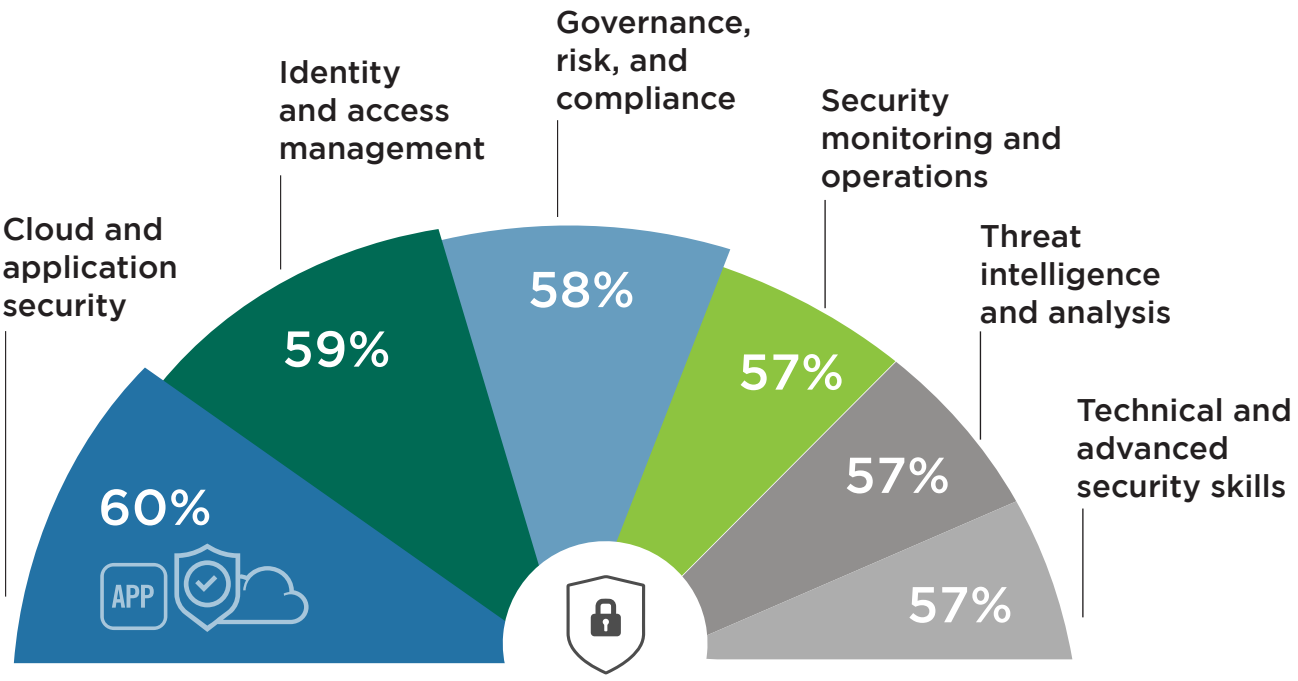
How would you rate your team's overall security skills?



Key Security Skills for the Cloud Era

The survey illuminates the cloud security skills most required in today's cloud environments, reflecting the complex demands of the cybersecurity landscape. Leading the essential skills, cloud and application security emerges as a top priority with 60%, underscoring the critical need for safeguarding cloud platforms and applications. Following closely, identity and access management (IAM), emphasized by 59%, highlights the significance of controlling access to maintain security integrity in cloud architectures. Skills in governance, risk, and compliance (GRC), security monitoring, and threat intelligence reflect a balanced emphasis across diverse skill sets, suggesting a comprehensive approach to cloud security talent development is crucial.

What are the most important security skills required in your organization?



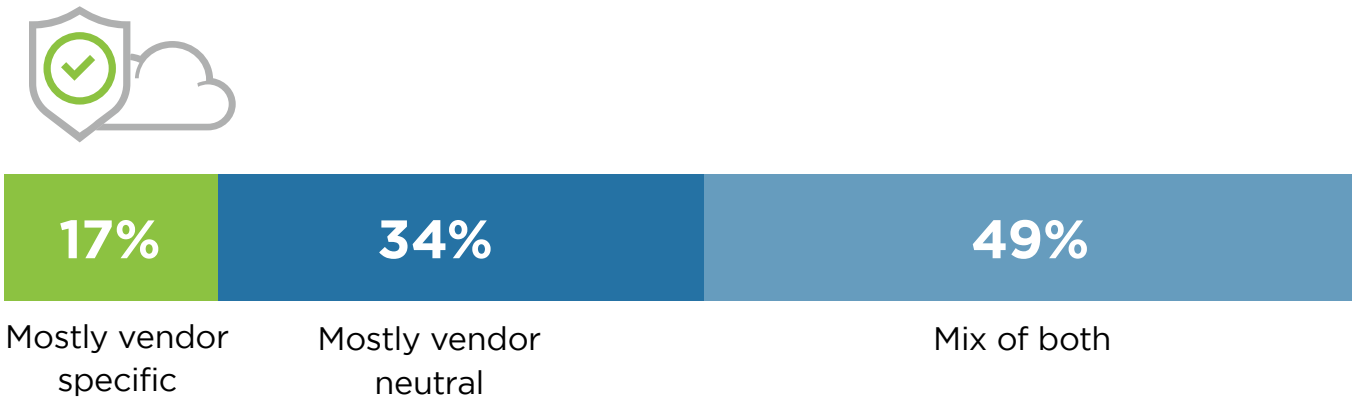
This nuanced ranking highlights the need for strategic investment in training and certification, enabling professionals to acquire a broad spectrum of competencies, which is crucial for navigating the complexities of cloud security and reinforcing an organization's resilience against evolving threats.

