2021

Cybersecurity
INSIDERS

CLOUD SECURITY REPORT

(ISC)²

INTRODUCTION

Cloud security concerns remain high as the adoption of public cloud computing continues to surge, especially in the wake of the 2020 COVID crisis and the resulting accelerated shift to remote work environments.

The 2021 Cloud Security Report has been produced by Cybersecurity Insiders to explore how organizations are responding to the evolving security threats in the cloud and the continued shortfall of qualified security staff.

Key survey findings include:

- Despite rapid adoption of cloud computing, security remains a primary issue for cloud customers. Virtually all surveyed cybersecurity professionals **(96%) confirm they are at least moderately concerned about public cloud security,** a small increase from last year's survey.
- We asked survey participants about the biggest barriers holding back faster cloud adoption. Among the key barriers to cloud adoption, organizations mention lack of **qualified staff (39%) as the biggest impediment to faster adoption**, followed by data security issues (34%) and legal & regulatory compliance (32%).
- A majority of organizations **(57%) expect their cloud security budget to increase over the next 12 months.** On average, organizations allocate 28% of their security budget to cloud security.
- We asked organizations how they would rate their overall security readiness. A majority of organizations **(73%) rate their security readiness average or below average.** Only half as many say they are above average (27%).
- As in previous years, the continuing shortage of qualified cybersecurity staff and the lack of security awareness and skills among all employees remains the number one security challenge for organizations. To alleviate this shortage, cybersecurity professionals agree that **6 out of 10 employees would benefit from security training and/or certification** for their jobs.

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

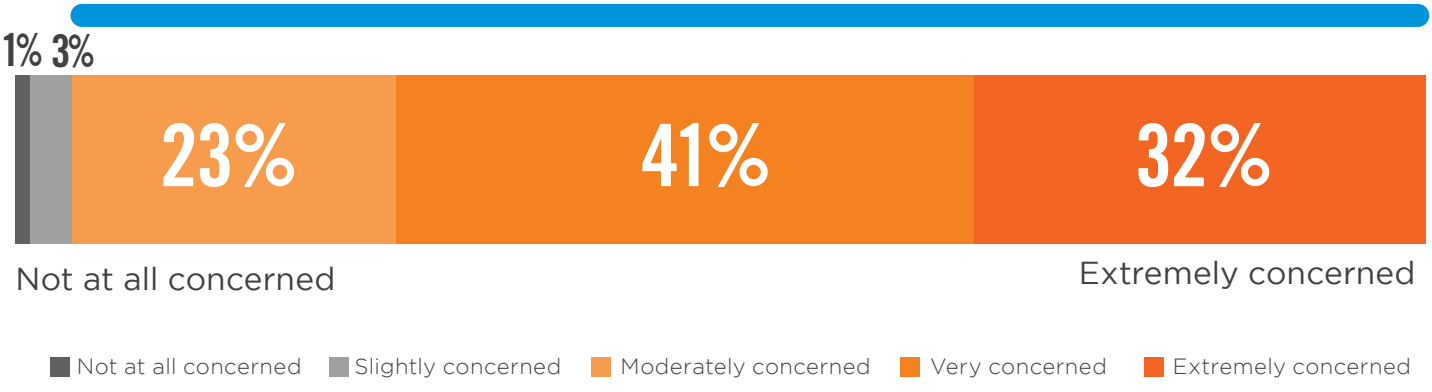
SECURITY IN PUBLIC CLOUDS

Despite rapid adoption of cloud computing, security remains a key issue for cloud customers. Virtually all surveyed cybersecurity professionals (96%) confirm they are at least moderately concerned about public cloud security, a small increase from last year's survey.

Cloud users are particularly concerned with risks arising from misconfiguration of the cloud platform, exfiltration of sensitive data, and unauthorized access (see page 8).

How concerned are you about the security of public clouds?

96% Of organizations are moderately to extremely concerned about cloud security.



