

2023

# Cloud Security Report



# Introduction

The 2023 Cloud Security Report highlights the critical cybersecurity concerns, incidents, and trends as organizations increasingly adopt multi-cloud environments. Despite growing cloud maturity, a staggering 95% of security professionals remain concerned about public cloud security, emphasizing the urgent need for education, training, and solutions that keep pace with complex multi-cloud environments and evolving threats.

An ongoing challenge faced by cybersecurity professionals is the lack of qualified security staff (43%). As 72% of respondents use two or more cloud providers, top security priorities such as preventing misconfigurations, securing cloud apps, and achieving regulatory compliance become increasingly challenging due to the rise in complexity and attack surface - made worse by the cybersecurity talent gap. Addressing the talent shortage issue through cybersecurity training and certifications emerges as a vital solution for organizations.

Barriers to cloud-based security are primarily people and process-related, rather than technology-focused. The lack of cybersecurity staff expertise and training (53%) remains the highest barrier, followed by budget challenges (44%) and data privacy issues (38%). The persistent shortage of qualified cybersecurity talent is also the most significant barrier to faster cloud adoption (37%), followed by legal and regulatory compliance issues (30%) and data security and leakage risks (29%).

In light of these challenges, a majority of organizations (83%) acknowledge that their teams require additional cloud security training and certifications to better operate in cloud environments. The report underscores the importance of addressing security concerns and investing in cybersecurity training and certifications to tackle the talent shortage and ensure a secure and robust cloud ecosystem.

We would like to thank [ISC2](#) for supporting this unique research. We hope you enjoy this report.

Thank you,

*Holger Schulze*



**Holger Schulze**

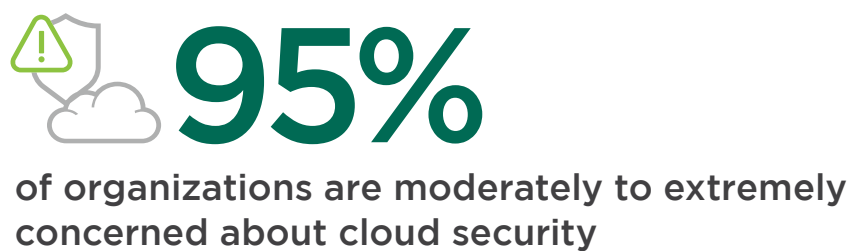
CEO and Founder  
Cybersecurity Insiders

**Cybersecurity**  
INSIDERS

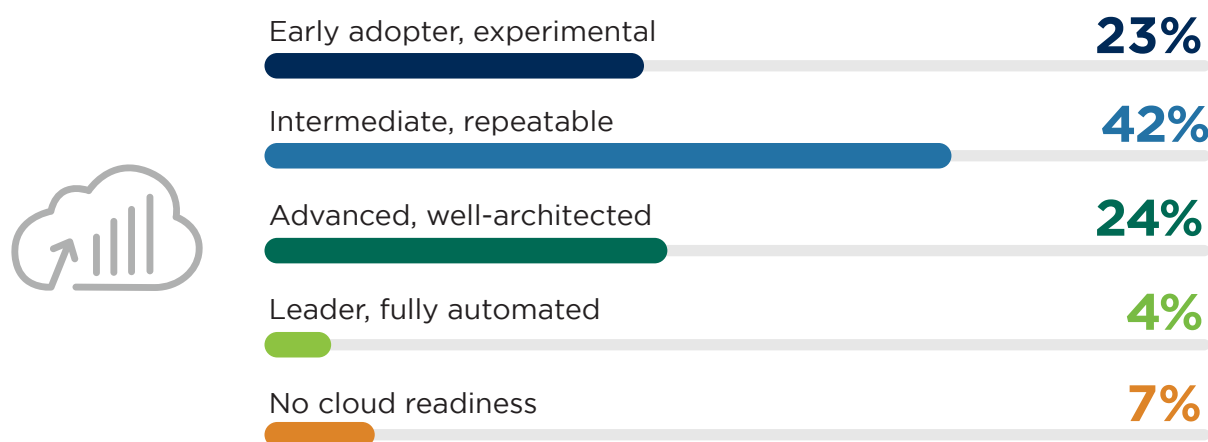
# Cloud Security Concerns

Despite the increasing maturity of cloud technology, 95% of security professionals still exhibit moderate to extreme concern regarding public cloud security. This persistent trend highlights the crucial need for ongoing cloud security education and the development of solutions that can adapt to the ever-evolving multi-cloud environments and threat landscapes. Consequently, organizations should place a high priority on cloud security, invest in comprehensive protection strategies, and offer continuous training to their teams to maintain a secure cloud environment.

► How concerned are you about the security of public clouds?



► How would you describe your organization’s cloud maturity level?



# Cloud Security Incidents

Security incidents happen frequently: 24% of organizations experienced a public cloud-related security incident in the last 12 months. Misconfiguration was the leading cause, followed by account compromise and exploited vulnerabilities.

This finding suggests that organizations should prioritize enhancing their cloud security measures and improving incident detection and reporting. Continuous monitoring and regular security audits can help organizations better understand their security posture and reduce the risk of cloud-related security incidents.

► **Did your organization experience a public cloud related security incident in the last 12 months?**



With multi-cloud complexity on the rise, it is not surprising that 67% of cybersecurity professionals are, at best, only moderately confident in their organization’s cloud security posture. The survey results emphasize the importance of continuous improvement in cloud security strategies, ongoing training, and the implementation of best practices to increase confidence and ensure a robust security posture in the face of evolving threats.

► **How confident are you in your organization’s cloud security posture?**




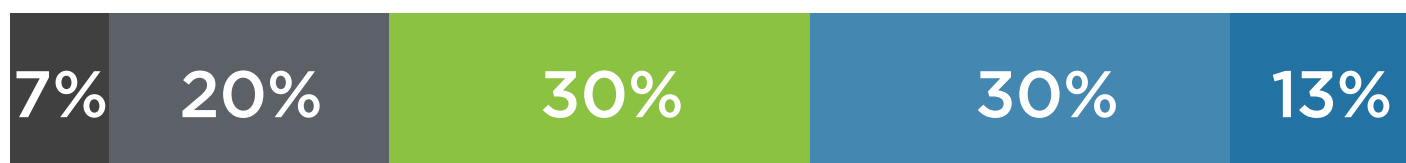
# Cloud Security Risk

How do cloud security professionals feel about the risk levels of cloud versus on-premise environments? While a third of respondents (30%) see the risk levels about equal, 43% observe a higher degree of risk in the cloud. A quarter of respondents (27%) see a lower risk for public cloud breaches.

These findings demonstrate a range of opinions among cybersecurity professionals regarding the risk of security breaches in public cloud environments. It highlights the importance of understanding the specific security requirements of an organization and implementing appropriate measures to mitigate potential risks, regardless of the chosen environment.

- Compared to traditional, on-premise IT environments, would you say the risk of security breaches in a public cloud environment is higher or lower?

**43%**   
say public cloud is at higher risk  
than on-premise environments

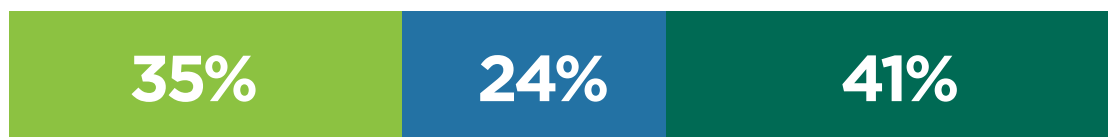


Significantly lower

Significantly higher

■ Significantly lower ■ Somewhat lower ■ About the same ■ Somewhat higher ■ Significantly higher

- Are public cloud apps/SaaS (such as Salesforce and Office 365) more or less secure than on-premise applications?



Public cloud apps  
are **MORE**  
secure than  
on-premises apps

Public cloud apps  
are **LESS**  
secure than  
on-premises apps

About the same

# Cloud Workloads

Organizations are rapidly shifting workloads to the cloud, with 39% already operating more than half of their workloads in the cloud. Additionally, 58% of respondents plan to make this shift within 12-18 months.

