2019

Cybersecurity INSIDERS

CLOUD SECURITY REPORT

(ISC)²®

INTRODUCTION

Organizations continue to adopt cloud computing at a rapid pace to benefit from the promise of increased efficiency, better scalability, and improved agility.

While cloud service providers like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) continue to expand security services to protect their evolving cloud platforms, it is ultimately the customers' responsibility to secure their data within these cloud environments.

The 2019 Cloud Security Report highlights what is and what is not working for security operations teams in securing their cloud data, systems, and services in this shared responsibility model. The results are a continuation of past challenges:

- The top cloud security concern of cybersecurity professionals is data loss and leakage (64%).
- Unauthorized access through misuse of employee credentials and improper access controls (42%) takes the number one spot in this year's survey as the single biggest perceived vulnerability to cloud security, tied with insecure interfaces and APIs (42%). This is followed by misconfiguration of the cloud platform (40%).
- The top two operational security headaches SOC teams are struggling with are compliance (34%) and lack of visibility into infrastructure security (33%).

Overall, the findings in this report emphasize that security teams must reassess their security posture and strategies, and address the shortcomings of legacy security tools to protect their evolving IT environments.

This 2019 Cloud Security Report has been produced by Cybersecurity Insiders, the 400,000 member information security community, to explore how organizations are responding to the evolving security threats in the cloud.

Many thanks to (ISC)² for supporting this important research project.

We hope you'll find this report informative and helpful as you continue your efforts in securing your cloud environments.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

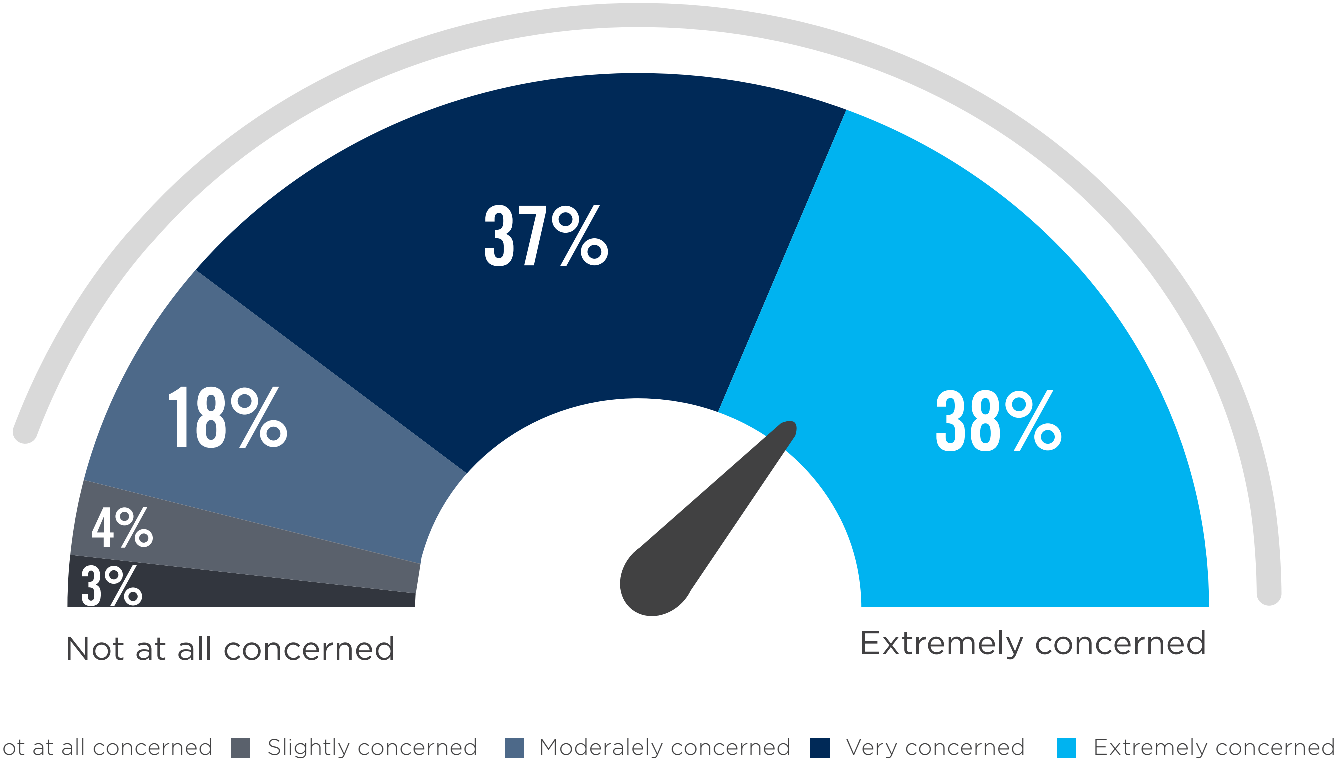
Cybersecurity INSIDERS

SECURITY IN PUBLIC CLOUDS

While adoption of public clouds continues to surge, security concerns are showing no signs of abating. An overwhelming majority of cybersecurity professionals (93%) say they are at least moderately concerned about public cloud security, a small increase from last year.

How concerned are you about the security of public clouds?