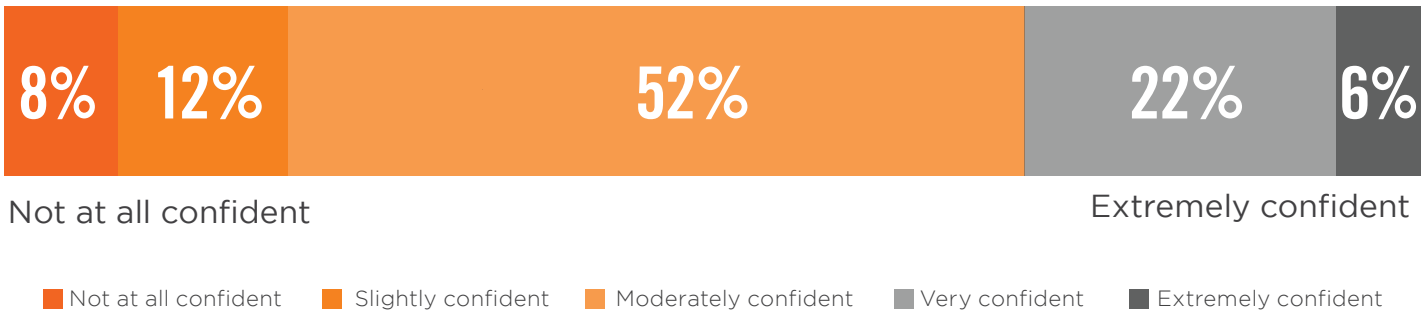
CLOUD SECURITY CONFIDENCE

The heightened concerns about cloud security have a negative impact on organizations' confidence in their own cloud security posture. A majority of organizations are at best only moderately confident in their cloud security posture (72% - up from 66% in last year's survey). While confidence has been declining over time, we still see an alarming degree of overconfidence not supported by the backdrop of security incidents and challenges presented in this report.

The biggest challenges causing loss of confidence in cloud security include concerns around data loss/leakage, data privacy/confidentiality, and accidental exposure of credentials (see page 5).

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

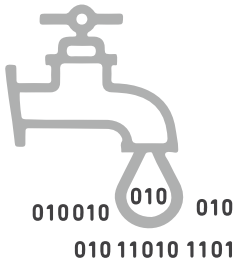
72% Of organizations are not at all confident to moderately confident in their cloud security posture.



CLOUD SECURITY CONCERNS

While cloud providers offer increasingly robust security measures as part of their cloud services, it is the customer who is ultimately responsible for securing their workloads in the cloud. The most significant cloud security challenges highlighted in our survey are unchanged from last year: data loss/leakage (64% - down five percentage points since last year), data privacy/confidentiality (62% - down four percentage points), and accidental exposure of credentials (46% - up two percentage points).

What are your biggest cloud security concerns?



64%

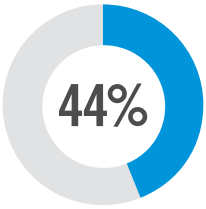
Data loss/leakage

62%

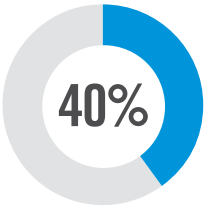
Data privacy/ confidentiality

46%

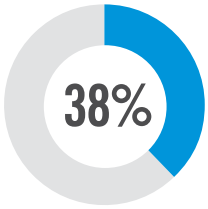
Accidental exposure of credentials



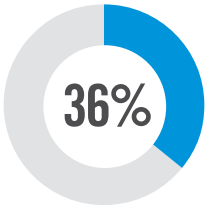
Legal and regulatory compliance



Visibility & transparency



Incident response



Data sovereignty/ residency/control

Lack of forensic data 24% | Business continuity 24% | Liability 23% | Availability of services, systems, and data 23% | Disaster recovery 22% | Having to adopt new security tools 18% | Performance 16% | Fraud (e.g., theft of SSN records) 15% | Not sure/other 5%

OPERATIONAL SECURITY HEADACHES

Cybersecurity professionals are faced with numerous complications around protecting cloud workloads. Lack of qualified security staff (49%) remains number one on the list of day-to-day headaches (up from 47% in last year's survey), followed by compliance (40%) and visibility into infrastructure security (36% - up from 33% in 2020).

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

49%

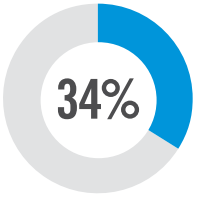
Lack of qualified staff

40%

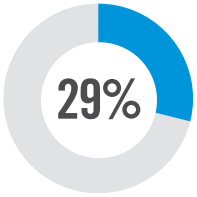
Compliance

36%

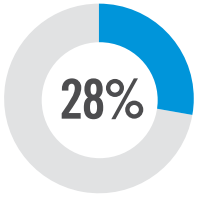
Visibility into infrastructure security



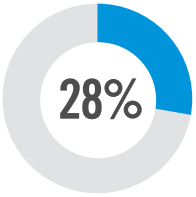
Can't identify misconfigurations quickly