Cloud Security Certification Preferences

When plotting the course for cloud security certification, the preferences within the cybersecurity community lean towards a balanced approach. A significant 49% of respondents favor a blend of both vendor-specific and vendor-neutral certifications, reflecting a comprehensive strategy for developing cloud security expertise. This mix allows professionals to gain deep insights into specific platforms while also acquiring broad, universally-applicable security skills.

Interestingly, a third of participants (34%) prioritize vendor-neutral certifications (up from 29% in 2023), underscoring the value placed on broad, foundational knowledge that transcends specific cloud environments. This approach aligns with the philosophy of building a versatile skill set that prepares individuals for a variety of challenges across the varied cloud security landscape. Meanwhile, 17% lean towards mostly vendor-specific certifications, which can provide deep, technical understanding of particular cloud services, essential for organizations heavily invested in specific cloud platforms.

When considering cloud security certification for yourself and/or your team, do you consider mostly vendor specific certifications or vendor neutral certifications?

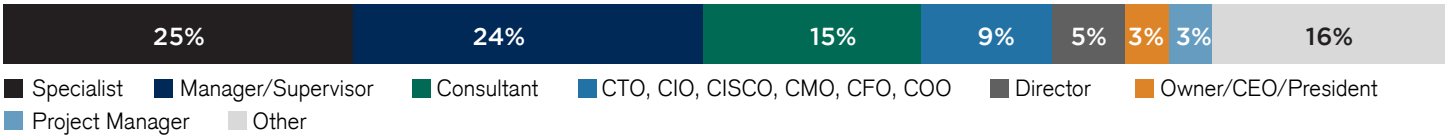


This preference distribution suggests a strategic emphasis on versatility and depth in cloud security education. Embracing both vendor-specific and vendor-neutral certifications can equip professionals with a rich background of knowledge and skills, fostering a robust cybersecurity workforce capable of addressing diverse and evolving threats.

Methodology & Demographics

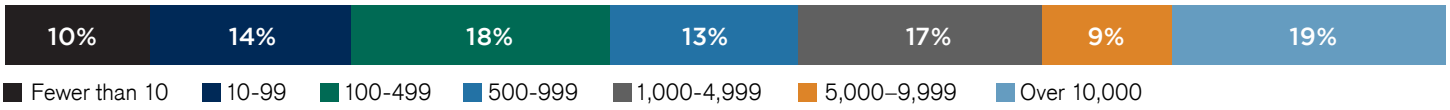
The 2024 Cloud Security Report is derived from an extensive survey of 951 cybersecurity professionals, conducted in April 2024. The study reveals how organizations utilizing cloud services are addressing security threats, as well as the training, certifications, and best practices prioritized by IT security leaders. The participants encompass a diverse range of roles, from technical executives to IT security practitioners, and represent a balanced cross-section of organizations of various sizes and industries.