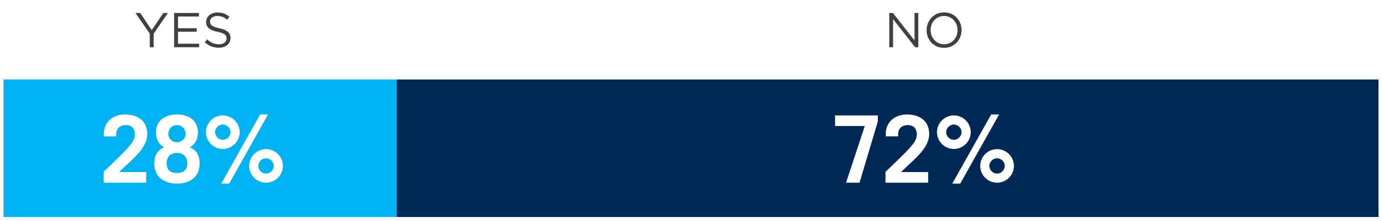
93% Organizations are moderately to extremely concerned about cloud security



CLOUD SECURITY INCIDENTS

One in four organizations (28%) confirmed they experienced a cloud security incident in the past 12 months. This rise in observed cloud security incidents (compared to last year's survey) further serves to support the increased security concerns related to adoption of cloud computing. Data exposure (27%) tops the list of incidents, followed by malware infections (20%) and compromised accounts (19%).

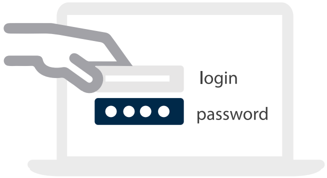
Did your organization experience a public cloud related security incident in the last 12 months?



If yes, what type of incident was it?

27%
Exposed data

20%
Malware infection



19%
Account compromise

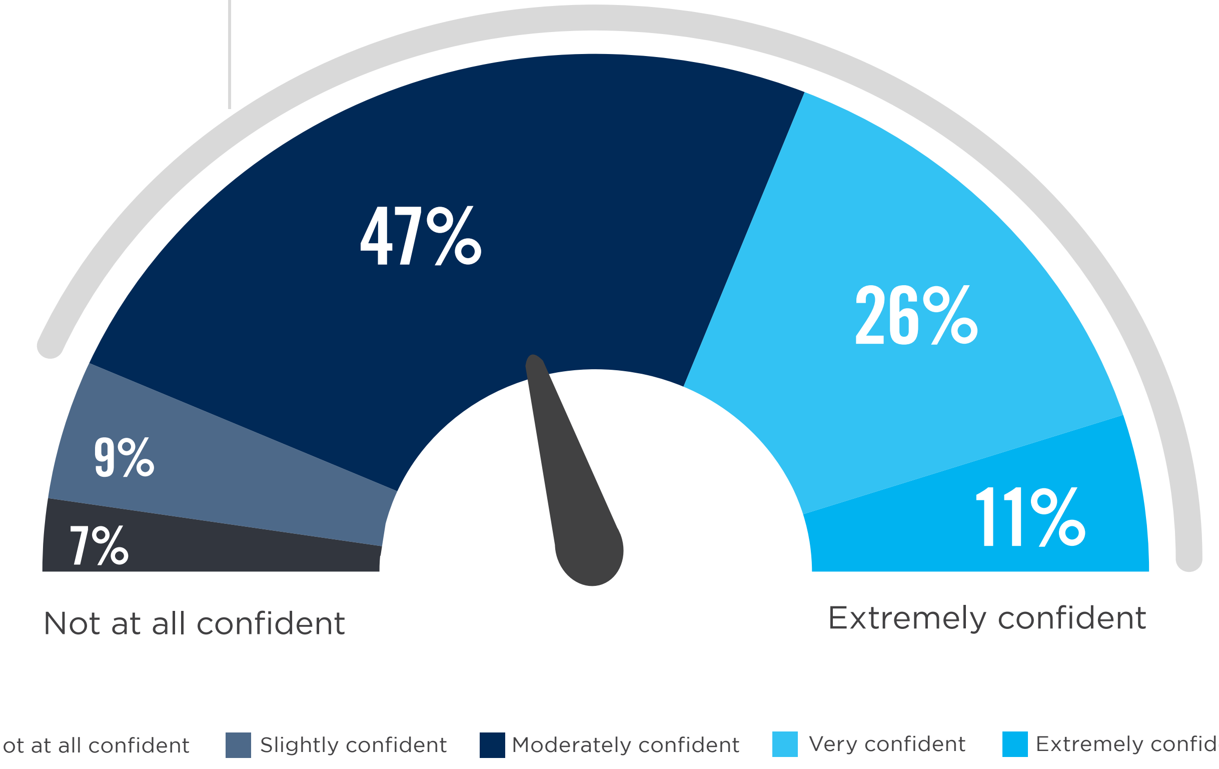
17%
Vulnerability exploited

CLOUD SECURITY CONFIDENCE

Most organizations are at least moderately confident in their cloud security posture (84%) – perhaps reflecting a level of overconfidence not supported by the security incidents and challenges presented in this report.

How confident are you in your organization's cloud security posture?

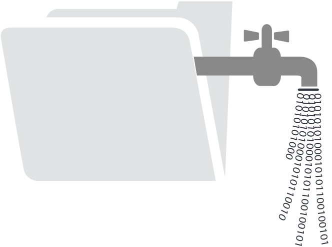
84% Most organizations are at least moderately confident in their cloud security posture



CLOUD SECURITY CONCERNS

Although cloud providers offer increasingly robust security measures, customers are ultimately responsible for securing their workloads in the cloud. The top cloud security challenges highlighted in our survey are about data loss (64%) and data privacy (62%). This is followed by compliance concerns (39%) tied with concerns about accidental exposure of credentials (39%).

What are your biggest cloud security concerns?