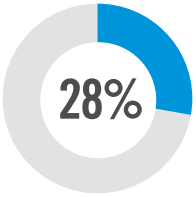
Setting consistent security policies



Implementing continuous and automated security controls in the cloud



Automatically enforcing security across multiple clouds



Justifying more security expenditure

Setting the correct user access privileges 28% | Security can't keep up with the pace of changes to new/existing applications 27% | Securing access from personal and mobile devices 26% | Lack of integration with on-prem security technologies 25% | Complex cloud to cloud/cloud to on-prem security rule matching 25% | No automatic discovery/visibility/control to infrastructure security 22% | Understanding network traffic patterns 21% | Securing traffic flows 20% | Reporting security threats 20% | Remediating threats 20% | Lack of feature parity with on-prem security solution 13% | No flexibility 3% | Not sure/other 11%

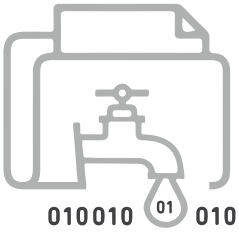
BARRIERS TO CLOUD ADOPTION

We asked survey participants about the biggest barriers holding back faster cloud adoption. Among the barriers to cloud adoption, organizations mention lack of qualified staff (39% - up from 37%) as the biggest impediment to faster adoption, followed by data security issues (34%) and legal & regulatory compliance (32%).

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

39%

Lack of staff resources or expertise

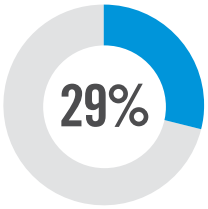


34%

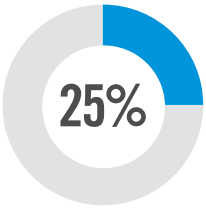
Data security, loss & leakage risks

32%

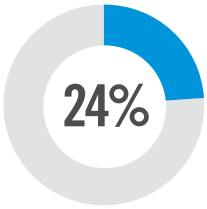
Legal & regulatory compliance



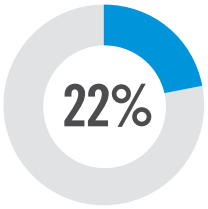
Integration with existing IT environment



General security risks



Fear of vendor lock-in



Loss of control

Internal resistance and inertia 21% | Complexity managing cloud deployment 21% | Lack of budget 20% | Cost/lack of ROI 19%

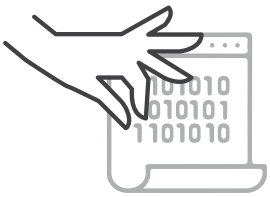
BIGGEST CLOUD SECURITY THREATS

We asked what security threats cybersecurity professionals see facing public clouds. The biggest threat remains misconfiguration of the cloud platform (67%), followed by exfiltration of sensitive data (59%) and tying at 49% are unauthorized access and insecure interfaces.

