

2022

Cybersecurity  
INSIDERS

# CLOUD SECURITY REPORT

(ISC)<sup>2</sup><sup>®</sup>

# INTRODUCTION

Cloud adoption is continuing to increase at a high rate. However, cloud technology is becoming more complex, and finding people with the right skills to ensure workloads in the cloud are deployed and secured continues to be a top concern.

This year's Cloud Security Report is one of the most comprehensive studies on cloud trends and the role security plays as organizations accelerate their transformation to the cloud.

## Key findings include:

- Today, 39% of respondents have more than half of their workloads in the cloud, while 58% plan to make this shift in the next 12-18 months.
- More than three-quarters (76%) of organizations are utilizing two or more cloud providers. Most organizations (72%) have a hybrid or multi-cloud deployment strategy.
- 78% claim traditional security solutions either don't work at all or have limited functionality in cloud environments.
- 93% of those polled are moderately to extremely concerned about the massive skills shortage of qualified cybersecurity professionals.
- 52% said the main barrier to migrating to cloud-based security solutions is lack of staff expertise and 57% said this lack of staff expertise makes cloud compliance challenging .
- Lack of staff expertise even prevents 40% from adopting cloud solutions for their organizations. The good news is that 83% believe their teams would benefit from cloud security training and/or certification. 56% feel that cloud security skills are the most important expertise their organizations need.

We would like to thank [\(ISC\)<sup>2</sup>](#) 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 COMPLEXITY RISING**

---

# WORKLOADS IN THE CLOUD

Organizations continue to shift workloads to the cloud at a rapid pace. Today, 39% of respondents have more than half of their workloads in the cloud, while 58% plan to make this shift in the next 12-18 months.

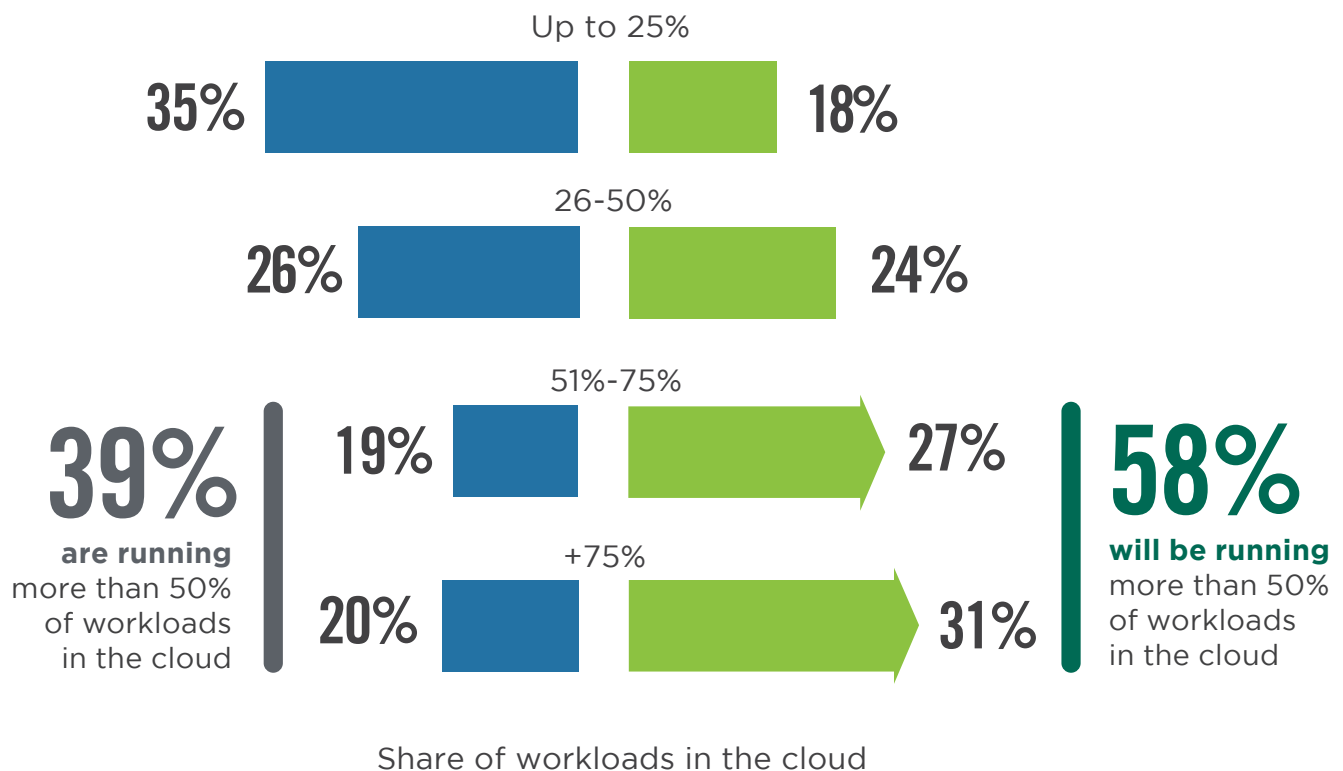
► What percentage of your workloads are in the cloud today?