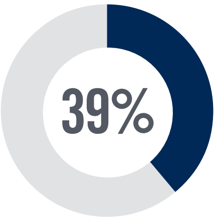


64%

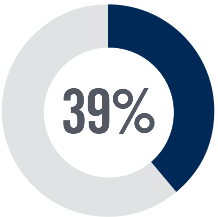
Data loss/leakage

62%

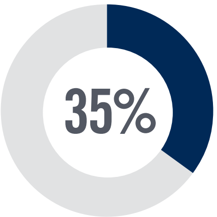
Data privacy/confidentiality



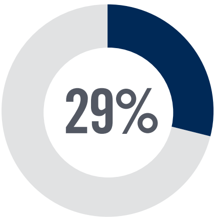
Legal and regulatory compliance



Accidental exposure of credentials



Data sovereignty/ residency/control



Incident response

Fraud (e.g., theft of SSN records) 28% | Visibility & transparency 28% | Lack of forensic data 27% | Disaster recovery 25% | Availability of services, systems and data 25% | Liability 24% | Performance 23% | Business continuity 23% | Having to adopt new security tools 19% | Not sure/other 8%

OPERATIONAL SECURITY HEADACHES

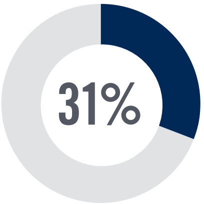
As workloads continue to move to the cloud, cybersecurity professionals are increasingly realizing the complications with protecting these workloads. The top two security headaches SOCs are struggling with are compliance (34%) and lack of visibility into infrastructure security (33%). Setting consistent security policies across cloud and on-premises environments (31%) and the continuing lack of qualified security staff (31%) are tied for third place.

▶ **What are your biggest operational, day-to-day headaches trying to protect cloud workloads?**

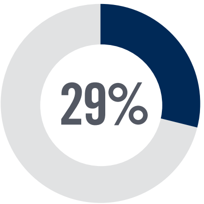
34%
Compliance

33%
Visibility into infrastructure security

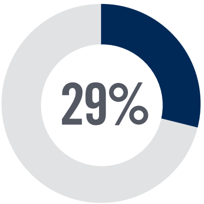
31%
Lack of qualified staff



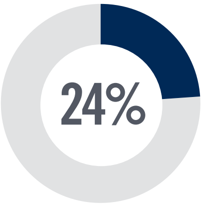
Setting consistent security policies



Lack of integration with on-premises security technologies



Security can’t keep up with the pace of changes to new/existing applications



Securing traffic flows

Can’t identify misconfigurations quickly 24% | Complex cloud to cloud/cloud to on-premises security rule matching 24% | Securing access from personal and mobile devices 23% | Reporting security threats 23% | Remediating threats 22% | Understanding network traffic patterns 21% | Justifying more security expenditure 21% | No automatic discovery/visibility/control to infrastructure security 19% | Automatically enforcing security across multiple datacenters 17% | Lack of feature parity with on-premises security solution 14% | No flexibility 8% | Not sure/other 10%

BIGGEST CLOUD SECURITY THREATS

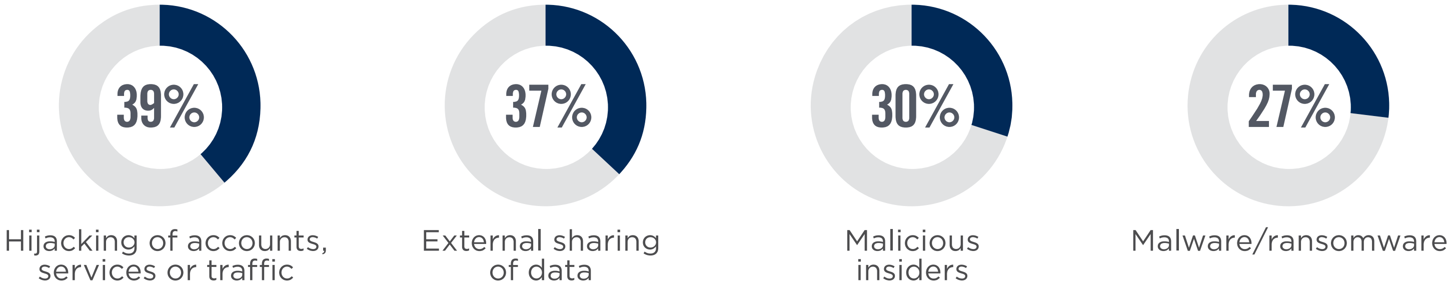
Unauthorized access (42%) and insecure interfaces (42%) take the number one spot in this year's survey as the single biggest vulnerability to cloud security. This is followed by misconfiguration of the cloud platform (40%), and hijacking of accounts (39%).