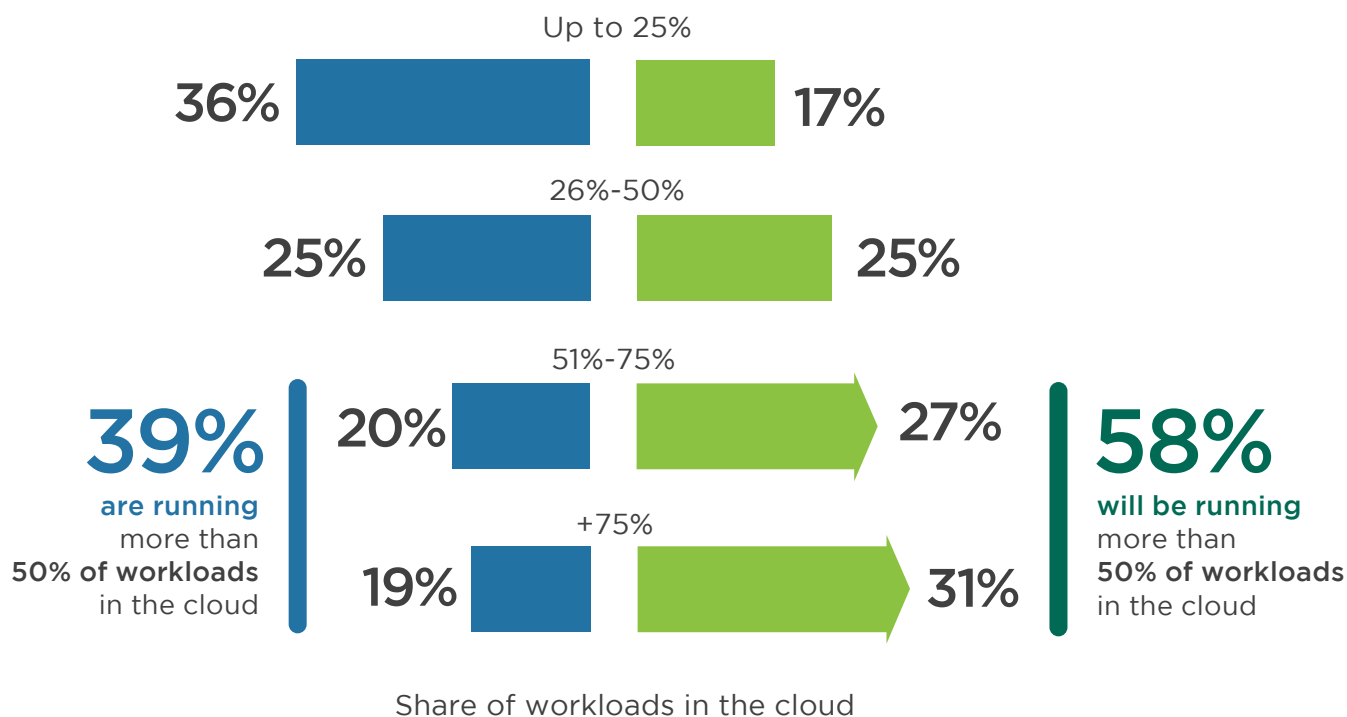
These findings indicate a growing recognition of the benefits of cloud computing, leading organizations to plan for further workload migration to the cloud. As cloud adoption continues to expand, it is crucial for businesses to consistently enhance their cloud security measures and strategies. This ensures the protection of workloads and establishes a robust security posture.

► What percentage of your workloads are in the cloud today?

► What percentage of your workloads will be in the cloud in the next 12-18 months?



TODAY    NEXT 12-18 MONTHS

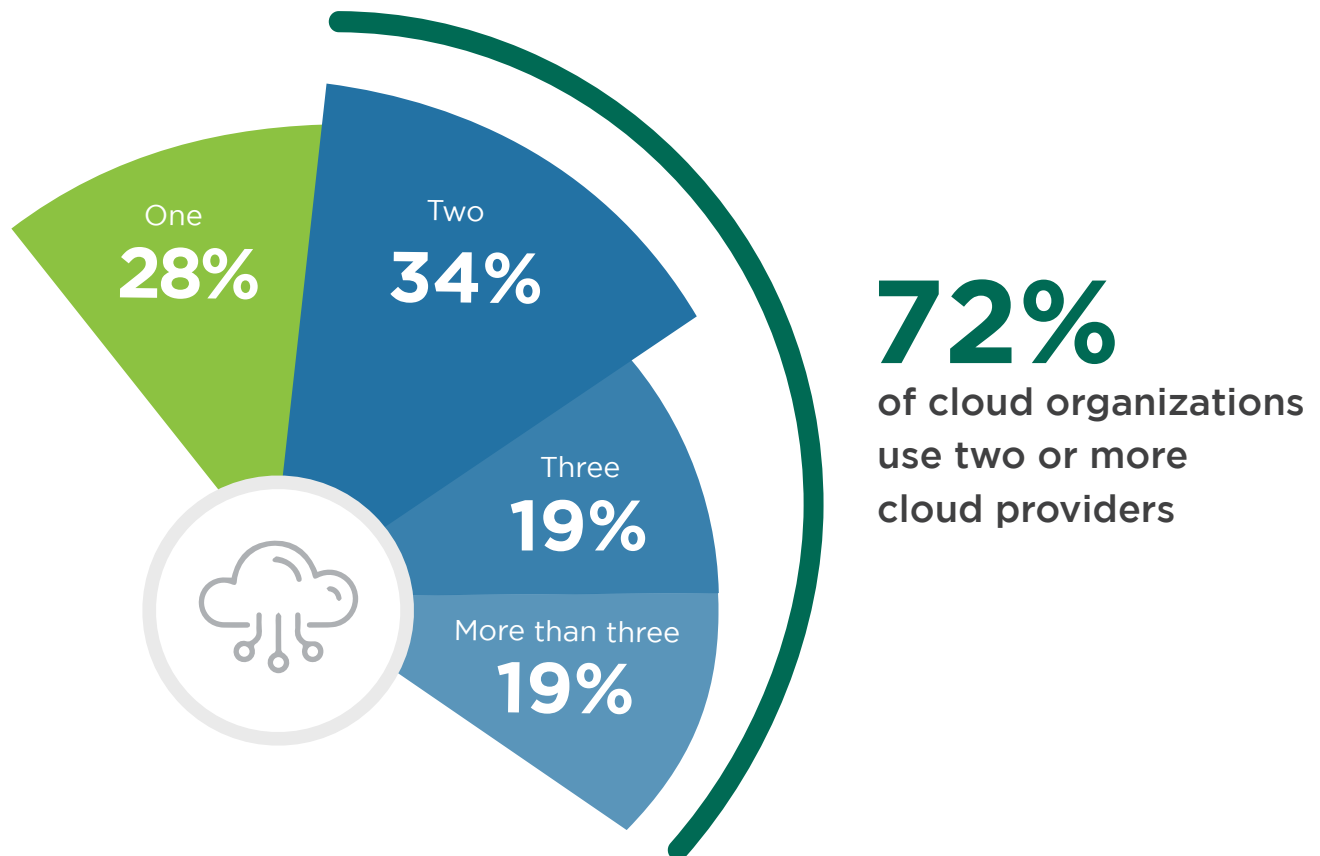


# Multiple Clouds

The results reflect the trend towards multi-cloud strategies that offer increased flexibility, redundancy, and the ability to leverage the strengths of different providers. This multi-cloud approach, however, also brings the challenge of managing and securing complex environments with multiple cloud providers.

With 72% of respondents using two or more cloud providers, top security priorities (such as preventing misconfigurations, securing cloud apps, and reaching regulatory compliance) are multiplied by the increase in complexity and attack surface.

## ► How many cloud providers does your organization currently use?



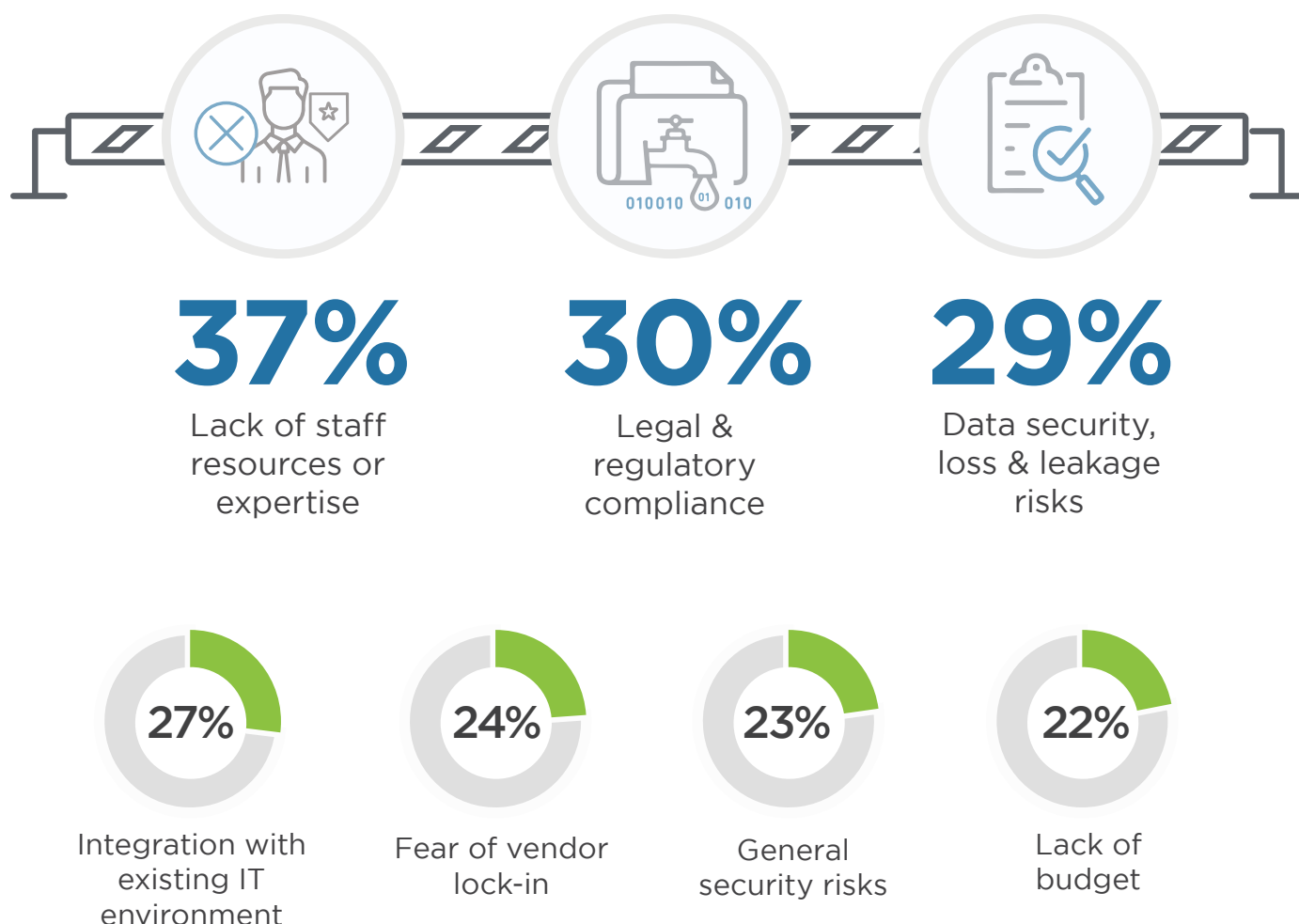


# Barriers to Cloud Adoption

What is holding back organizations from increasing their investment in the cloud? The ongoing lack of qualified cybersecurity talent with the necessary knowledge and experience to effectively implement and manage cloud solutions continues to be the most critical barrier to faster cloud adoption (37%). This is followed by legal and regulatory compliance issues (30%) and data security and leakage risks (29%).