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

67%

Misconfiguration of the cloud platform/wrong setup



59%

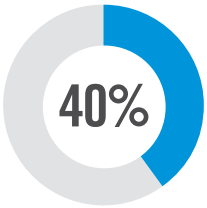
Exfiltration of sensitive data

49%

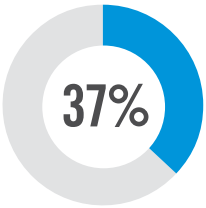
Unauthorized access

49%

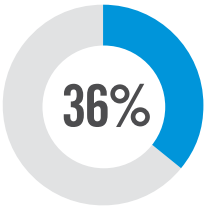
Insecure interfaces/APIs



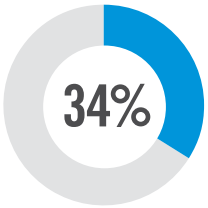
External sharing of data



Hijacking of accounts, services, or traffic



Malicious insiders



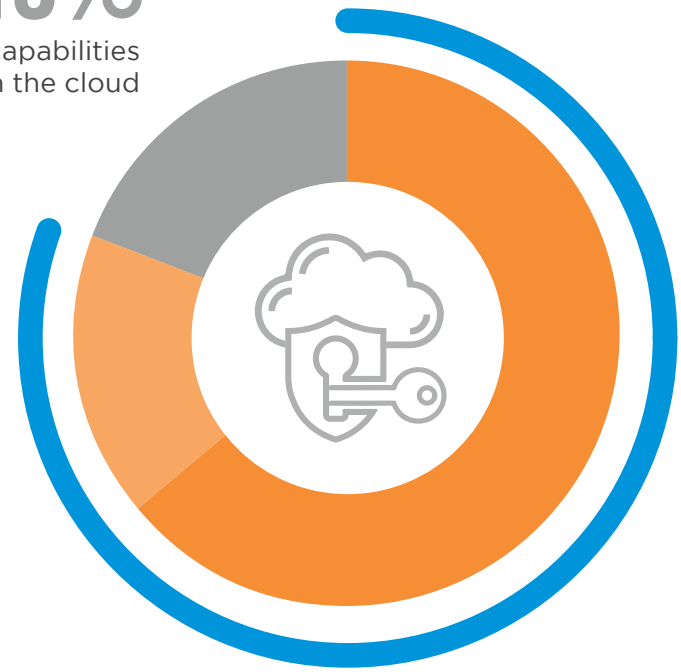
Foreign state-sponsored cyber attacks

Malware/ransomware 31% | Denial of service attacks 26% | Cloud cryptojacking 16% | Theft of service 13% | Lost mobile devices 8%
Don't know/other 7%

TRADITIONAL TOOLS IN THE CLOUD

Organizations are faced with unique security challenges presented by cloud computing. Unfortunately, most legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. Eighty-one percent of organizations say traditional security solutions either don't work at all in cloud environments or have only limited functionality – a one percentage point improvement from last year's survey (82%).

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



19%
All capabilities work in the cloud

17%
Our traditional network security tools don't work in the cloud

64%
Limited functionality

81%
Claim traditional security solutions either don't work at all or have limited functionality.

DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS

Organizations recognize several key drivers for the rapid adoption of cloud computing and the deployment of cloud-based security solutions. Better scalability (55%), faster time to deployment (48%), and cost savings (40%) are the top three drivers. This is followed by reduced efforts around patches and software updates (38%) and better performance (35%).

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

55%

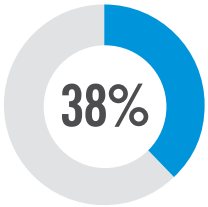
Better scalability

48%

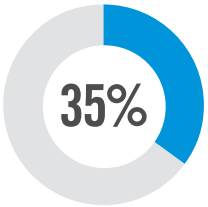
Faster time to deployment

40%

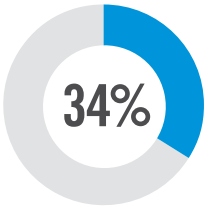
Cost savings



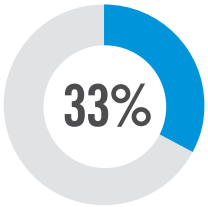
Reduced effort around patches and upgrades of software



Better performance



Better visibility into user activity and system behavior



Need for secure app access from any location

Our data/workloads reside in the cloud (or are moving to the cloud) 32% | Meet cloud compliance expectations 30% | Easier policy management 27% | Better uptime 26% | Reduction of appliance footprint in branch offices 23% | Other 1%

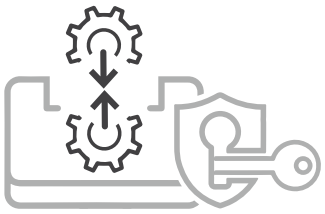
BARRIERS TO CLOUD-BASED SECURITY ADOPTION

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 about technology, but people and processes. Staff expertise and training (53%) continues to rank as the highest barrier, followed by lack of integration with on-premises security technologies (37%) and budget challenges (36%).

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

53%

Staff expertise/ training

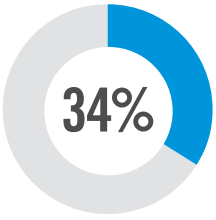


37%

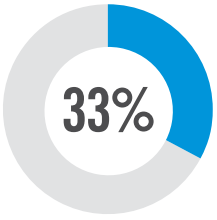
Lack of integration with on-premises security technologies

36%

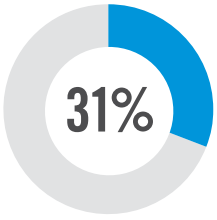
Budget



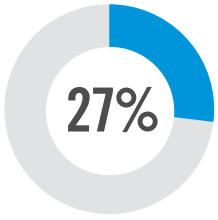
Data privacy



Data residency



Regulatory compliance requirements



Solution maturity

Sunk cost into on-premises tools 20% | Limited control over encryption keys 18% | Integrity of cloud security platform (DDoS attack, breach) 13% | Scalability and performance 9% | Not sure/other 9%

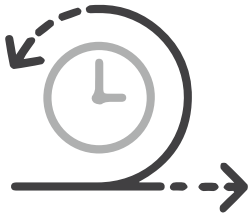
CLOUD BENEFITS

Cloud users confirm that the cloud is delivering on the promise of flexible capacity and scalability (57%), increased agility (47%), and improved availability and business continuity (46%).