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



TODAY

NEXT 12-18 MONTHS

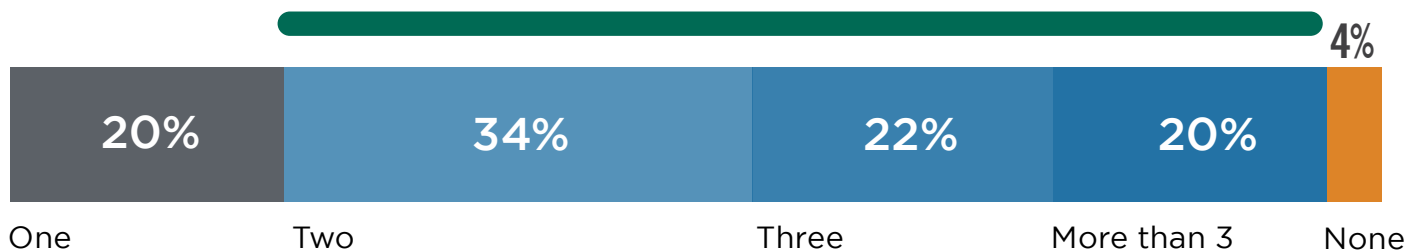


# CLOUD PROVIDERS

More than three-quarters of organizations (76%) are utilizing two or more cloud providers, which means an increase in complexity, security risk and opportunities for errors. Only a few companies (20%) rely on a single cloud deployment for their business needs.

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

**76%** use two or more cloud providers



# CLOUD DEPLOYMENT STRATEGIES

Most organizations (72%) are pursuing a hybrid or multi-cloud strategy for integration of multiple services, scalability, or business continuity reasons. While overall beneficial, this strategy also increases the complexity of managing multiple environments.

## ► What is your primary cloud deployment strategy?

39%



### **MULTI-CLOUD**

(e.g., multiple providers without integration)

33%



### **HYBRID**

(e.g., integration between private and public clouds)

27%



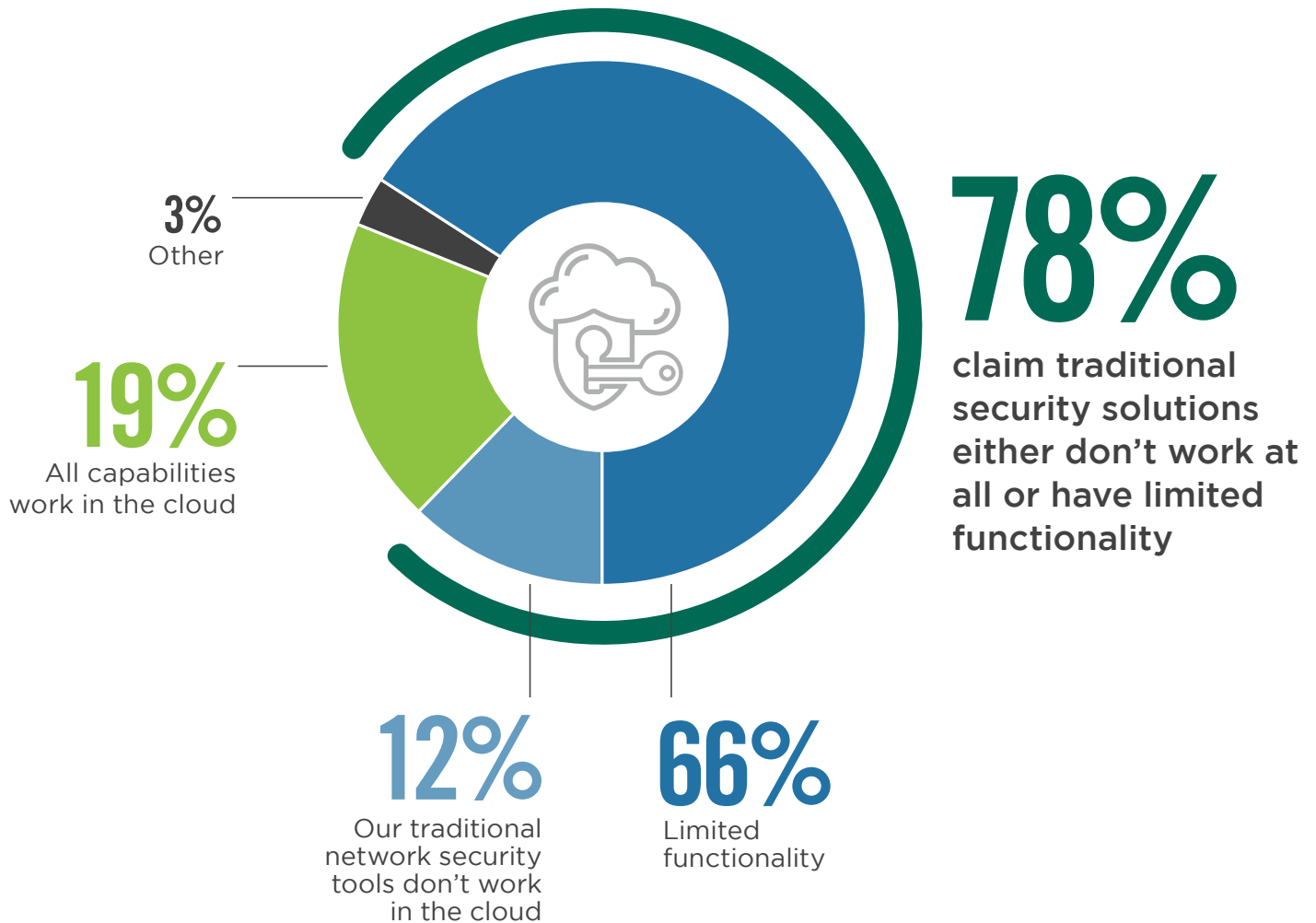
### **SINGLE CLOUD**

Other 1%

# TRADITIONAL TOOLS IN THE CLOUD

The dynamic, distributed, and virtual nature of cloud computing presents unique security challenges that most legacy security tools are simply not designed to address. Seventy-eight percent of organizations confirm that traditional security solutions either don't work at all in their cloud environments or have only limited functionality.