To overcome these barriers, organizations should invest in staff training and certification, develop robust security and compliance strategies, and work closely with cloud service providers to ensure seamless integration and to address security concerns.

## ► What are the biggest barriers holding back cloud adoption in your organization?



Cost/lack of ROI 21% | Internal resistance and inertia 20% | Loss of control 19% | Complexity managing cloud deployment 18% | Lack of transparency and visibility 15% | Billing & tracking issues 14% | Lack of maturity of cloud service models 13% | Lack of management buy-in 13% | Dissatisfaction with cloud service offerings/performance/pricing 12% | Lack of customizability 10% | Lack of support by cloud provider 8% | Performance of apps in the cloud 8% | Availability 8% | Other 5%

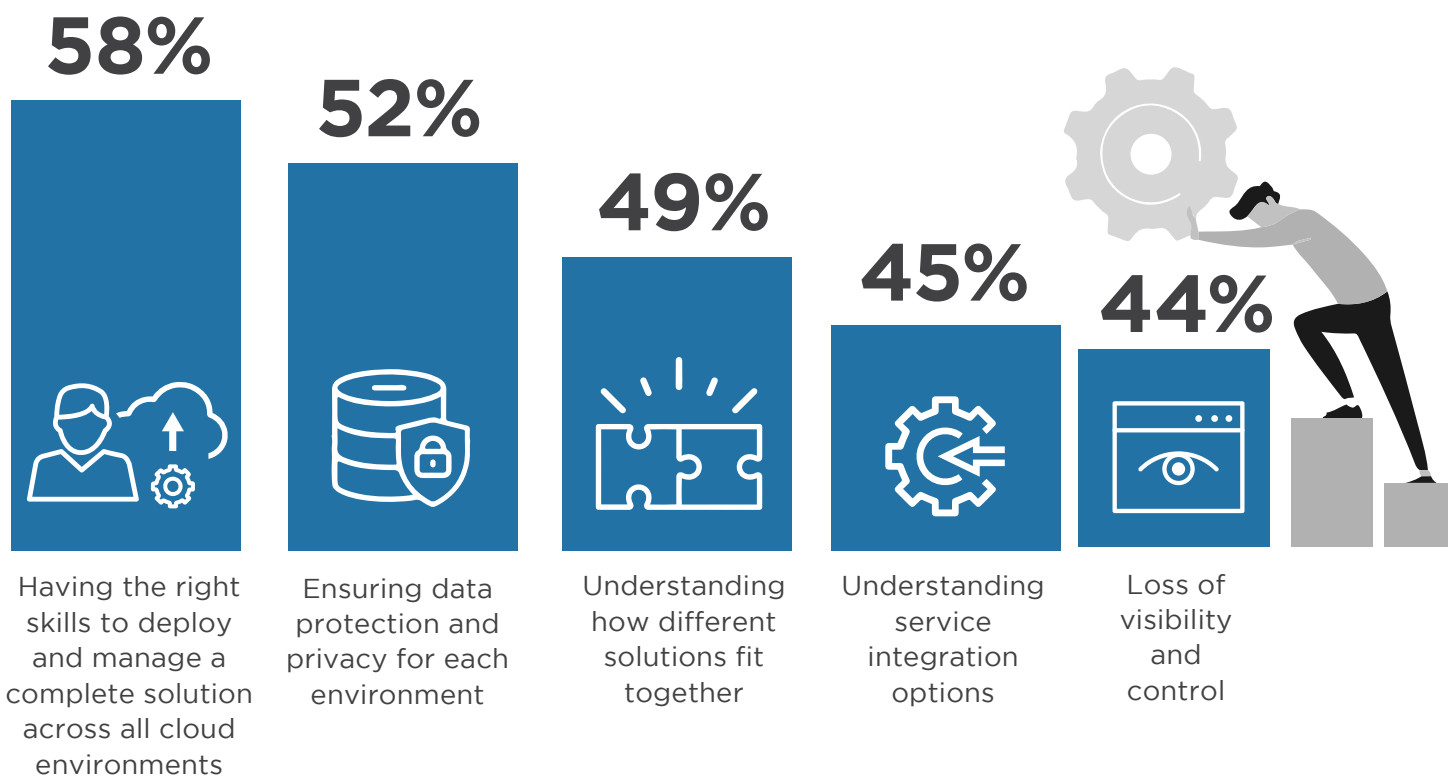


# Challenges of Securing Multi-Cloud

Multi-cloud increases complexity and causes new security challenges. The skills and expertise that multi-cloud environments demand is clearly highlighted in the fact that three out of the four top challenges are related to having the right talent, along with an in-depth understanding of each cloud platform.

The ongoing skills gap is clearly the most significant challenge, emphasizing the importance of having a skilled workforce that can effectively manage and deploy security solutions across multiple cloud platforms.

## ► What are your biggest challenges securing multi-cloud environments?

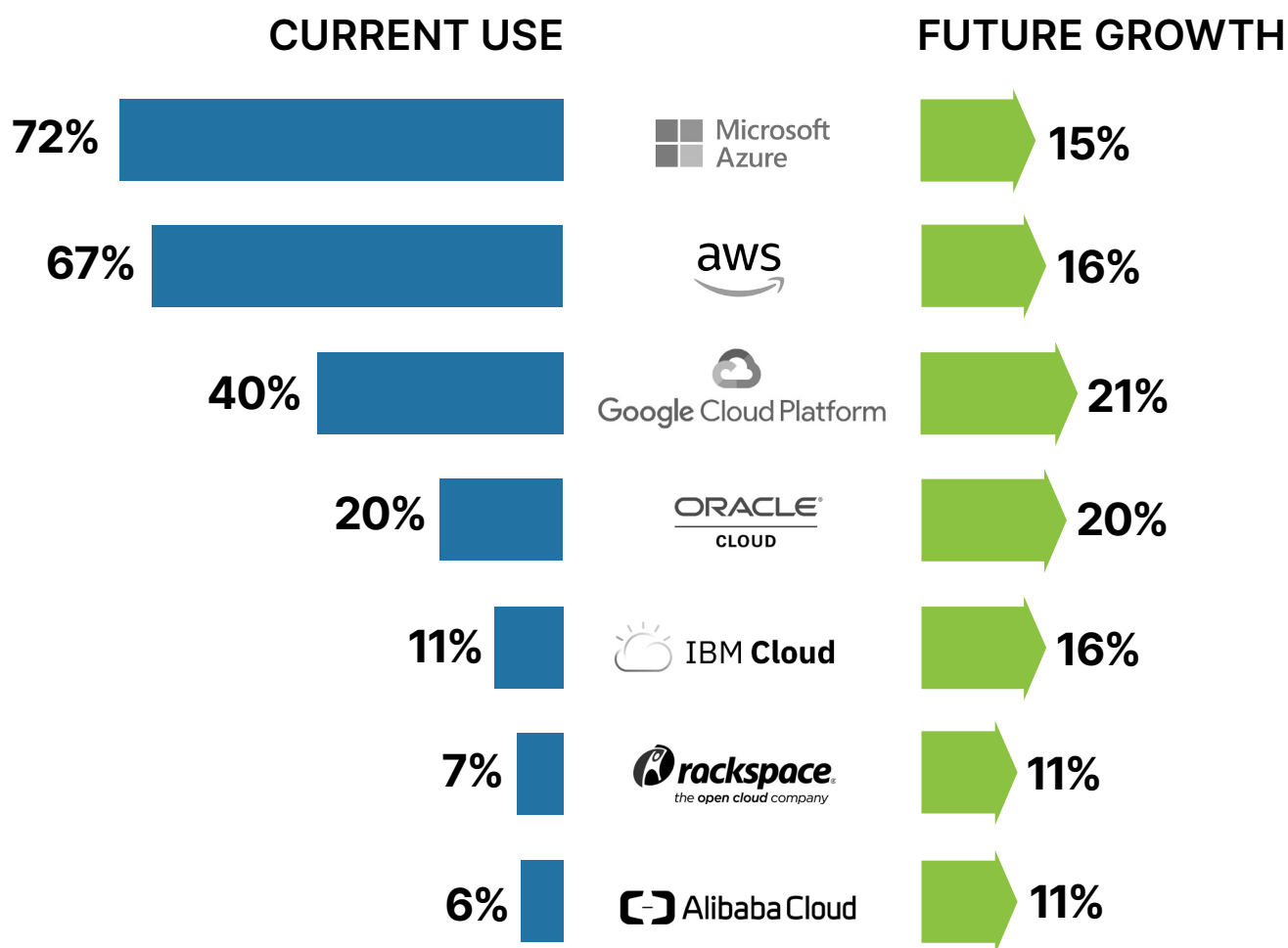


Keeping up with the rate of change 38% | Managing the costs of different solutions 37% | Providing seamless access to users based on their credentials 37% | Selecting the right set of services 36% | Other 3%

# Preferred Cloud Providers

Which providers are organizations prioritizing for their cloud use? The big name providers, such as Microsoft Azure (72%) and Amazon Web Services (67%), continue to dominate the market. However, predicted future cloud adoption is strong for Google Cloud Platform (21%) and Oracle Cloud (20%).