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

57%

More flexible capacity/scalability

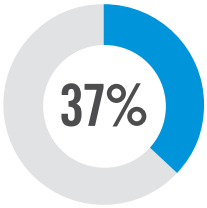


47%

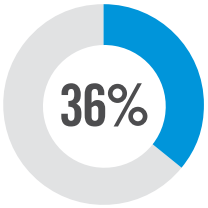
Increased agility

46%

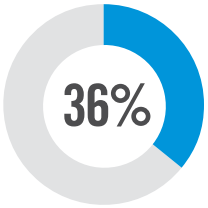
Improved availability and business continuity



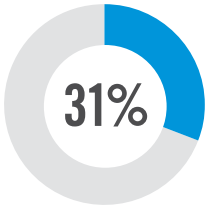
Moved expenses from fixed CAPEX (purchase) to variable OPEX (rental/subscription)



Accelerated deployment and provisioning



Accelerated time to market



Reduced cost

Improved performance 31% | Improved security 28%

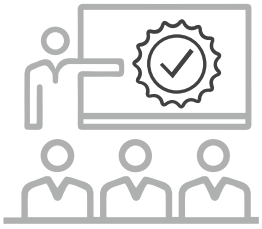
PATHS TO STRONGER CLOUD SECURITY

When asked about organizations' responses to changing security needs, the use of native cloud provider security tools (62%) and training and certifying IT staff (61%) rank as the top tactics organizations deploy to assure their evolving security needs are met. This is followed by partnering with an MSSP (33%), hiring staff dedicated to cloud security (31%), and deploying security software from independent vendors (30%).

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

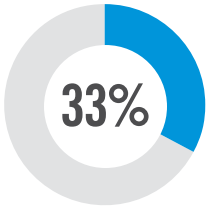
62%

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

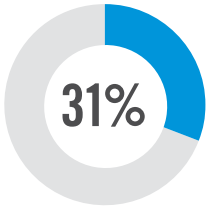


61%

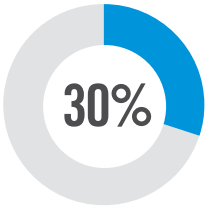
Train and/or certify existing IT staff



Partner with a Managed Security Services Provider (MSSP)