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

42% Unauthorized access

42% Insecure interfaces /APIs

40% Misconfiguration of the cloud platform /wrong setup

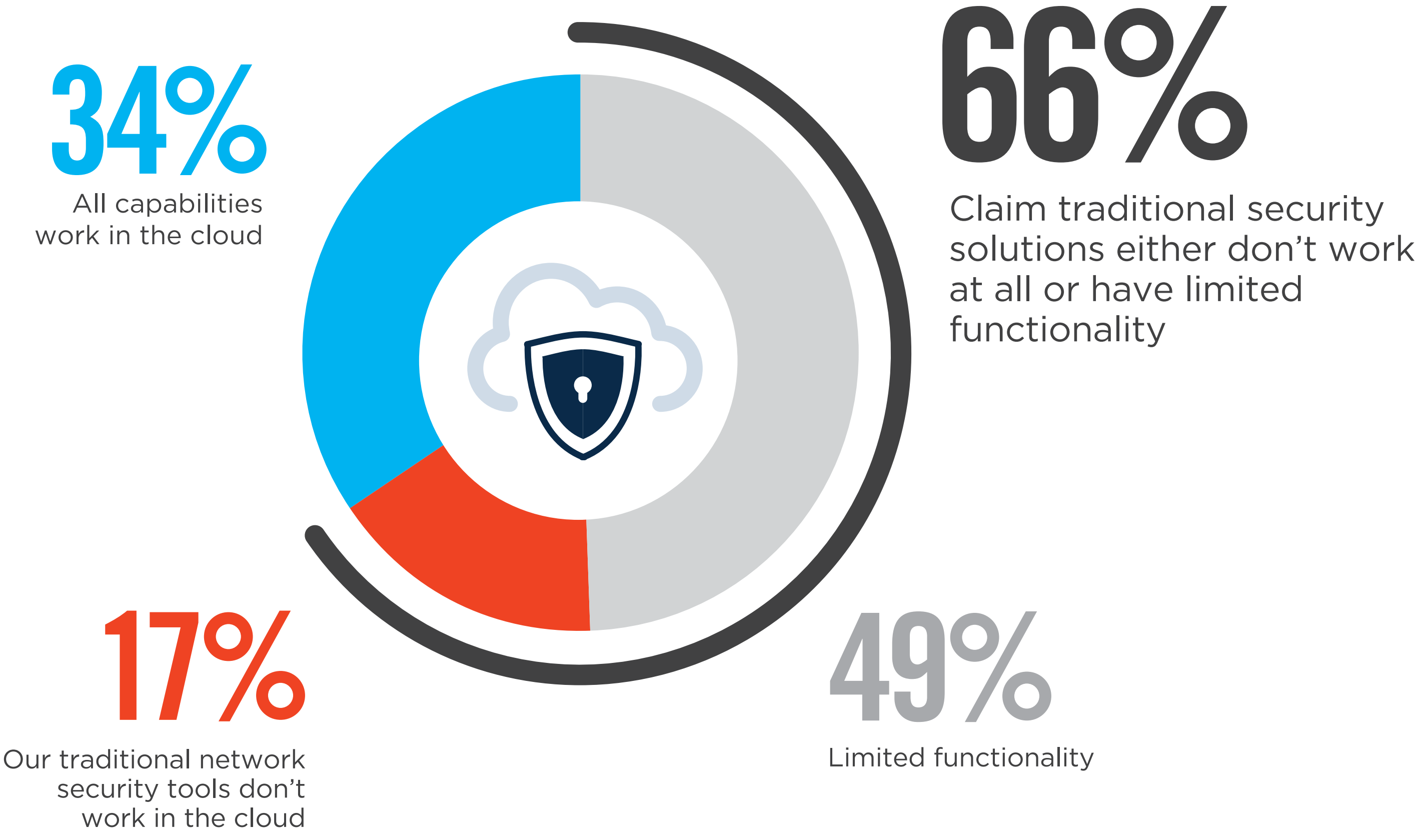


Denial of service attacks 24% | Foreign state-sponsored cyber attacks 22% | Cloud cryptojacking 19% | Theft of service 16% | Lost mobile devices 13% | Other 1%

TRADITIONAL TOOLS IN THE CLOUD

As workloads continue to move to the cloud, organizations are faced with unique security challenges that cloud adoption presents. Many legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. Sixty-six percent of respondents say traditional security solutions either don't work at all in cloud environments or have only limited functionality – a marked improvement from last year's survey.

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



DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS

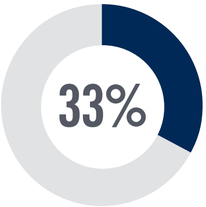
Organizations recognize several key advantages of deploying cloud-based security solutions. Respondents selected cost savings (42%) along with faster time to deployment (39%) and better performance (34%) as the top three factors for selecting cloud-based security solutions.

What are the main drivers for considering cloud-based security solutions?

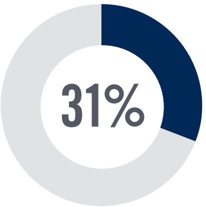
42%
Cost savings

39%
Faster time to deployment

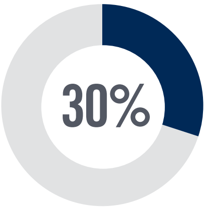
34%
Better performance



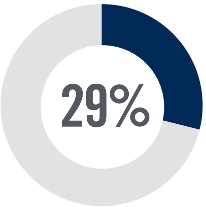
Our data/workloads reside in the cloud (or are moving to the cloud)



Reduced effort around patches and upgrades of software



Need for secure app access from any location



Meet cloud compliance expectations

Better visibility into user activity and system behavior 25% | Reduction of appliance footprint in branch offices 23% | Easier policy management 22% | Other 2%

BARRIERS TO CLOUD-BASED SECURITY ADOPTION

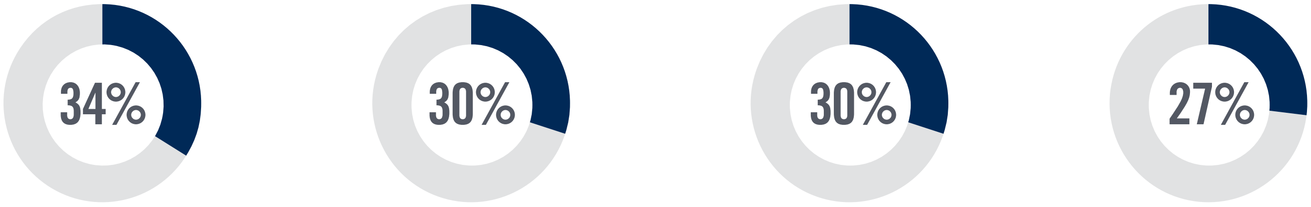
Despite the significant advantages offered by cloud-based security solutions, some barriers to adoption still exist. When it comes to business transformation and cloud adoption, three important aspects must be aligned: people, process and technology. Our survey reveals that the biggest challenge organizations are facing is not technology, but people and processes. Staff expertise and training (41%) continues to rank as the highest barrier, followed by budget challenges (40%), data privacy concerns (38%), and lack of integration with on-premises platforms (34%).

