2020

Cybersecurity
INSIDERS

CLOUD SECURITY REPORT

(ISC)²

INTRODUCTION

Companies continue to rapidly migrate workloads from datacenters to the cloud, utilizing new technologies such as serverless, containers, and machine learning to benefit from increased efficiency, better scalability, and faster deployments from cloud computing.

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.

Key survey findings include:

- Security remains a key issue for cloud customers, despite continued rapid adoption of cloud computing. A majority of cybersecurity professionals (94%) confirm they are at least moderately concerned about public cloud security, a small increase from last year's survey.
- Among the key barriers to cloud adoption, organizations mention a lack of qualified staff (37%) as the biggest impediment to faster adoption – up from the fifth spot on last year's survey.
- For the fourth year in a row, training and certifying IT staff (61%) ranks as the primary tactic organizations deploy to assure their evolving security needs are met. Fifty-eight percent of respondents rely on their cloud provider's native security tools, and 34% are looking to hire more staff dedicated to cloud security.
- A majority of six of 10 organizations expect their cloud security budget to increase over the next 12 months. On average, organizations allocate 27% of their security budget to cloud security.
- When asked how organizations rate their overall security readiness, 69% rate their team's security readiness average or below average. Only half as many say they are above average (31%). Of those, 80% believe their teams would benefit from cloud security training and/or 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. Cybersecurity professionals agree that 59% of employees would benefit from security training and/or certification for their jobs.

This 2020 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.

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

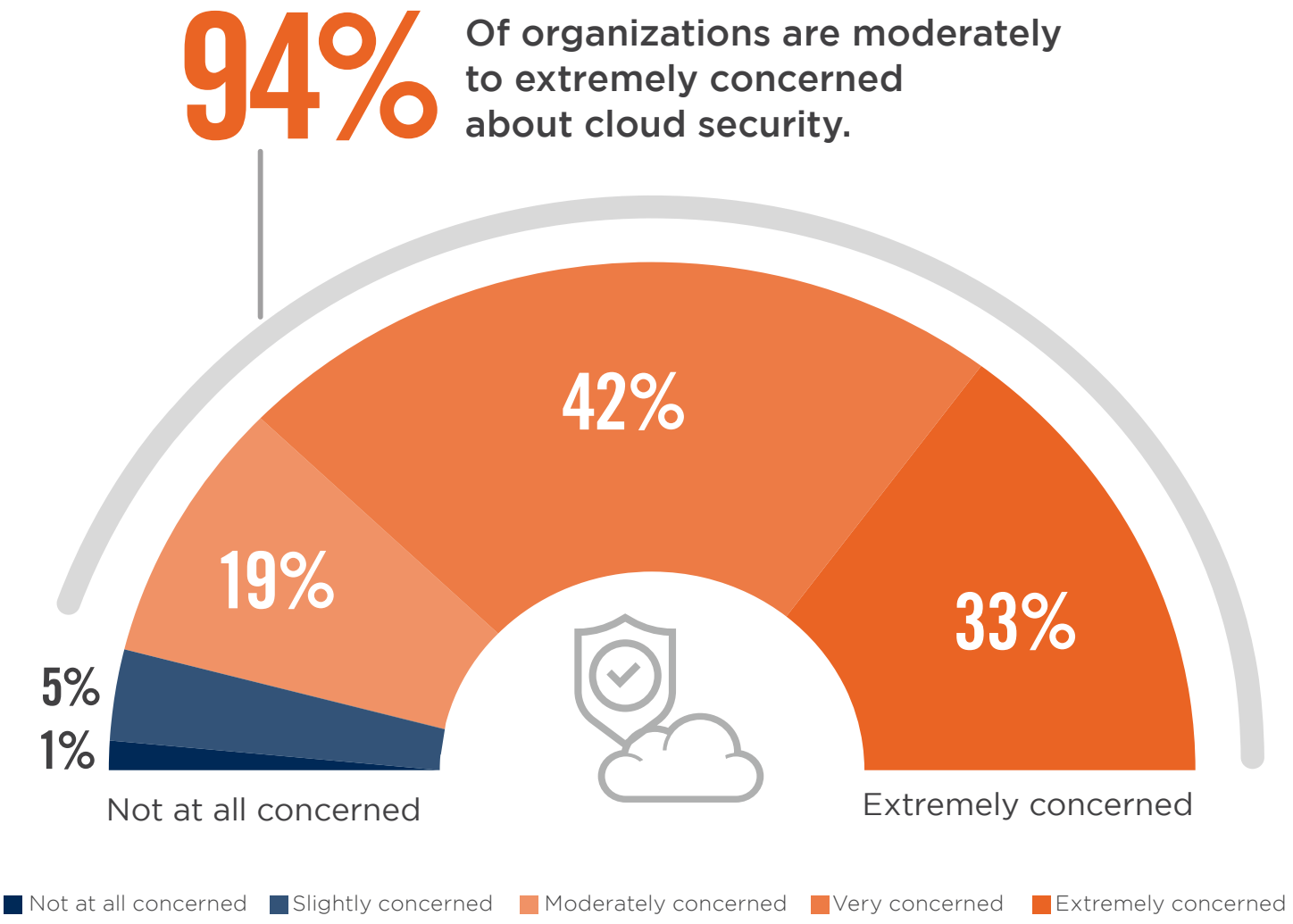
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

SECURITY IN PUBLIC CLOUDS

Security remains a key issue for cloud customers, despite continued rapid adoption of cloud computing. A majority of cybersecurity professionals (94%) confirm they are at least moderately concerned about public cloud security, a small increase from last year's survey.