Hire staff dedicated to cloud security

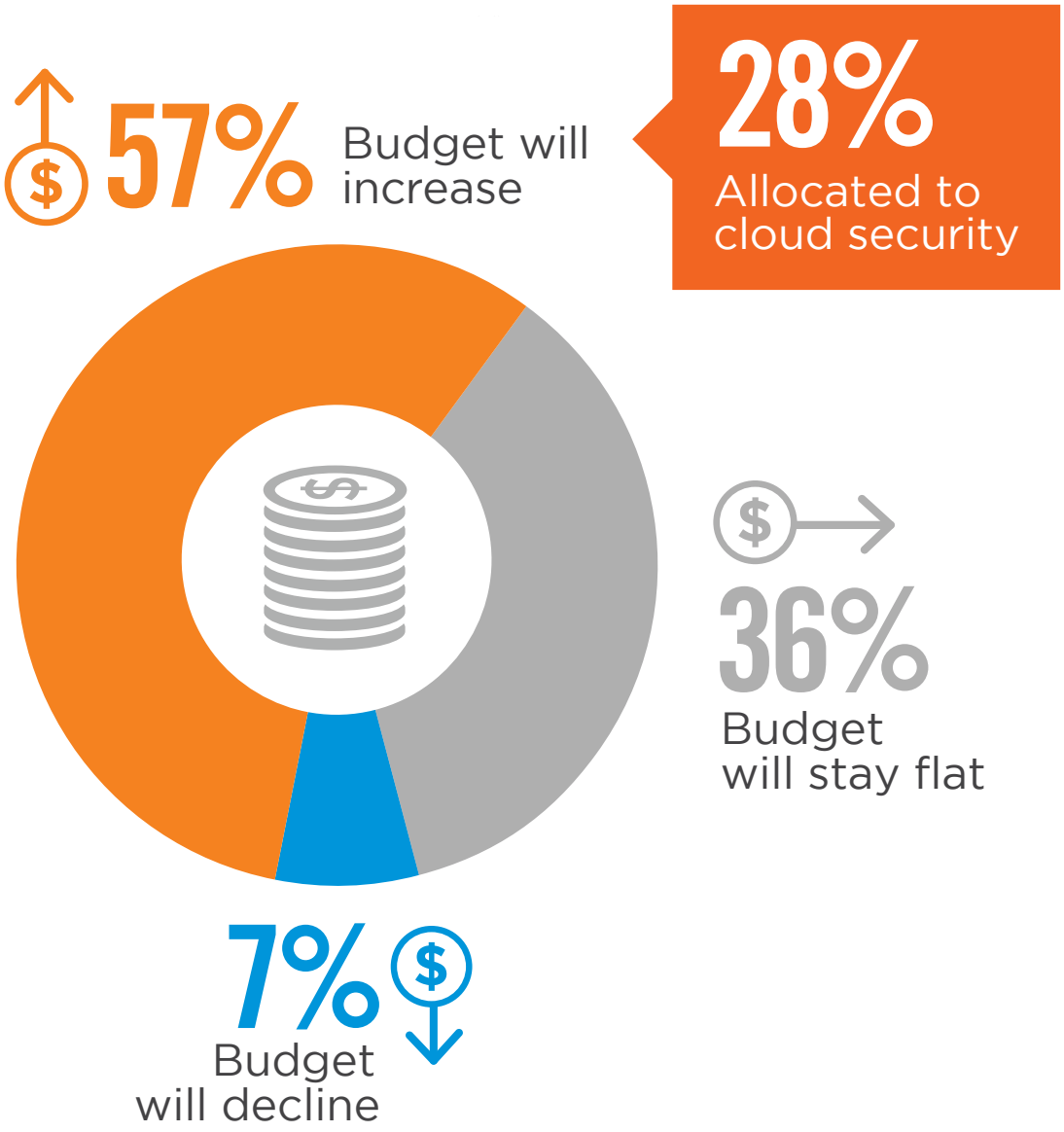


Deploy security software from independent vendors

CLOUD SECURITY BUDGET

A majority of organizations (57%) expect their cloud security budget to increase over the next 12 months. On average, organizations allocate 28% of their security budget to cloud security.

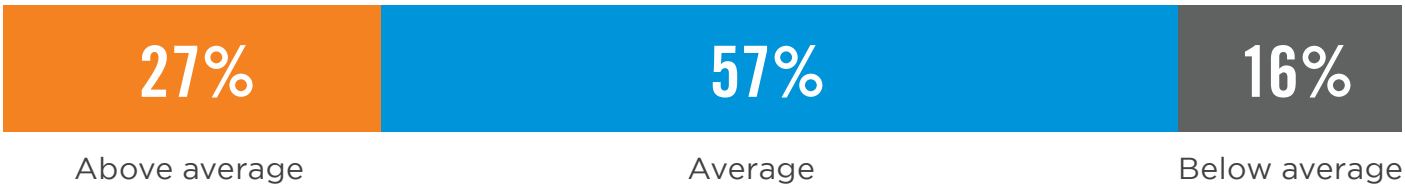
How is your cloud security budget changing in the next 12 months? What percentage of your IT security budget is allocated to cloud security?



SECURITY READINESS

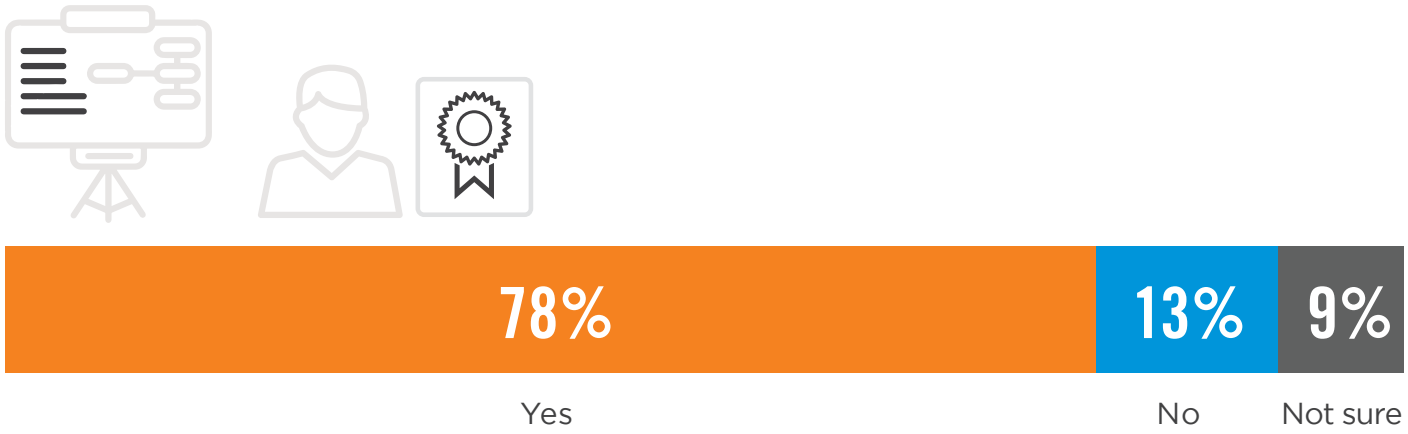
We asked organizations how they would rate their overall security readiness. A majority of organizations (73%) rate their security readiness average or below average. Only half as many say they are above average (27%).