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

41% Staff expertise/ training

40% Budget

38% Data privacy



34% Lack of integration with on-premises security technologies

30% Regulatory compliance requirements

30% Solution maturity

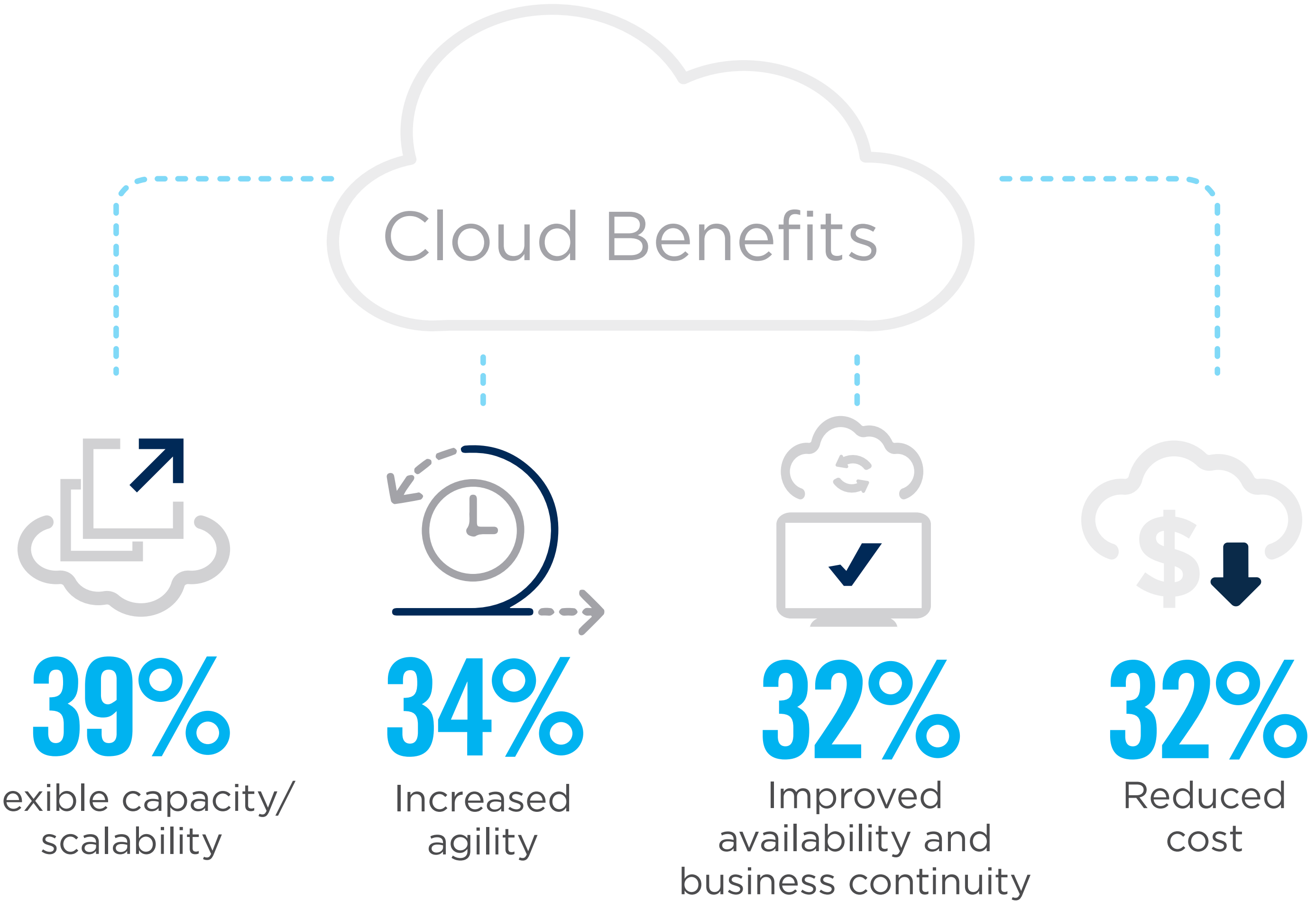
27% Data residency

Limited control over encryption keys 21% | Scalability and performance 21% | Integrity of cloud security platform (DDoS attack, breach) 19% | Sunk cost into on-premises tools 17% | Not sure/other 8%

CLOUD BENEFITS REALIZED

The organizations participating in this survey generally confirmed that cloud is delivering on its promise of flexible capacity and scalability (39%), increased agility (34%) and improved availability (32%) – tied with cost savings (32%). Consistent with other findings in this survey, improved security is further down the list at only 26%.

▶ **What overall benefits have you already realized from your cloud deployment?**



Cloud Benefits

39% Flexible capacity/ scalability

34% Increased agility

32% Improved availability and business continuity

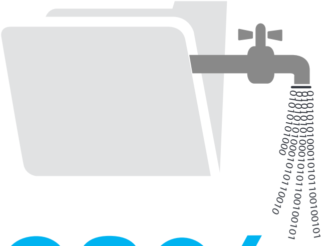
32% Reduced cost

Accelerated deployment and provisioning 29% | Accelerated time to market 26% | Improved performance 26% | Improved security 26% | Increased employee productivity 24% | Moved expenses from fixed CAPEX (purchase) to variable OPEX (rental/subscription) 24% | Increased geographic reach 19% | Reduced complexity 19% | Regulatory compliance 16% | Not sure/other 13%

BARRIERS TO CLOUD ADOPTION

Despite all of its benefits, cloud computing is still not without challenges. Data security (29%) and general security risks (28%) combined with lack of budget (26%), compliance challenges (26%) and lack of qualified staff (26%) top the list of barriers to faster cloud adoption.