## ► How well do your traditional network security tools/appliances work in cloud environments?



---

**CYBER PROS  
ARE NEEDED**

---

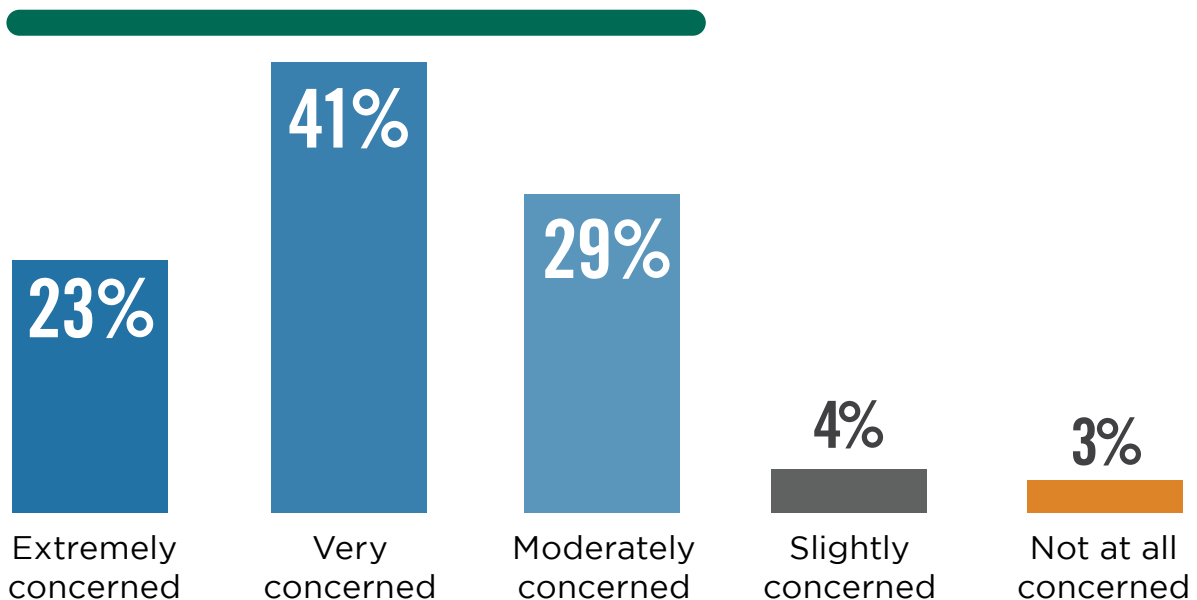
# SKILLS SHORTAGE CONCERN

Virtually all organizations in our survey (93%) are moderately to extremely concerned about the massive skills shortage of qualified cybersecurity professionals. Together, the Cybersecurity Workforce Estimate and Cybersecurity Workforce Gap suggest the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets.

- ▶ **Together, the Cybersecurity Workforce Estimate and Cybersecurity Workforce Gap suggest the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets. How concerned are you about the industry wide skills shortage of qualified cybersecurity professionals?**



of organizations are moderately to extremely concerned about the shortage of qualified cybersecurity professionals



# MULTI-CLOUD SECURITY CHALLENGES

When asked about the biggest challenges in securing multi-cloud environments, organizations emphasized the significant lack of security skills (61%), followed by data protection (53%) and understanding how different security solutions fit together (51%).

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



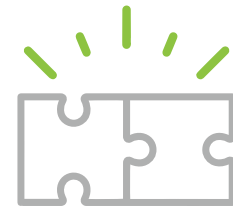
**61%**

Having the right skills to deploy and manage a complete solution across all cloud environments



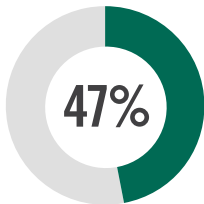
**53%**

Ensuring data protection and privacy for each environment

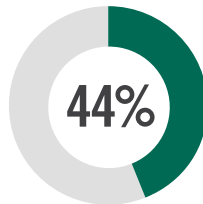


**51%**

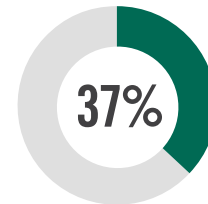
Understanding how different solutions fit together



Loss of visibility and control



Understanding service integration options



Keeping up with the rate of change

Selecting the right set of services 36% | Managing the costs of different solutions 36% | Providing seamless access to users based on their credentials 34% | Other 3%

# OPERATIONAL SECURITY HEADACHES

Cybersecurity professionals are faced with numerous complications when it comes to protecting cloud workloads. Lack of qualified security staff (44%) remains number one on the list of day-to-day headaches, followed by compliance (42%) and visibility into infrastructure security (36%).