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



Of those rating their overall security readiness average or below average, 78% 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?

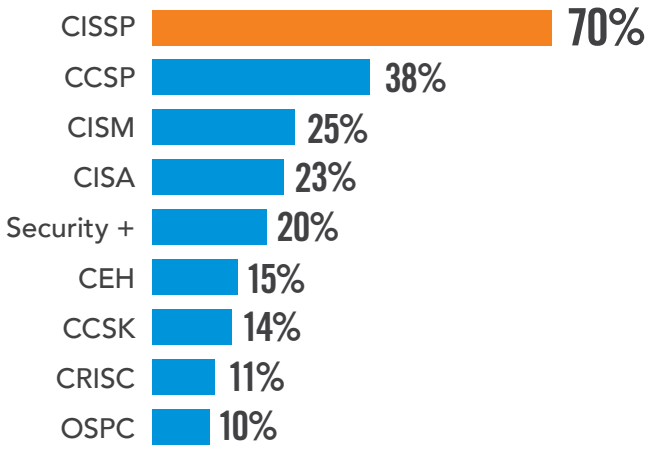


SECURITY TRAINING AND CERTIFICATION

As in previous years, the continuing shortage of qualified cybersecurity staff and the lack of security awareness and skills among all employees remains the number one security challenge for organizations. To alleviate this shortage, cybersecurity professionals agree that six out of 10 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?

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



TRAINING FOCUS

We asked what security training topics organizations would find most valuable. The top priorities include cloud-enabled cybersecurity (68%), followed by incident response (45%), risk-based frameworks (39%), and application security (38%).

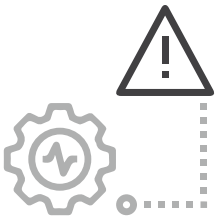
Which of the following topic areas would you find most valuable for ongoing training and education to be successful in your current role?

68%

Cloud-enabled cybersecurity

45%

Incident response

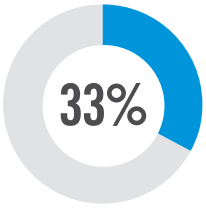


39%

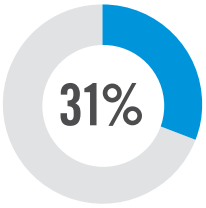
Risk-based frameworks

38%

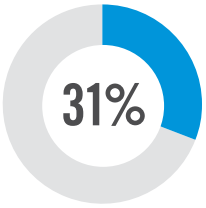
Application security



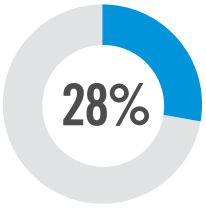
Regulatory compliance



DevOps



Soft skills (e.g., leadership, effective teamwork, communicating to persuade/educate)



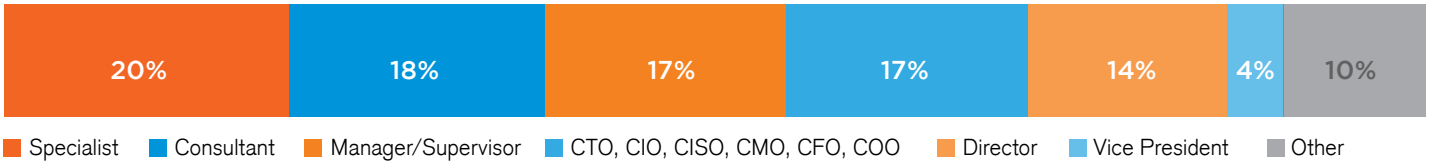
Mobile security

PII 26% | Digital forensics 23% | Internet of Things (IoT) 20% | Identifying social engineering/phishing 20% | Open source vulnerabilities 15% | Not sure/other 5%