▶ **What are the biggest barriers holding back cloud adoption in your organization?**



29%

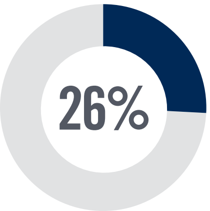
Data security,
loss & leakage risks

28%

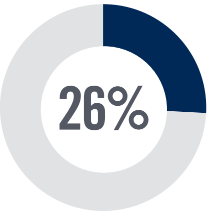
General security
risks

26%

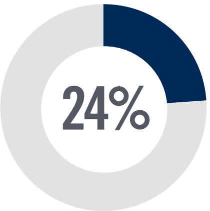
Lack of budget



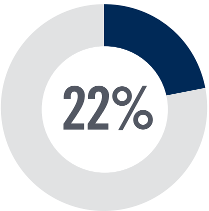
Legal & regulatory
compliance



Lack of staff
resources or expertise



Integration with existing
IT environment



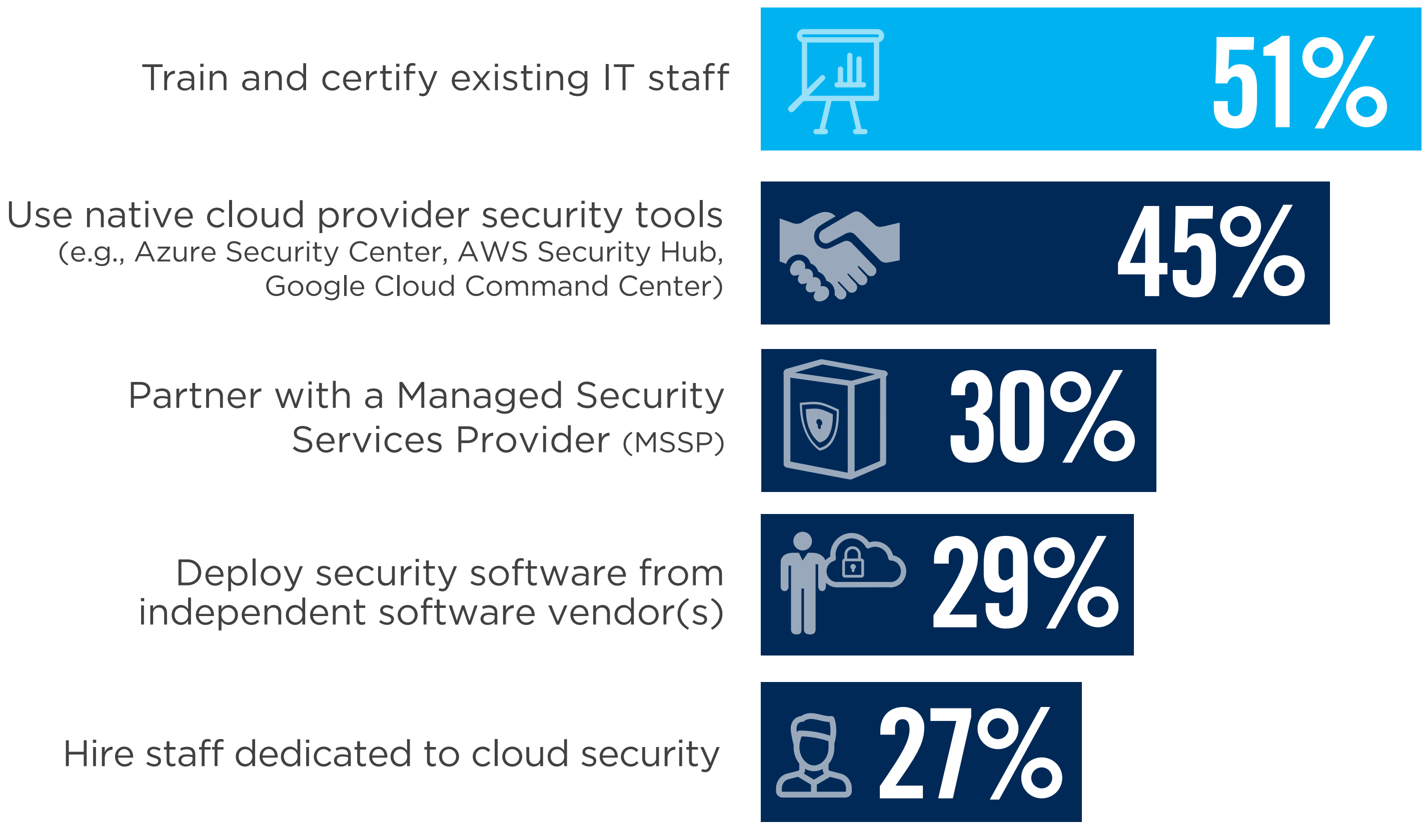
Loss of
control

Complexity managing cloud deployment 20% | Fear of vendor lock-in 20% | Cost/lack of ROI 19% | Internal resistance and inertia 19% | Performance of apps in the cloud 16% | Lack of transparency and visibility 16% | Lack of customizability 16% | Billing & tracking issues 15% | Lack of management buy-in 13% | Availability 13% | Lack of maturity of cloud service models 13% | Dissatisfaction with cloud service offerings/performance/pricing 11% | Lack of support by cloud provider 10% | Other 4%

PATHS TO STRONGER CLOUD SECURITY

For the third year in a row, training and certifying IT staff (51%) ranks as the primary tactic organizations deploy to assure that their evolving security needs are met. Forty-five percent of respondents rely on their cloud provider's native security tools, and 30% partner with a managed security services provider to fill any gaps in capabilities.