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



44%

Lack of qualified staff



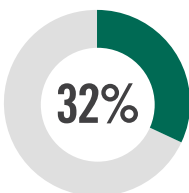
42%

Compliance

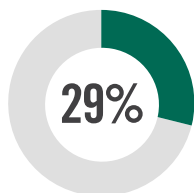


36%

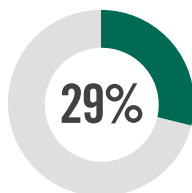
Visibility into infrastructure security



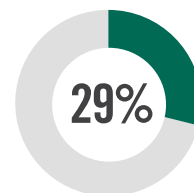
Can't identify misconfigurations quickly



Setting consistent security policies



Complex cloud-to-cloud/  
cloud to on-premises security rule matching



Implementing continuous and automated security controls in the cloud

Automatically enforcing security across multiple clouds 28% | Remediating threats 28% | Securing traffic flows 28% | Security can't keep up with the pace of changes to new/existing applications 27% | Securing access from personal and mobile devices 27% | Setting the correct user access privileges 27% | Lack of integration with on-premises security technologies 25% | Understanding network traffic patterns 25% | Justifying more security expenditure 24% | No automatic discovery/visibility/control to infrastructure security 23% | Reporting security threats 23% | Lack of feature parity with on-premises security solution 13% | No flexibility 6% | Not sure/other 11%

# BIGGEST SECURITY THREATS

We asked cybersecurity professionals about the cloud security threats that most concern them. Misconfiguration of cloud security remains the biggest cloud security risk according to 62% of cybersecurity professionals in our survey. This is followed by insecure interfaces/APIs (54%), exfiltration of sensitive data (51%) and unauthorized access (50%).

## ► What do you see as the biggest security threats in public clouds?



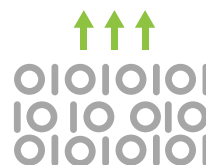
62%

Misconfiguration of the cloud platform/wrong setup



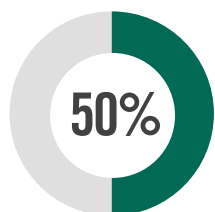
54%

Insecure interfaces/APIs

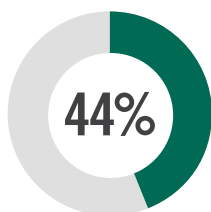


51%

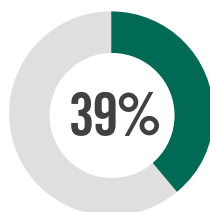
Exfiltration of sensitive data



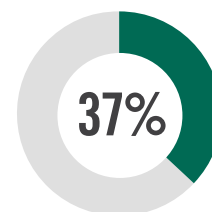
50%  
Unauthorized access



44%  
Hijacking of accounts, services, or traffic



39%  
External sharing of data



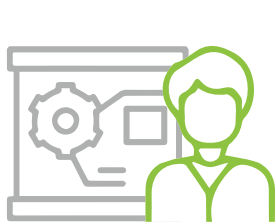
37%  
Foreign state-sponsored cyber attacks

Malware/ransomware 36% | Malicious insiders 34% | Denial of service attacks 33% | Cloud cryptojacking 20% | Theft of service 18% | Lost mobile devices 10% | Don't know/other 8%

# BARRIERS TO CLOUD-BASED SECURITY ADOPTION

Cloud-based security solutions offer significant advantages, yet barriers to cloud adoption still exist. The survey reveals that the biggest challenges organizations are facing are not primarily about technology, but people and processes. Staff expertise and training (52%) continues to rank as the highest barrier, followed by budget challenges (44%) and data privacy issues (40%).

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



52%

Staff expertise/  
training



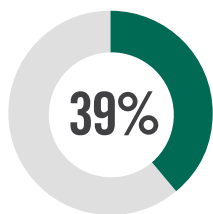
44%

Budget

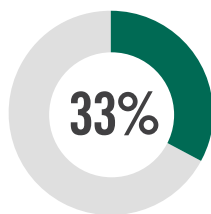


40%

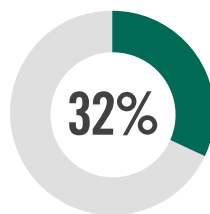
Data  
privacy



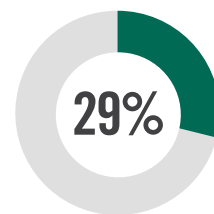
Regulatory  
compliance  
requirements



Solution  
maturity



Data  
residency



Lack of integration  
with on-premises  
security technologies

Sunk cost into on-premises tools 20% | Limited control over encryption keys 19% | Integrity of cloud security platform (DDoS attack, breach) 18% | Scalability and performance 14% | Not sure/other 8%

# CLOUD COMPLIANCE CHALLENGES

When asked about the most challenging aspects of the compliance process, organizations report that lack of staff expertise/knowledge (57%) ranks highest. This is followed by continuously staying in compliance as cloud environments change (44%), and going through audit/risk assessments (39%).