METHODOLOGY & DEMOGRAPHICS

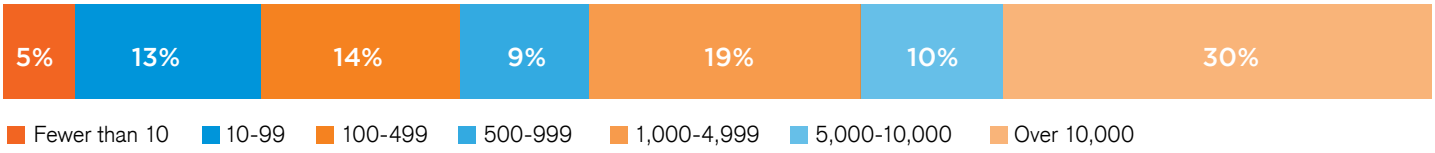
The 2021 Cloud Security Report is based on a comprehensive survey of 613 cybersecurity professionals conducted in May 2021, to uncover how cloud user organizations are responding to security threats in the cloud, and what training, certifications, and best practices IT cybersecurity leaders are prioritizing 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

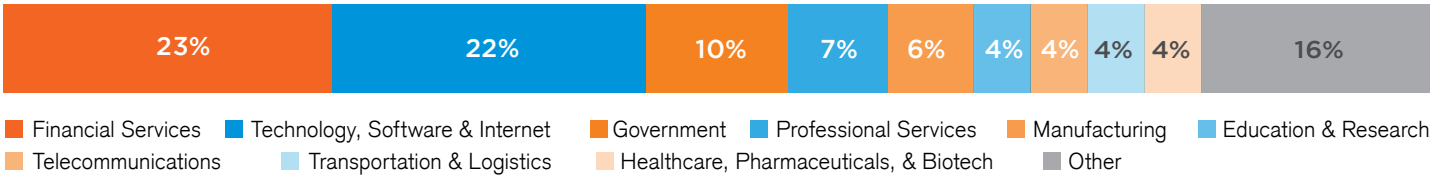


DEPARTMENT

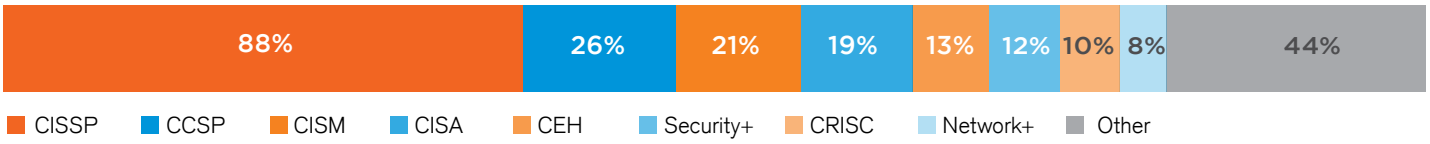
COMPANY SIZE



INDUSTRY



SECURITY CERTIFICATIONS HELD



(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 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 150,000 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.

Are You Staying Ahead of Emerging CLOUD SECURITY TRENDS?

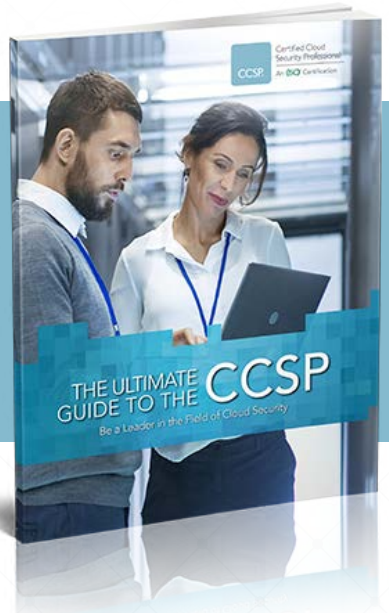
55% of organizations are likely or very likely to deploy a new cloud security solution within the next year.

78% 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 **55%**
- Migrating to Cloud-based security solutions **53%**
- Cloud Adoption **39%**

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



Exclusive Features:

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

GET YOUR GUIDE

CERTIFICATION MAGAZINE
2021 TOP CERT
CCSP
(ISC)²
THE NEXT BIG THING

CCSP tops "**The Next Big Thing**" list as the #1 certification survey respondents plan to earn in 2021.

CCSP
Certified Cloud Security Professional
An (ISC)² Certification