► What cloud IaaS provider(s) do you currently use or plan to use in the future?

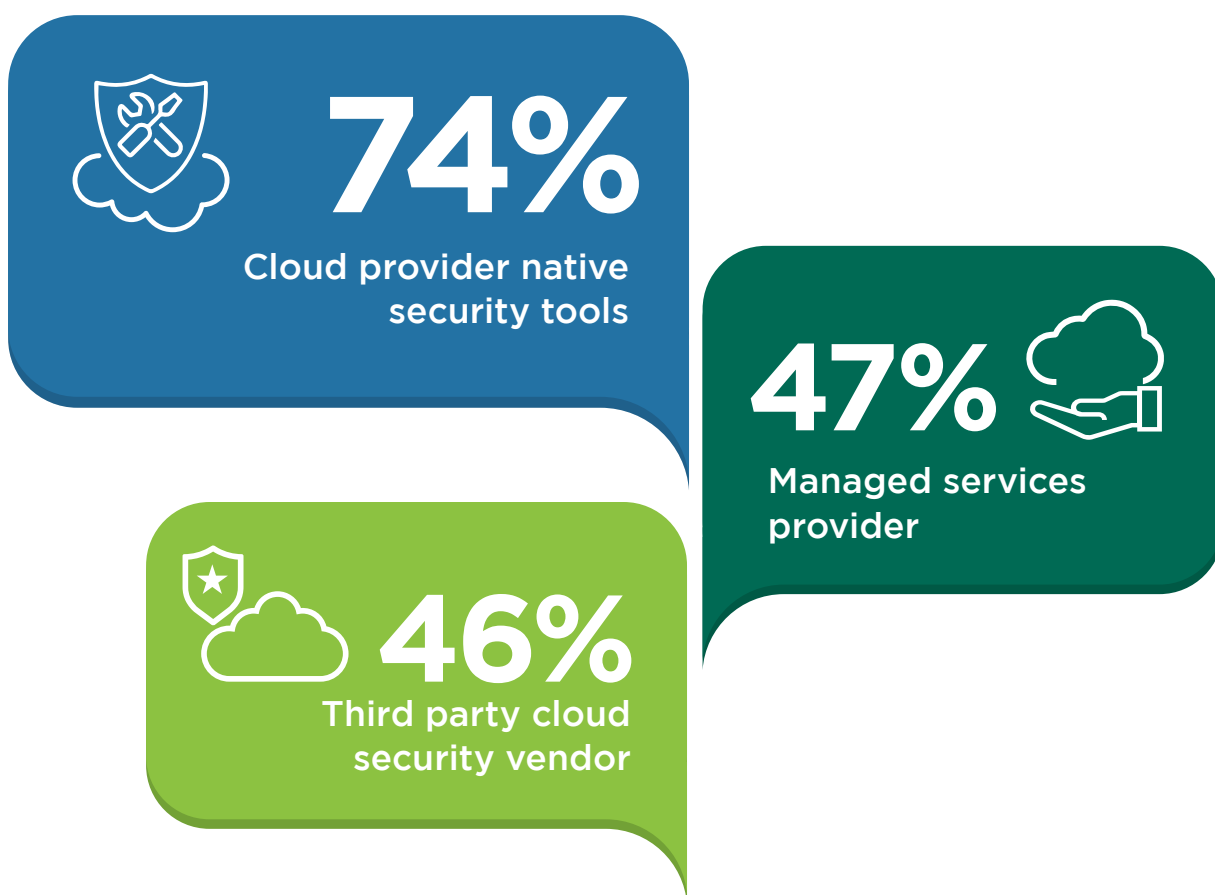


# Cloud Security Choices

When it comes to the choice of cloud security delivery, the majority of organizations rely on the native security tools provided by their cloud providers (74%). These built-in tools offer a level of protection and integration tailored to the specific cloud environment, making them a popular choice.

A significant number of organizations (47%) choose to work with managed services providers for their cloud security needs. By outsourcing to a managed services provider, organizations can benefit from the provider's expertise and resources, which can help them manage the complexities of securing their cloud environments. Many organizations also opt for third-party cloud security vendors to enhance their security posture (46%). These vendors offer specialized solutions that can complement or extend the capabilities of native security tools provided by the cloud providers.

## ► How do you source cloud security?



# Native Security vs Third-Party

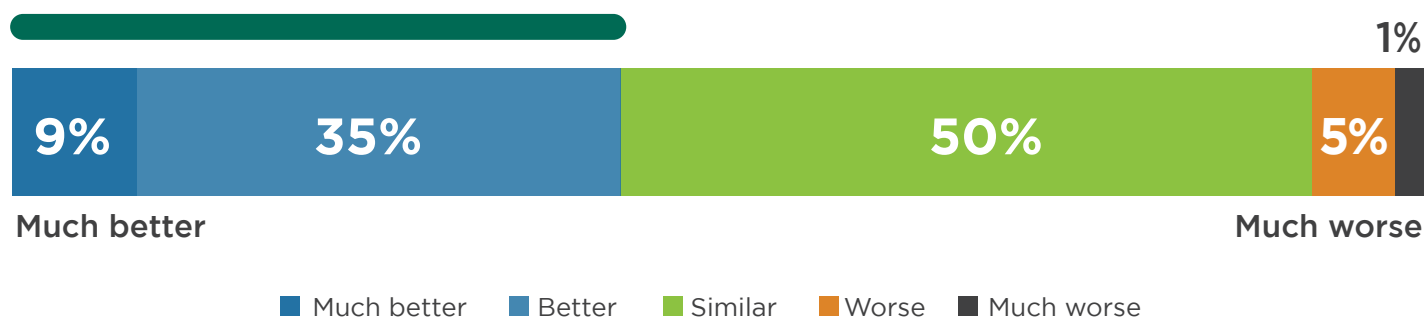
When asked how third-party security solutions compare to native cloud security platforms provided by the cloud operator, half of cybersecurity professionals think both perform similarly (50%). This is followed by 44% who think dedicated third-party security solutions perform better.

These findings suggest that there is a general belief among cybersecurity professionals that third-party security vendors can either provide similar or, in some cases, better cloud security compared to cloud vendors. This emphasizes the importance of evaluating security options and choosing the most appropriate solution for an organization's specific needs and requirements.

- How do you think cloud security from a 3rd-party security vendor compares with cloud security from a cloud vendor?

## 44%

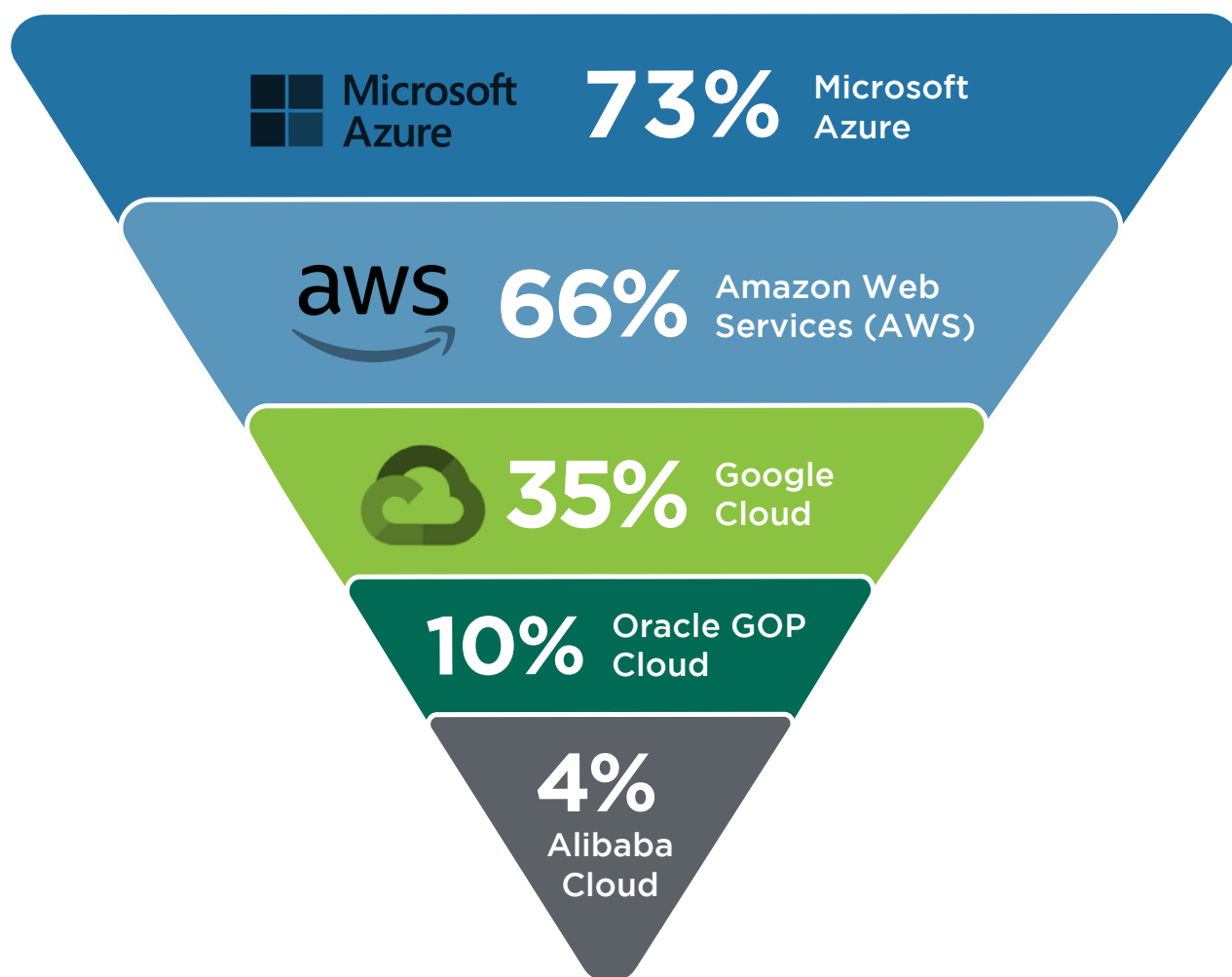
think that cloud security from an independent security vendor is better than cloud vendors