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



# 57%

Lack of staff expertise/knowledge



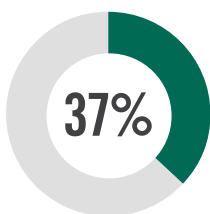
# 44%

Continuously staying in compliance as cloud environment changes

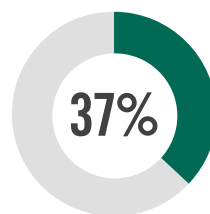


# 39%

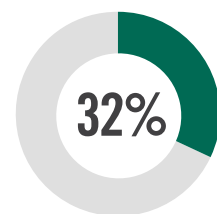
Going through audit/risk assessment within the cloud environment



Monitoring for compliance with policies and procedures



Monitoring for new vulnerabilities in cloud services that must be secured



Staying up to date about new/changing compliance and regulatory requirements

Applying/following the shared responsibility model 26% | Scaling and automating compliance activities 25% | Data quality and integrity in regulatory reporting 20% | Not sure/other 6%

# BARRIERS TO CLOUD ADOPTION

Among the most critical barriers to cloud adoption, organizations report the perennial lack of qualified cybersecurity staff (40%) as the biggest impediment to faster adoption. This is followed by legal and regulatory compliance (33%) and data security issues (31%).

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



# 40%

Lack of staff resources or expertise



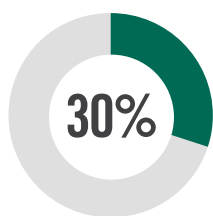
# 33%

Legal and regulatory compliance

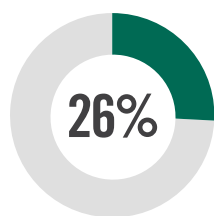


# 31%

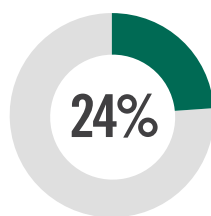
Data security, loss and leakage risks



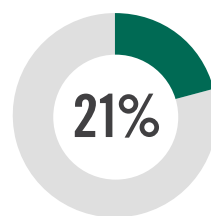
Integration with existing IT environment



Fear of vendor lock-in



General security risks



Loss of control

Internal resistance and inertia 20% | Cost/lack of ROI 18% | Lack of budget 18% | Complexity managing cloud deployment 18% | Lack of transparency and visibility 16% | Lack of maturity of cloud service models 15% | Billing & tracking issues 11% | Lack of management buy-in 11% | Dissatisfaction with cloud service offerings/performance/pricing 10% | Lack of support by cloud provider 9% | Performance of apps in the cloud 9% | Lack of customizability 7% | Availability 6% | Other 6%

# PATHS TO STRONGER CLOUD SECURITY

When asked about their responses to ever-changing security needs, organizations rank training and certifying of IT security staff as the top tactic (64%). This is followed by using native cloud provider security tools (63%).

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



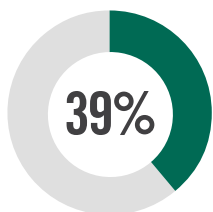
64%

Train and/or certify existing IT staff

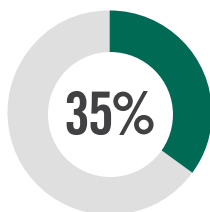


63%

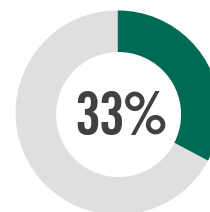
Use native cloud provider security tools  
(e.g., Azure Security Center, AWS Security Hub, Google Cloud Command Center)



Hire staff dedicated to cloud security



Partner with a Managed Security Services Provider (MSSP)



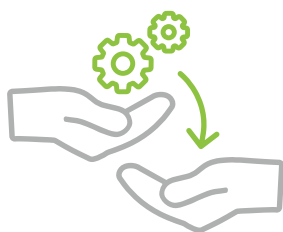
Deploy security software from independent vendors

Other 1%

# HUMAN CAPITAL MANAGEMENT

Organizations have a variety of tactics at their disposal for managing human capital as it relates to improving cloud and security competencies. The most popular tactics, born out of necessity due to the unavailability of qualified security professionals in the labor market, focus on the transition of skills of existing IT professionals (61%) combined with an evaluation of present qualifications and needs for coaching and training (60%).

## ► How are you approaching human capital management in addressing your cloud infrastructure needs and security competence?



61%

Transition skills of existing teams and individuals



60%

Evaluate team and individual qualifications and needs for coaching and training



36%

Hire new managers, specialists, and teams



21%

Reduce or reassign staff without required experience or willingness to adapt and learn

Other 4%

# SECURITY READINESS

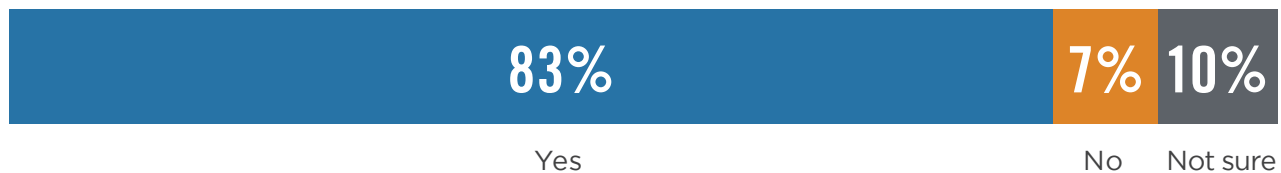
We asked organizations how they would rate their overall security readiness. A majority of organizations (70%) rate their security readiness as average or below average. Only 30% say they are above average.