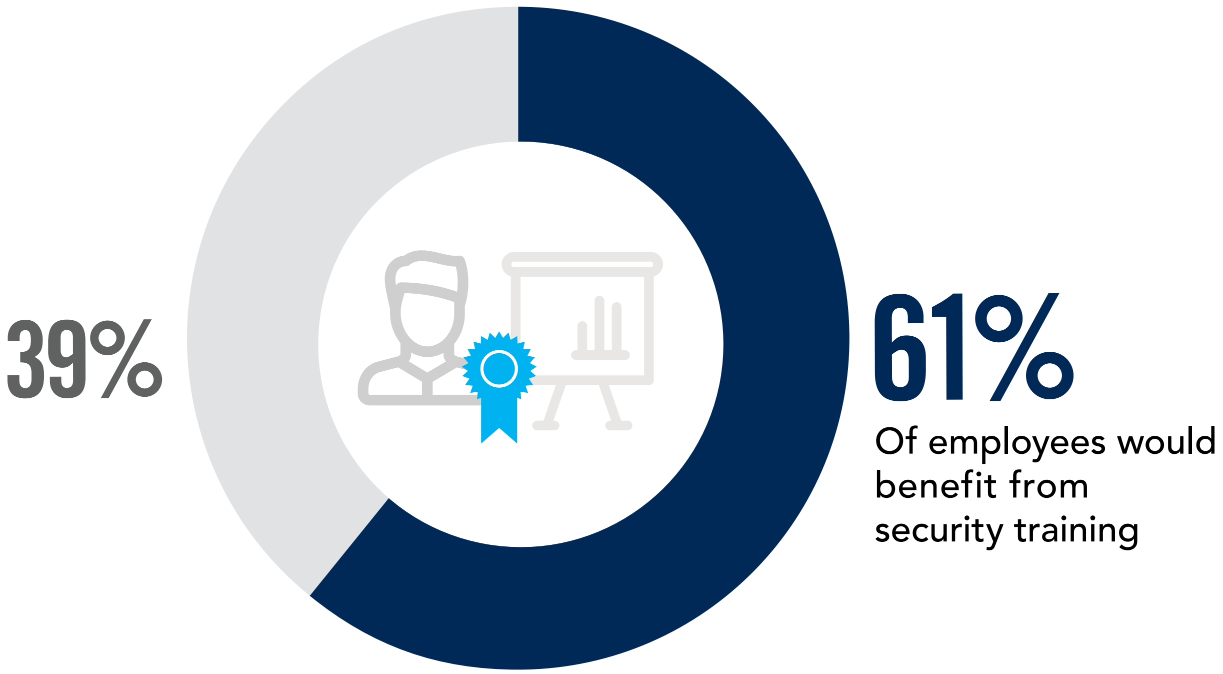
When moving to the cloud, how do you handle your changing security needs?



SECURITY TRAINING AND CERTIFICATION

The main recurring theme in this survey is the continuing shortage of not only qualified cybersecurity staff, but also the lack of security awareness and skills among all employees. Sixty-one percent of organizations agree that their employees would benefit from security training and/or certification of their jobs.

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



▶ **Top 10 most valued security certifications**

#1	CISSP
#2	CCSP
#3	CISM
#4	CCSK
#5	Security+
#6	CISA
#7	CEH
#8	Network+
#9	CCISO
#10	Cloud+

TRAINING FOCUS

When it comes to prioritizing security training topics, the participants in our survey selected cloud-enabled cybersecurity (49%), followed by application security (41%), and incident response (34%).

Which of the following topic areas would you find most valuable for ongoing training and education to be successful in your current role?

49%

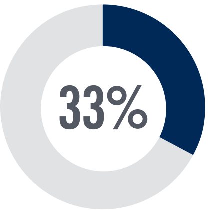
Cloud-enabled cybersecurity

41%

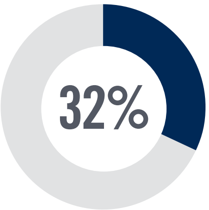
Application security

34%

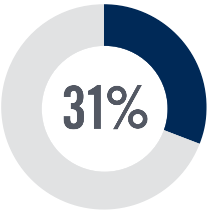
Incident response



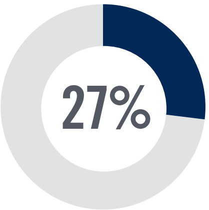
DevOps



Regulatory compliance



Mobile security



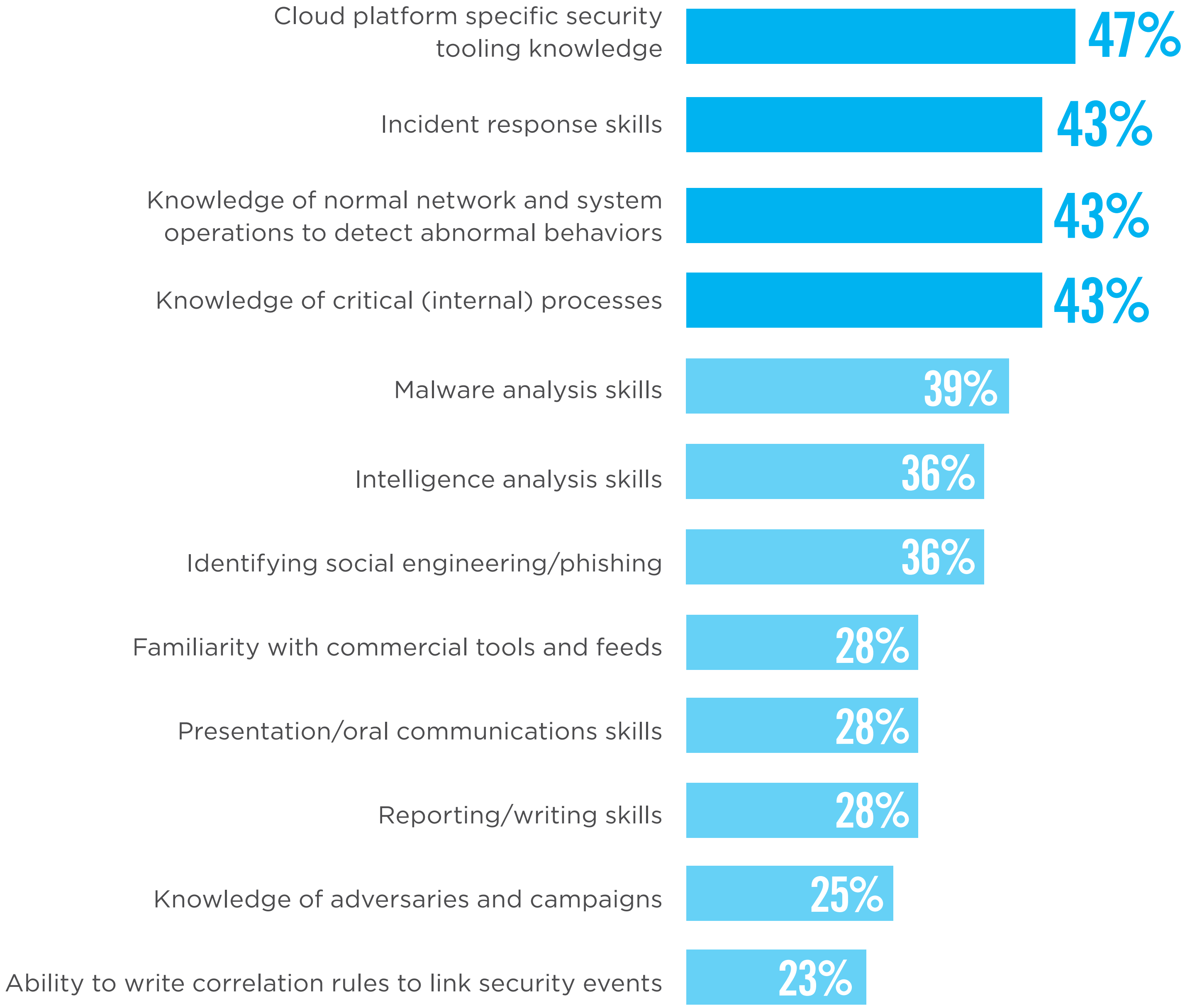
Internet of Things (IoT)