# Best Native Cloud Security

How do cybersecurity professionals rate the completeness of their cloud providers' native security? The majority of respondents believe Azure offers the most sufficient native cloud security controls and services (73%), reflecting high confidence in Microsoft's security features and capabilities. AWS is also highly regarded by respondents for its native cloud security controls (66%), demonstrating strong trust in Amazon's security offerings. Though less popular compared to Azure and AWS, a significant portion of respondents still consider Google Cloud's native security controls and services to be sufficient (35%).

- Which of the following platforms provide the most sufficient native cloud security controls and services?



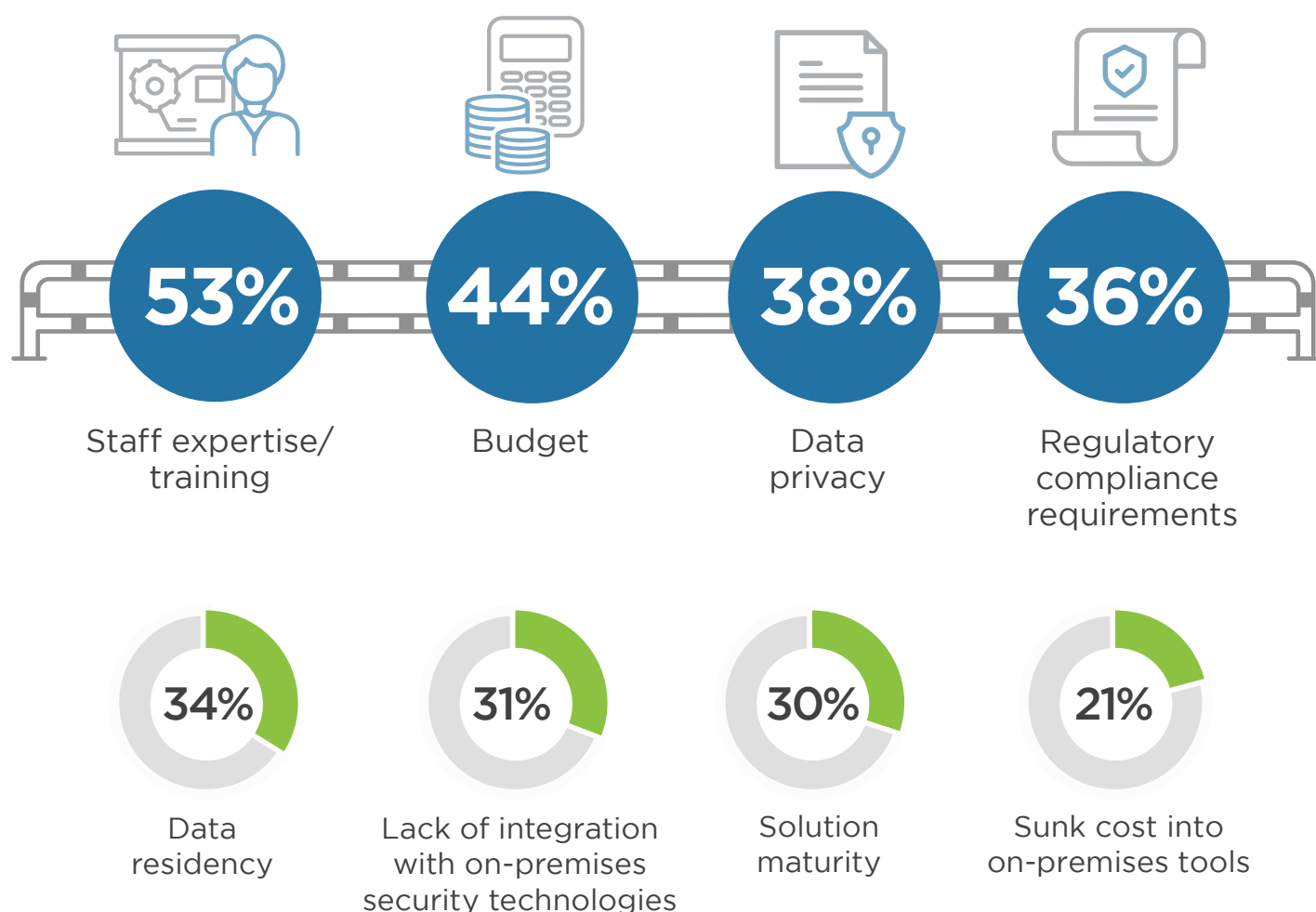
Other 4%

# Barriers to Cloud-Based Security

What are the biggest barriers that slow migration to cloud-based security? Interestingly, the biggest challenges organizations are facing are not primarily about security technology, but about people and processes. Lack of cybersecurity staff expertise and training (53%) continues to rank as the highest barrier to migrating to cloud-based security solutions. Organizations continue to face challenges in upskilling their teams and providing them with the necessary knowledge to effectively manage and secure cloud environments.

This is followed at a distance by budget challenges (44%) and data privacy issues (38%).

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

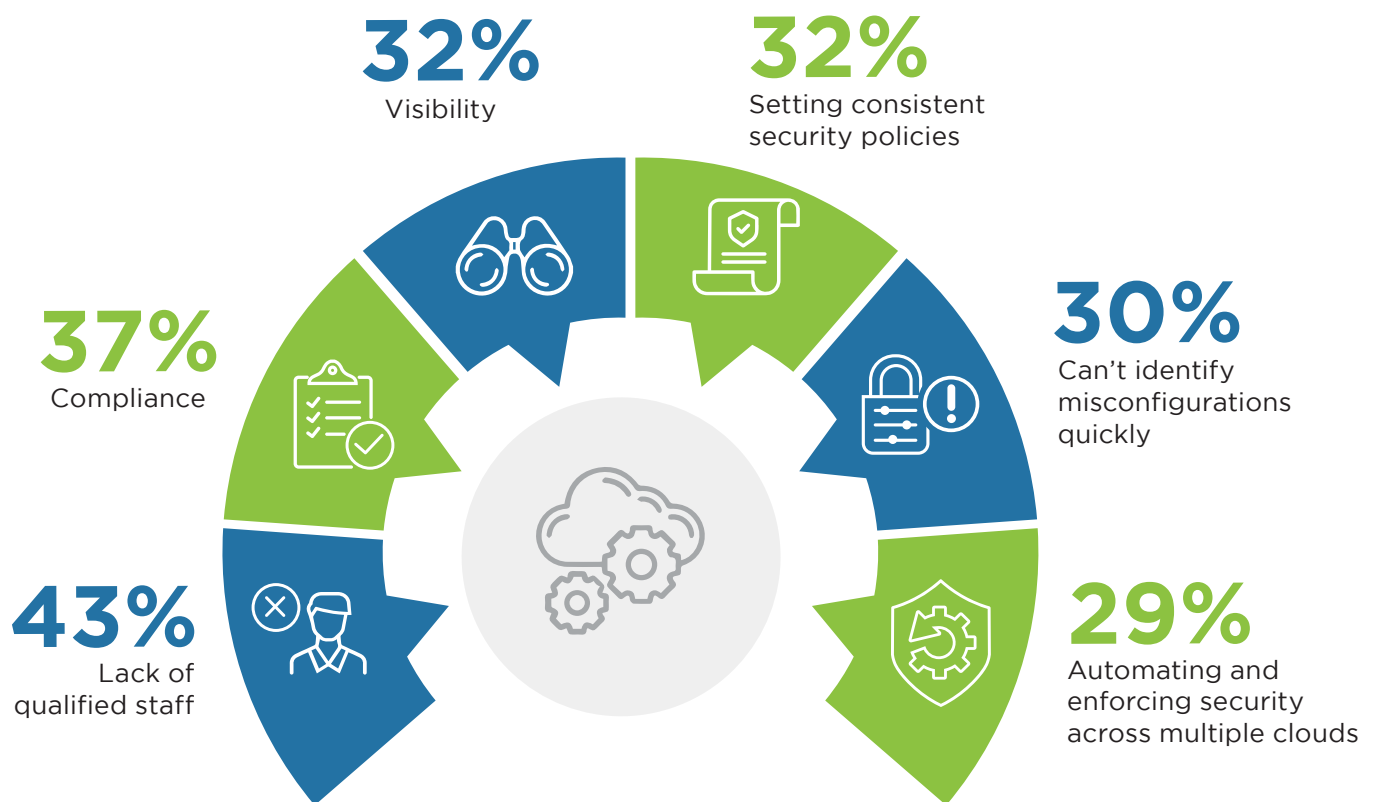


Integrity of cloud security platform (DDoS attack, breach) 19% | Limited control over encryption keys 18% | Scalability and performance 14% | Not sure/other 9%