## ► How would you rate your team's overall security readiness?



Of those rating their overall security readiness as average or below average, 83% believe their teams would benefit from cloud security training and/or certification.

## ► Do you think you or your team need cloud security training and/or certification(s) to be better equipped to operate in cloud environments?



# SECURITY TRAINING AND CERTIFICATION

The continuing shortage of qualified cybersecurity staff and the lack of security awareness and skills among all employees remain as the top security challenges for organizations. To alleviate this shortage, cybersecurity professionals agree that six out of ten employees would benefit from security training and/or certification for their jobs.

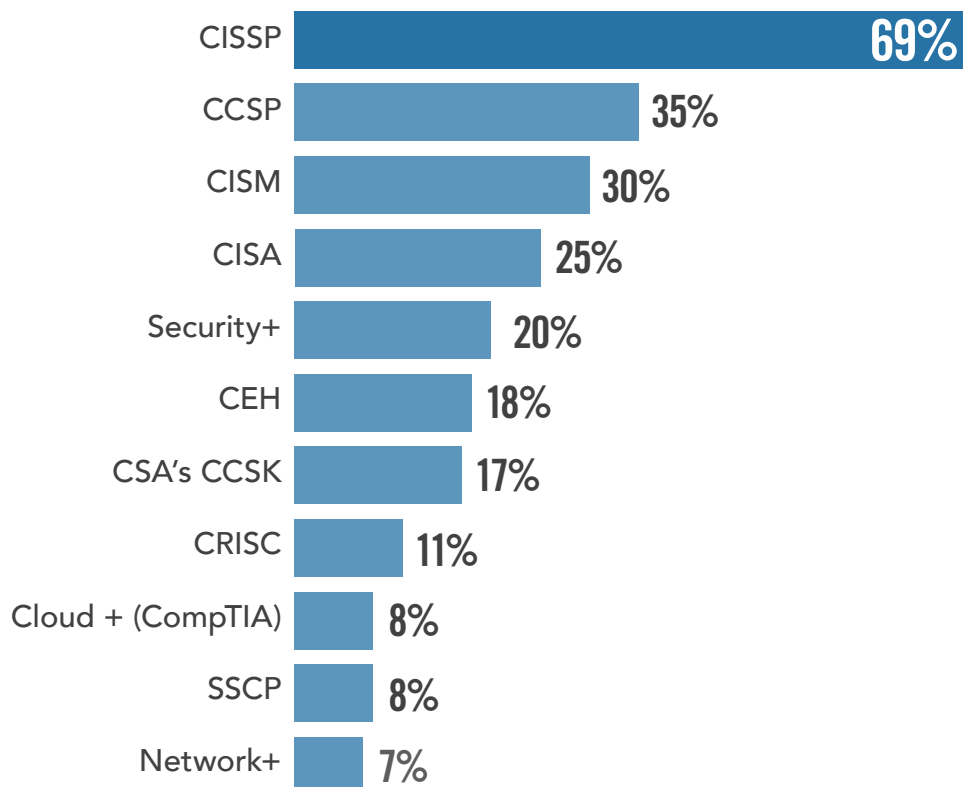
## ► What percentage of your employees would benefit from security training and/or certification for their job?



**61%**

of employees would benefit from security training and/or certification for their job

## ► Which of the following certifications does your employer require you or your team to have?



# SECURITY SKILLS

When asked about the most critical security skills organizations are requiring, 58% prioritize incident response skills, alongside cloud security skills (56%) and knowledge of critical business processes (52%).

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



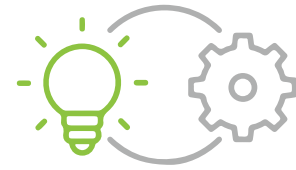
**58%**

Incident response



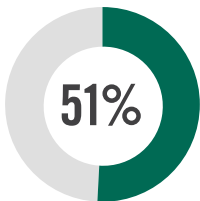
**56%**

Cloud platform specific security tooling knowledge

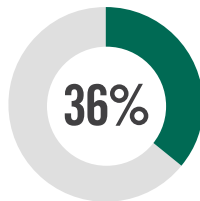


**52%**

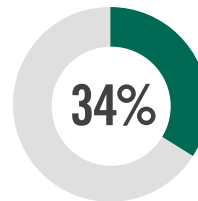
Knowledge of critical (internal) business processes



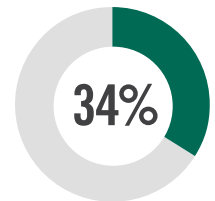
51%  
Knowledge of normal network and system operations to detect abnormal behaviors