CAREER LEVEL

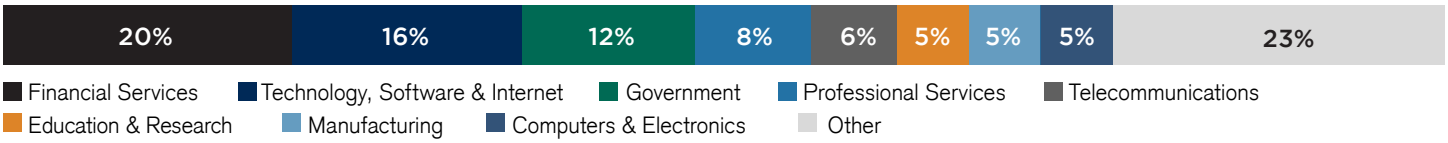


DEPARTMENT

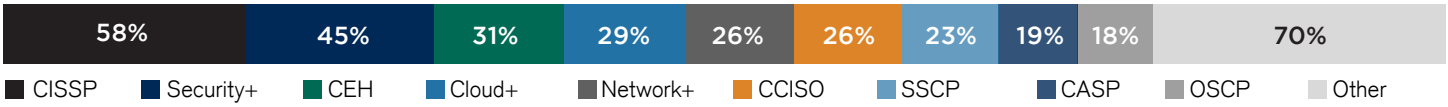
COMPANY SIZE



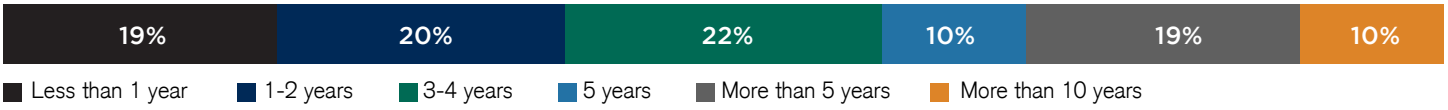
INDUSTRY



SECURITY CERTIFICATIONS HELD



YEARS OF SECURITY EXPERIENCE



Best Practices for Cloud Security Strategy

In the face of evolving threats and complexities, safeguarding your cloud environment demands strategic, actionable measures.

Prioritize Multi-Layered Security: Implement a comprehensive security framework that integrates with your cloud services, addressing vulnerabilities at every level. The report's finding that 96% of organizations are concerned about public cloud security underscores the need for robust, layered defenses.

Embrace Continuous Monitoring: Adopt real-time monitoring tools to promptly detect and respond to threats. With 69% of organizations managing their cloud security through three or more solutions, integrating continuous monitoring can simplify and enhance security oversight.

Enhance Data Protection: To safeguard sensitive information, utilize encryption, access controls, and data loss prevention techniques. 55% of respondents identify data protection as a primary challenge in multi-cloud environments, highlighting its importance.

Invest in Training and Certification: Address the skills gap and empower your team with the latest cloud security knowledge. 93% of respondents expressed concern over a shortage of qualified professionals, which can be mitigated through targeted education and certification programs.

Adopt a Zero Trust Model: Assume no entity is trusted by default, from inside or outside the network, requiring verification from anyone trying to access resources in your network. This approach is critical in a landscape where trust assumptions can lead to vulnerabilities.

Streamline with Cloud Security Posture Management (CSPM): Leverage CSPM tools to automate the identification and remediation of risks across cloud platforms, reducing complexity and enhancing security posture.

Implement Identity and Access Management (IAM): With 59% highlighting the significance of IAM, ensure that only authorized users can access certain data or systems, minimizing the risk of data breaches.

Plan for Incident Response: Develop and regularly update an incident response plan tailored to cloud-specific scenarios, ensuring your team can act swiftly and effectively in the event of a security breach.

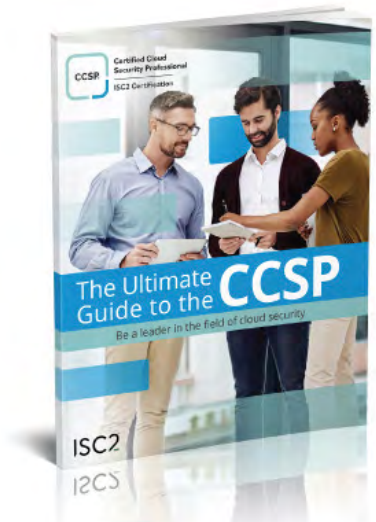
By integrating these best practices into your cloud security strategy, you can address the key challenges highlighted in the 2024 Cloud Security Report while positioning your organization to navigate the cloud landscape confidently and securely.

Rise to the Top in Cloud Security

Reach new heights in your cybersecurity career with globally recognized CCSP certification from ISC2, creator of the CISSP.

Find out everything you need to know about cloud security's premier credential in The Ultimate Guide to the CCSP.

- **Fast Facts**
- **Benefits of Certification**
- **Exam Overview**
- **Tips to Prepare**
- **Study Tools and Resources**
- **And more**



Get The Ultimate Guide

CCSP is a window to your future.
Start your journey today.

CERTIFICATION MAGAZINE
2023 TOP CERT
CCSP
ISC2
THE NEXT BIG THING

CCSP tops Certification Magazine's 2024 list of credentials experts plan to earn as "The Next Big Thing."

CCSP®
Certified Cloud Security Professional
ISC2 Certification

ISC2 is an international nonprofit membership associate focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, ISC2 offers a portfolio of credentials that are a part of a holistic, pragmatic approach to security. Our association of candidates, associates and members is made up of certified cyber, information software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is support by our commitment to educate and reach the general public through our charitable foundation - The Center for Cyber Safety and Education™.

For more information on ISC2, visit www.isc2.org, follow us on X or connect with us on Facebook and LinkedIn.

Cybersecurity
INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit cybersecurity-insiders.com