# Operational Security Headaches

Overall, the key findings suggest that organizations face multiple challenges in securing their cloud workloads, including a shortage of skilled staff (43%), ensuring compliance (37%), and visibility into their infrastructure security (32%). Addressing these issues will require a combination of improved security tools and processes, and increased investment in cybersecurity training and workforce development.

## ► What are your biggest operational, day-to-day headaches trying to protect cloud workloads?



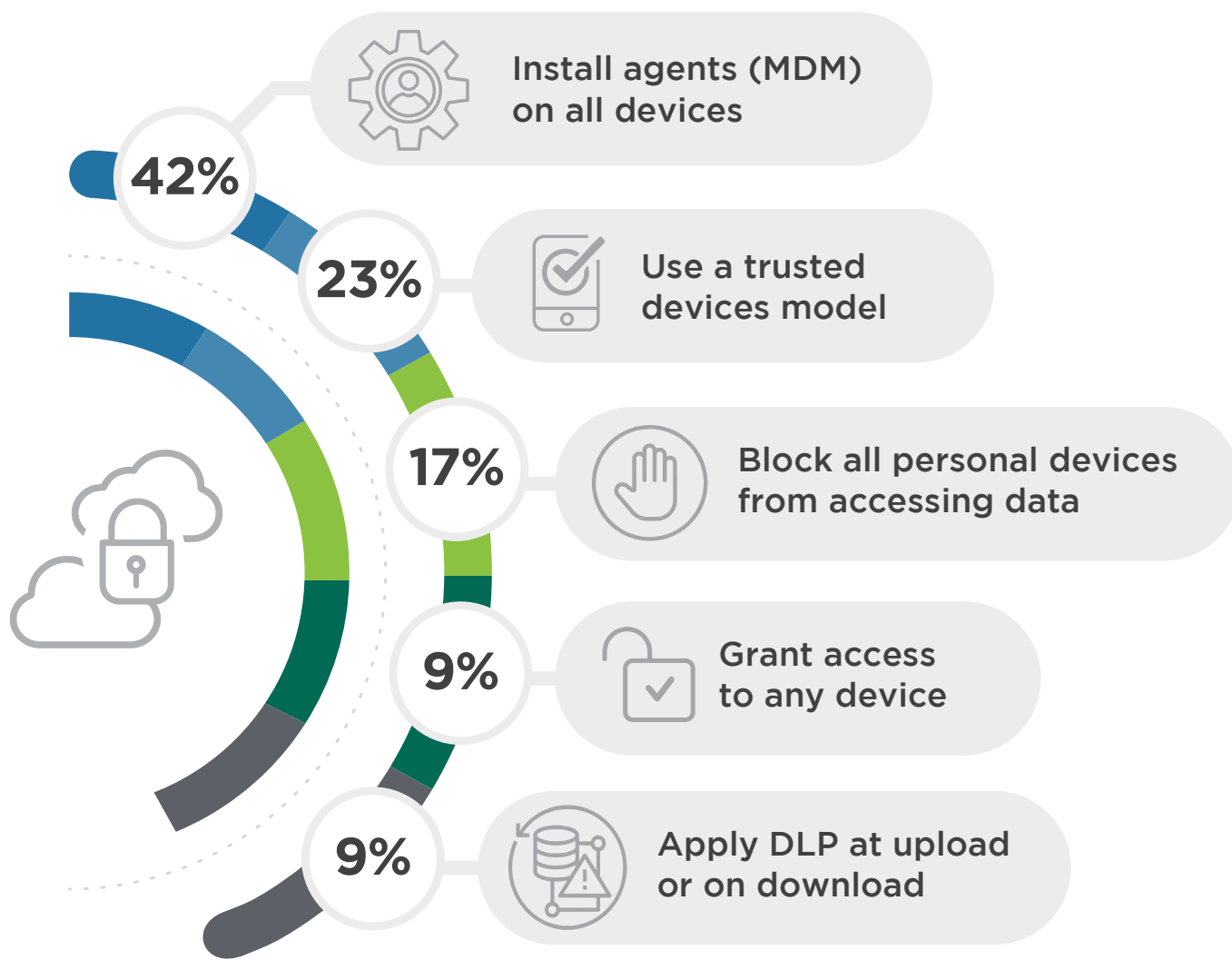


# Personal Device Security

Personal devices are a popular and important endpoint for employees accessing cloud data and services – but they are also a weak link. How do organizations protect cloud data that is accessed, used, and stored on personal devices?

The most common security measure is installation of MDM agents that monitor use of data and cloud services on personal devices (42%), followed by using trusted device models (23%). And, 17% of organizations don't even permit personal device access to sensitive cloud resources.

## ► What does your organization do for securing cloud data on employees' personal devices?



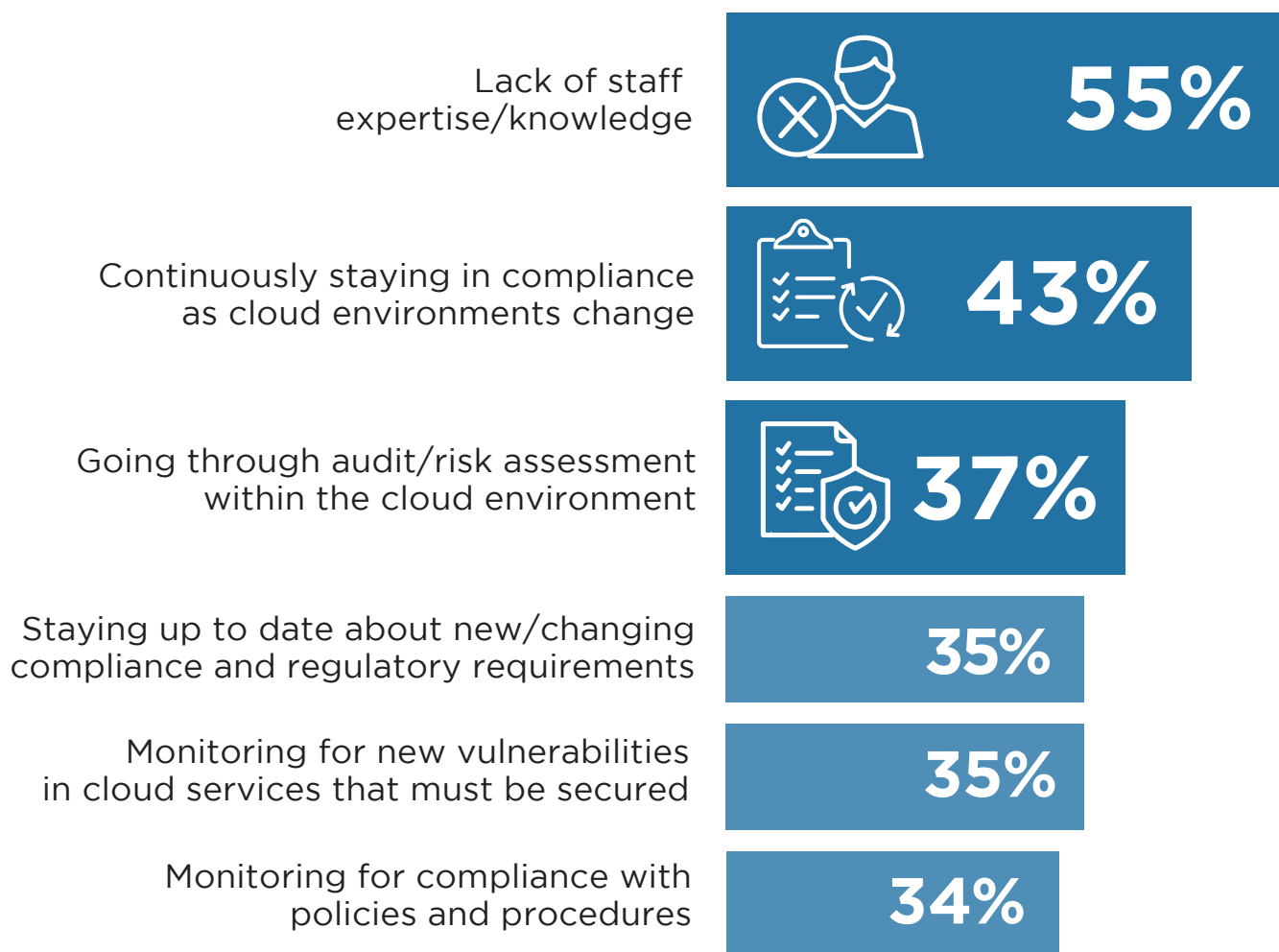
# Cloud Compliance Challenges

The top challenge faced by organizations in maintaining cloud compliance is the lack of staff expertise and knowledge (55%). Organizations struggle to find qualified personnel who can effectively manage and ensure compliance in cloud environments – this issue has been the top challenge for a number of years.