36%  
Reporting/writing skills



34%  
Intelligence analysis skills



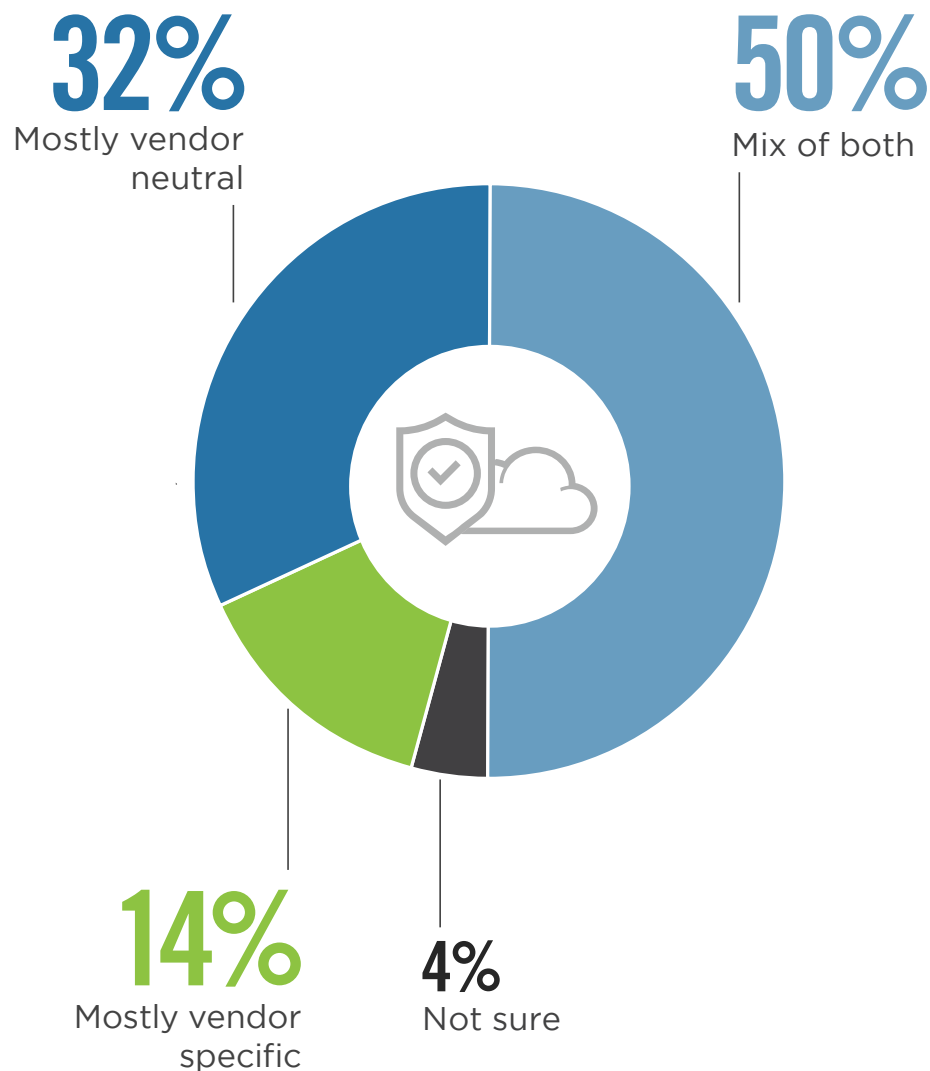
34%  
Presentation/oral communications skills

Identifying social engineering/phishing 34% | Familiarity with commercial tools and feeds 28% | Malware analysis skills 27% | Ability to write correlation rules to link security events 25% | Knowledge of adversaries and campaigns 25% | Other 3%

# VENDOR CERTIFICATIONS

We asked cybersecurity professionals whether they have a preference for vendor-specific or vendor-neutral cloud security certifications. Eighty-two percent of organizations prefer a mix of vendor-specific and vendor-neutral approaches or mostly vendor-neutral certifications. Only a minority of organizations in the survey prefer vendor-specific cloud security certifications (14%).

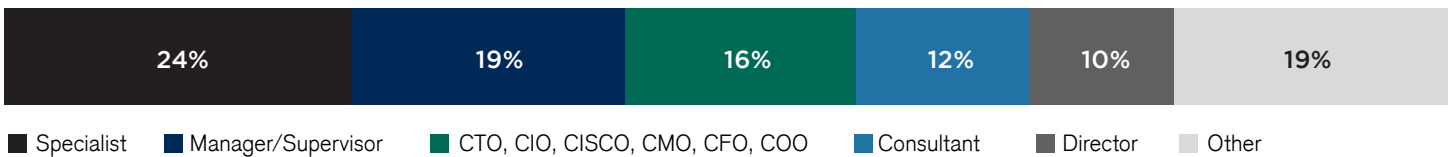
- ▶ **When considering cloud security certification for yourself and/or your team, do you consider mostly vendor-specific certifications or vendor-neutral certifications?**



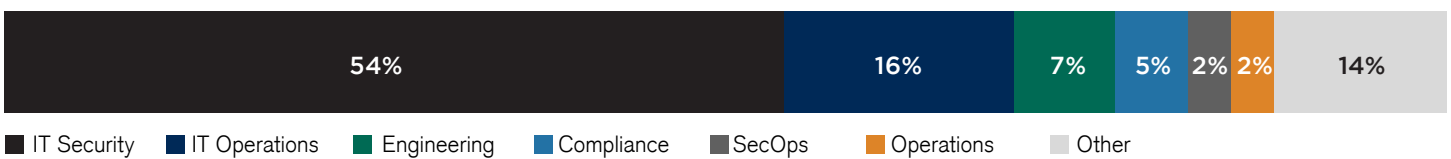
# METHODOLOGY & DEMOGRAPHICS

The 2022 Cloud Security Report is based on a comprehensive survey of 823 cybersecurity professionals conducted in March 2022, to uncover how cloud user organizations are responding to security threats in the cloud, and what training, certifications, and best practices IT cybersecurity leaders are prioritizing in their move to the cloud. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