Soft skills (leadership, effective teamwork, communicating to persuade/educate) 26% | Risk-based frameworks 25% | Open source vulnerabilities 25% | Digital forensics 24% | Identifying social engineering/phishing 22% | PII 18% | Not sure/other 4%

MOST CRITICAL SECURITY SKILLS

Among the 10 most critical cloud security skills, organizations prioritize knowledge of cloud-specific security tools (47%), followed by incident response skills (43%), and knowledge of network behaviors (43%).

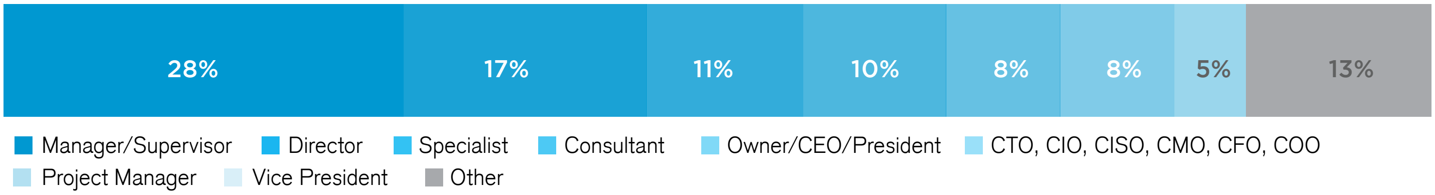
▶ **What are the most important security skills required in your organization?**



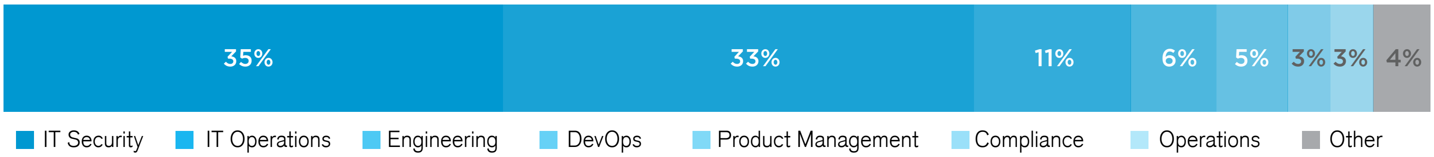
METHODOLOGY & DEMOGRAPHICS

This Cloud Security Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in March of 2019 to gain deep insight into the latest trends, key challenges and solutions for cloud security. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

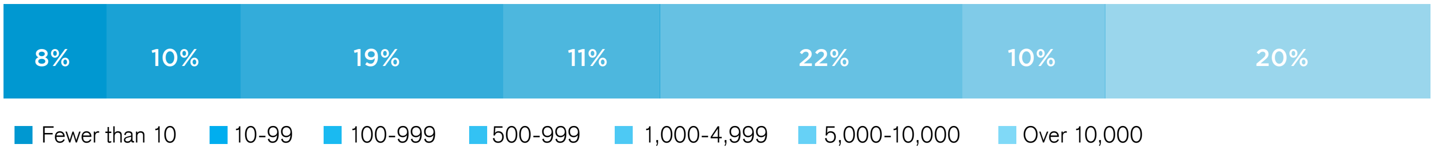
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



Celebrating its 30th anniversary this year, (ISC)² 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)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. In 2015, (ISC)² and the Cloud Security Alliance (CSA) partnered to launch 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 140,000 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)², visit www.isc2.org, follow us on Twitter or connect with us on Facebook and LinkedIn.

Give yourself a competitive edge with the #1 cloud security certification

CCSP® Certified Cloud Security Professional

51%

of organizations want to train and certify their current IT staff, to ensure that their evolving security needs are met.

27%

want to hire staff dedicated to cloud security.

Start with The Ultimate Guide to the CCSP

Is the CCSP Right for Me?
5 YEARS
Discover Your Path
THE ULTIMATE GUIDE TO THE CCSP
Be a Leader in the Field of Cloud Security

EXCLUSIVE FEATURES

- ✓ Is CCSP Right for Me?
- ✓ Fast Facts about CCSP
- ✓ Benefits
- ✓ Exam Overview
- ✓ Training and Self-Study Resources
- ✓ Pathway to Certification

YES, GIVE ME THE FREE GUIDE >