This is followed by the challenge of continuously staying in compliance as cloud environments change (43%) and performing regular audit/risk assessments (37%).

To overcome these challenges, organizations should invest in staff training and certification, develop effective compliance monitoring processes, and stay up-to-date on regulatory changes and emerging threats in the cloud environment.

## ► Which part of the cloud compliance process is the most challenging?

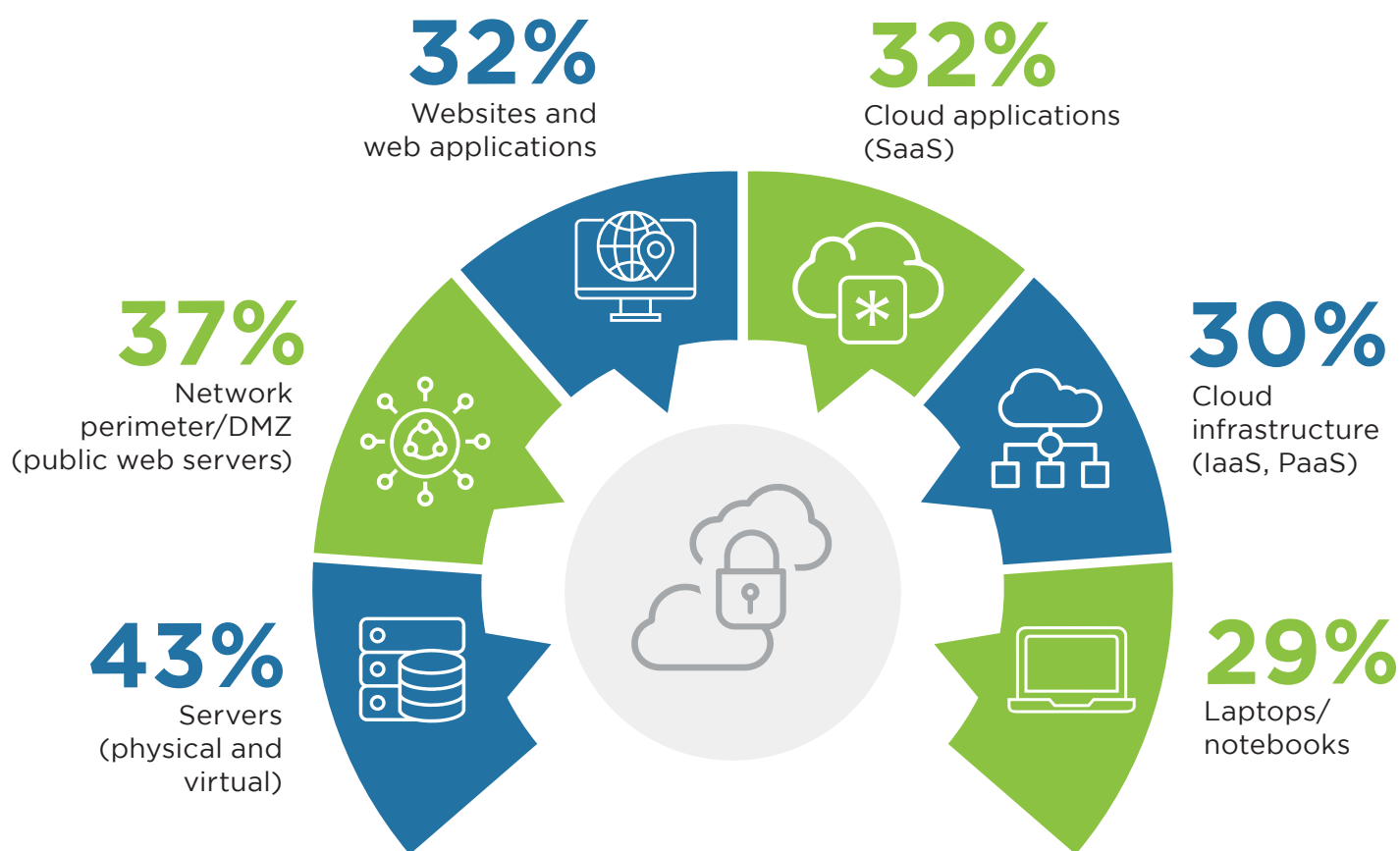


Scaling and automating compliance activities 24% | Data quality and integrity in regulatory reporting 22% | Not sure/other 7%

# Confidence in Security

In which components of their broader cloud environments are cybersecurity professionals most confident regarding their ability to secure in the cloud? Core cloud components such as servers (43%), network (37%), and web applications (32%) received the highest confidence scores, indicating that respondents feel more comfortable securing these components. Industrial control systems (ICS)/SCADA devices and Internet of Things (IoT) on the other hand show the lowest confidence levels among respondents, indicating these areas may require additional attention, education, and resources.

- Of the following components, which are you most confident in being able to secure in the cloud?



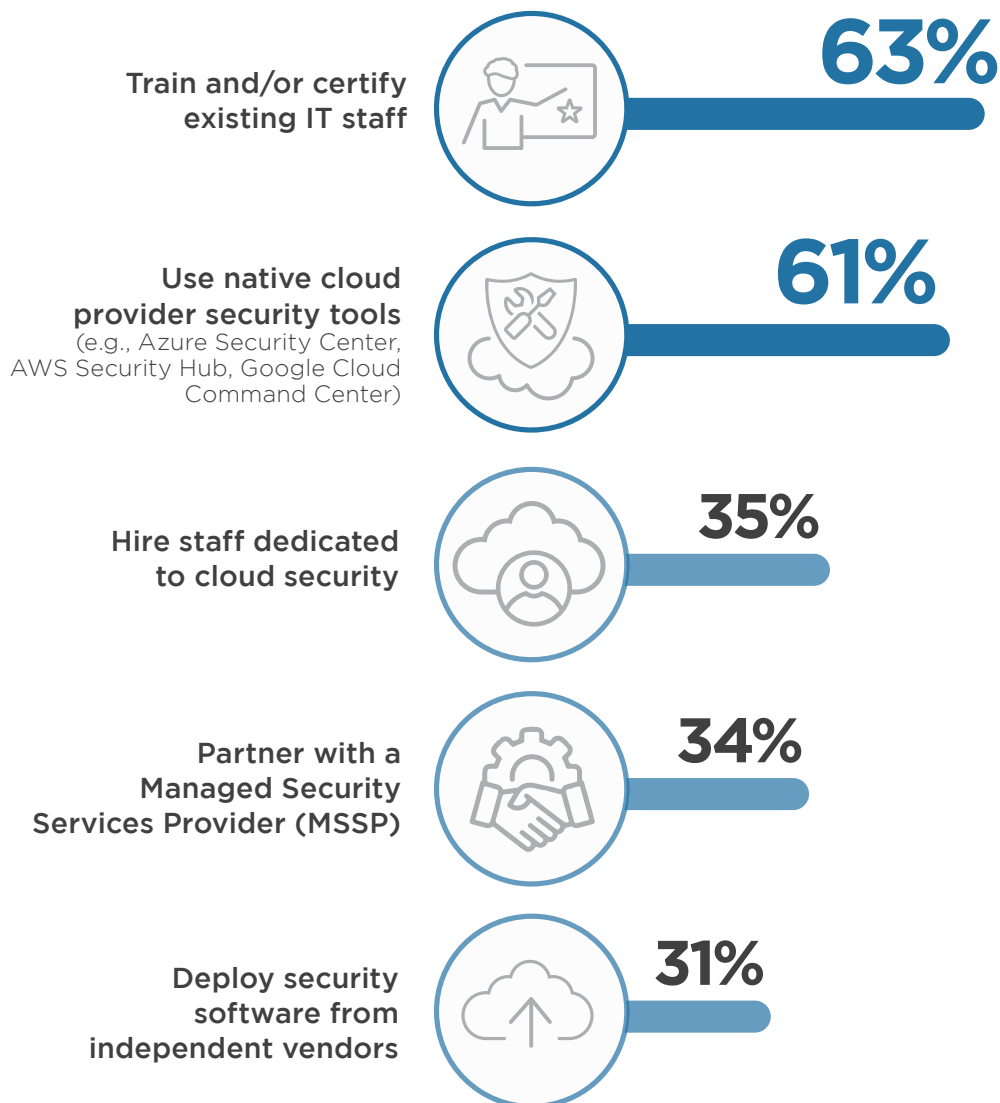
# Changing Security Needs

How do organizations respond to changing security needs? The most popular approach among organizations is to invest in training and certification for their existing IT and information security staff (63%). This helps to bridge the skills gap and empowers employees to better handle the unique security challenges that arise in the cloud environment.

This is closely followed by using native cloud provider security tools (61%) – perhaps indicating cloud providers adapt their platforms in the face of changing security risks. Hiring new cloud security staff only follows at a distant third spot (35%).

By investing in training and certification for their IT/IS staff, organizations can better handle the evolving security needs of their cloud environments and make the most of native cloud provider security tools.