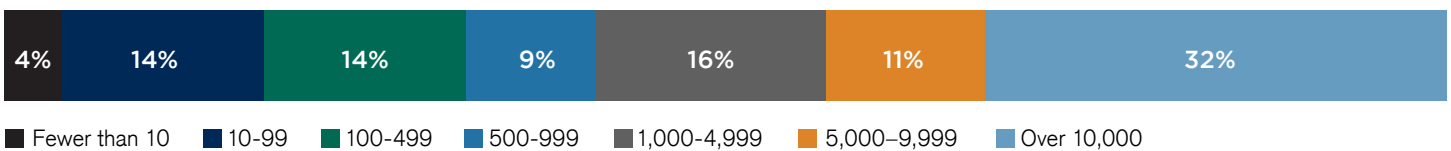
## CAREER LEVEL



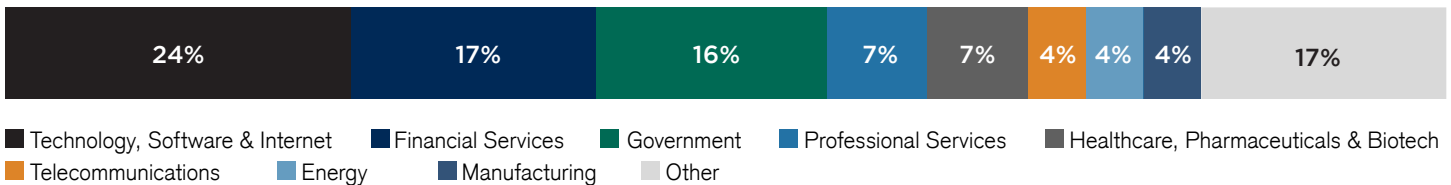
## DEPARTMENT



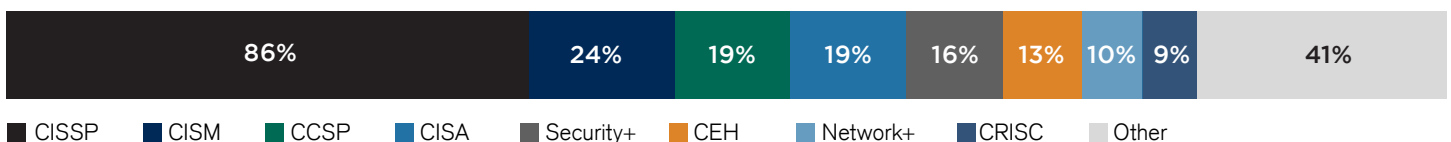
## COMPANY SIZE



## INDUSTRY



## SECURITY CERTIFICATIONS HELD



# Are You Staying Ahead of Emerging CLOUD SECURITY TRENDS?



**93%** of organizations are moderately to extremely concerned about the shortage of qualified cybersecurity professionals.



**83%** of survey respondents indicated they or their team need cloud security training and/or certification(s) to be better equipped to operate in cloud environments.

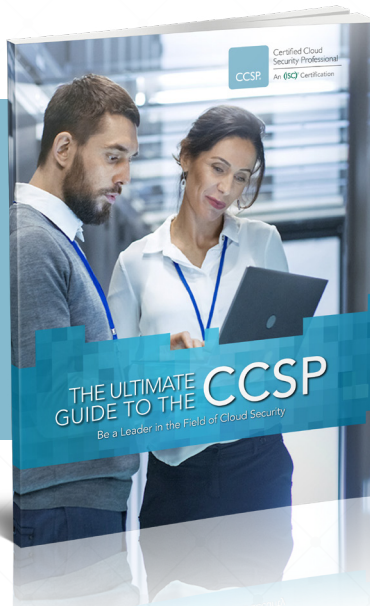
Respondents indicated that **lack of qualified staff** was the main barrier and challenge for:

Cloud Compliance **57%**

Migrating to Cloud-based Security Solutions **52%**

Cloud Adoption **40%**

Get the  
**ULTIMATE GUIDE**  
to the Ultimate Cloud  
Security Certification



**Get Your Guide**

#### Exclusive Features:

- Fast facts about CCSP
- Benefits of CCSP certification
- CCSP Exam Overview
- Training and Self-Study Resources
- Pathway to Certification



CCSP tops "The Next Big Thing" list as the #1 certification survey respondents plan to earn in 2022.



Certified Cloud  
Security Professional  
An (ISC)<sup>2</sup> Certification



(ISC)<sup>2</sup> 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, (ISC)<sup>2</sup> offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. In 2015, (ISC)<sup>2</sup> launched the Certified Cloud Security Professional (CCSP®) credential for security professionals whose day-to-day responsibilities involve procuring, securing, and managing cloud environments or purchased cloud services. It is now our fastest growing certification. Our membership, more than 168,000 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 (ISC)<sup>2</sup>, 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 is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

**For more information please visit  
[www.cybersecurity-insiders.com](http://www.cybersecurity-insiders.com)**