## ► When moving to the cloud, how do you handle your changing security needs?



Other 2%

# Cloud Business Outcomes

The survey results reveal several business outcomes organizations have realized by moving to the cloud, highlighting the diverse benefits of cloud adoption. Organizations rank responsiveness to customer needs (52%) as the most common beneficial outcome they received by moving to the cloud. This is followed by accelerated time to market (48%). Organizations also see a degree of risk reduction (42%), closely followed by reduced cost (41%).

These results demonstrate that cloud adoption not only drives cost savings and operational efficiency, but also fosters innovation, agility, and market competitiveness.

## ► What business outcomes have you realized by moving to the cloud?

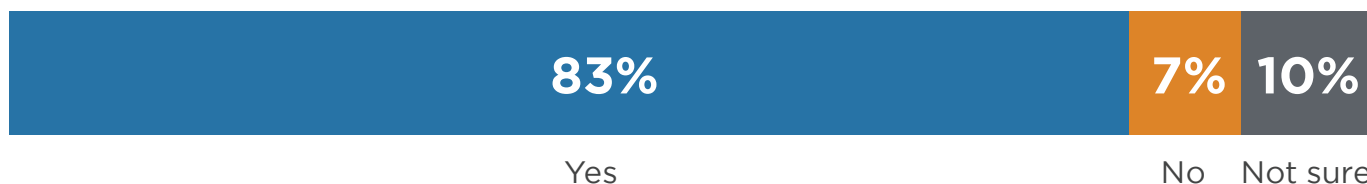


Other 7%

# Cloud Security Training

The survey results highlight the strong demand for cloud security training and certifications among respondents. A large majority of respondents believe that they or their team would benefit from cloud security training and/or certifications (83%), indicating that there is a significant need for skill development in order to effectively operate in cloud environments.

- ▶ **Do you think you or your team needs cloud security training and/or certification(s) to be better equipped to operate in cloud environments?**



We asked cybersecurity professionals whether they have a preference for vendor-specific or vendor-neutral cloud security certifications. The results indicate that a balanced approach to cloud security certifications, incorporating both vendor-specific and vendor-neutral credentials, is preferred by the majority of respondents (51%). This approach ensures that professionals are equipped with a comprehensive skill set, enabling them to effectively navigate and secure diverse cloud environments.

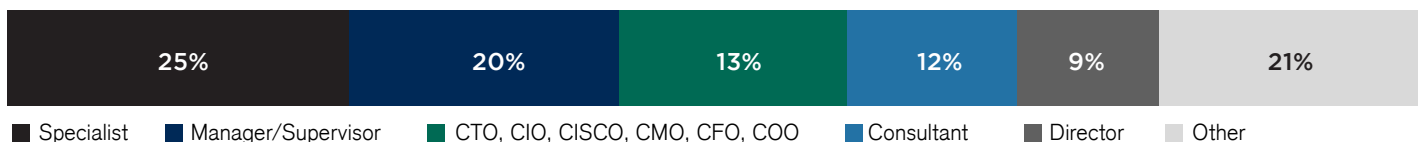
- ▶ **When considering cloud security certification for yourself and/or your team, do you consider mostly vendor-specific certifications or vendor-neutral certifications?**



# Methodology & Demographics

The 2023 Cloud Security Report is derived from an extensive survey of 823 cybersecurity professionals, conducted in March 2023. 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.

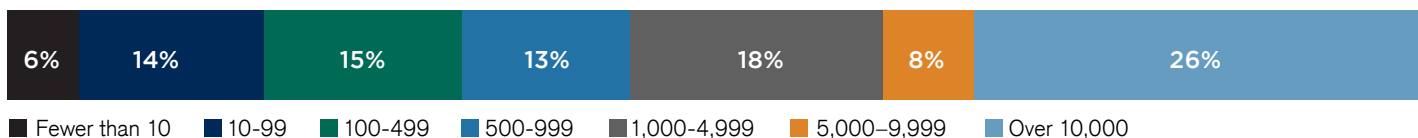
## CAREER LEVEL



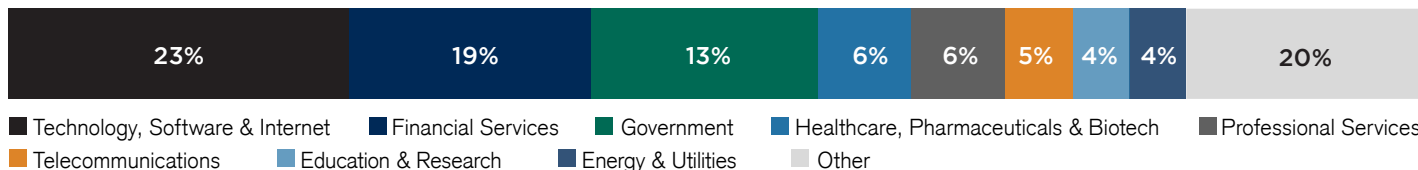
## DEPARTMENT



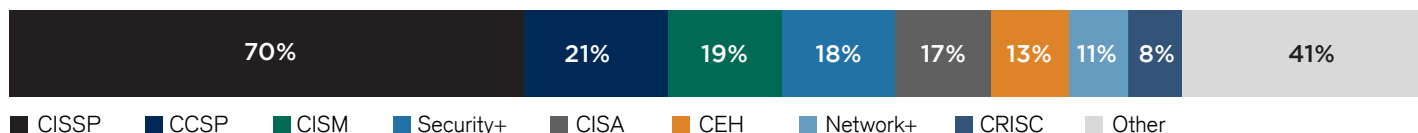
## COMPANY SIZE



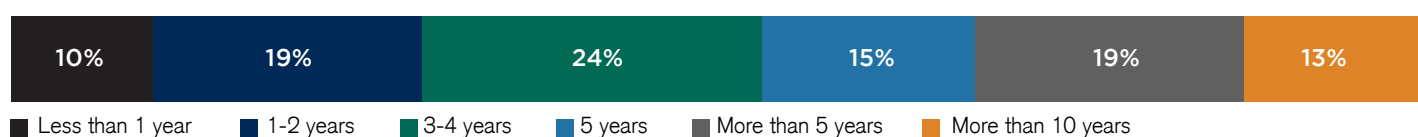
## INDUSTRY



## SECURITY CERTIFICATIONS HELD



## YEARS OF SECURITY EXPERIENCE





# How to Address the Cybersecurity Talent Gap

Based on the findings of the 2023 Cloud Security Report, the ongoing talent and skills gap is a significant challenge for all organizations. Here are practical ways to overcome this challenge:



**Invest in training and certifying existing IT staff in cloud security**, such as the Certified Cloud Security Professional (CCSP), as continuous learning can help them adapt to the ever-evolving cloud environment.



**Hire dedicated staff with cloud security expertise**, and prioritize acquiring talent with a diverse range of skills and experience (especially with recognized certifications like CCSP or CISSP, as these professionals demonstrate a high level of knowledge and commitment to industry best practices).



**Foster a culture of collaboration and knowledge-sharing between teams**, as this can help in building internal expertise and keeping everyone up to date with the latest security trends.



**Consider a mix of vendor-specific and vendor-neutral certifications for your team**, ensuring that they have both in-depth knowledge of specific platforms and a broader understanding of cloud security principles.



**Collaborate with Managed Security Services Providers (MSSPs) and leverage security-as-a-service providers**, to fill any immediate gaps in expertise and resources, while continuously working to develop your organization's internal capabilities.

By addressing the cybersecurity talent and skills gap through these measures and partnering with [ISC2](#), organizations can better protect their cloud environments and maintain a strong security posture in the face of growing threats.



**Certified Cloud  
Security Professional**

ISC2 Certification

# Take Your Career Higher into the Cloud

## Build the confidence to succeed in cloud security

As more critical data and assets move to the cloud, they've become prime targets for cybercriminals. Organizations worldwide need cloud security professionals who understand the evolving complexities to identify and mitigate security risks.

CCSP certification, the global gold standard in cloud security, puts you on a path to rise higher in your career.

### Take the first step to CCSP Certification

[Join ISC2 as a Candidate](#). Sign up now and gain access to exclusive benefits, including **20% off Official ISC2 Training** so you can start preparing for the CCSP exam. More benefits include:

- Free training for ISC2 Certified in Cybersecurity certification
- Discounted learning resources
- ISC2 Security Congress annual conference
- Industry event discounts
- ISC2 Local Chapter – join or start one

Your first year is free — no cost to you.\*

**Get Started at [isc2.org/candidate](https://isc2.org/candidate)**

*\*If you choose to renew after the first year, U.S. \$50 due annually.*



**CCSP is named  
among the top  
cloud certifications**

*by SC Magazine*



ISC2 is an international nonprofit membership association 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 part of a holistic, pragmatic approach to security. In 2015, ISC2 launched the Certified Cloud Security Professional (CCSP®) for security professional whose day-to-day responsibilities involve procuring, securing and managing cloud environments or purchased cloud services. Our association of candidates, associates and members, nearly 365,000 strong, 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 supported 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](http://www.isc2.org), follow us on [Twitter](#) or connect with us on [Facebook](#) and [LinkedIn](#).



# Cybersecurity

---

## I N S I D E R S

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](mailto:info@cybersecurity-insiders.com) or visit [cybersecurity-insiders.com](https://www.cybersecurity-insiders.com)