How concerned are you about the security of public clouds?

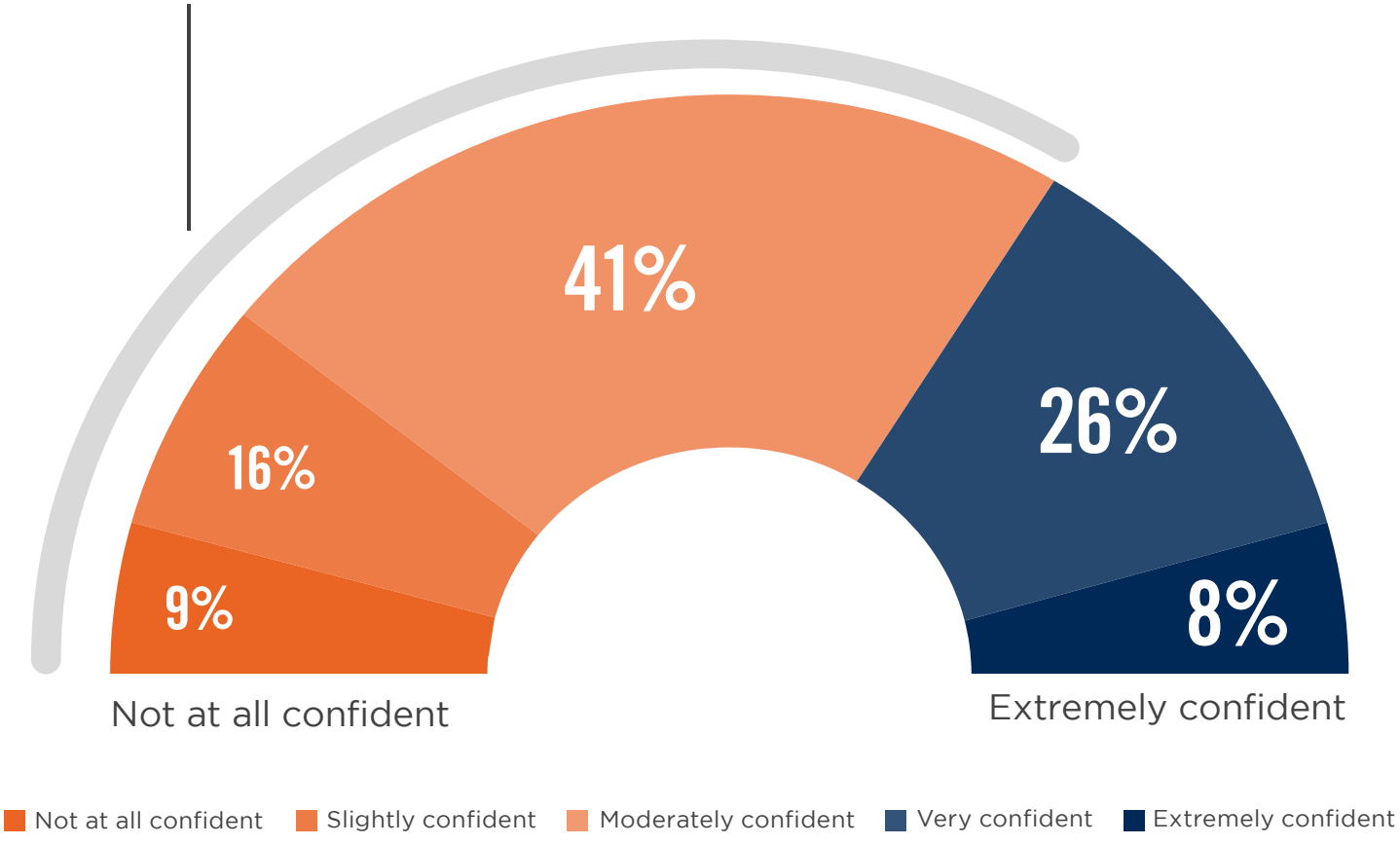


CLOUD SECURITY CONFIDENCE

Most organizations are not confident at all to moderately confident in their cloud security posture (66%). While confidence has been declining from 84% last year, we still see a degree of overconfidence not supported by the backdrop of security incidents and challenges presented in this report.

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

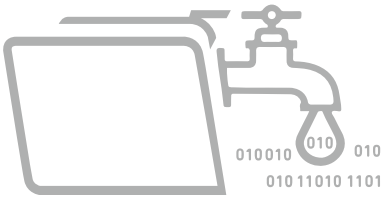
66% **Of organizations are not confident at all to moderately confident in their cloud security posture.**



CLOUD SECURITY CONCERNS

Cloud providers offer increasingly robust security measures as part of cloud services, but customers are ultimately responsible for securing their workloads in the cloud. The top cloud security challenges highlighted in our survey are about data loss/leakage (69% - up five percentage points since last year) and data privacy/confidentiality (66% - up four percentage points). This is followed by concerns about accidental exposure of credentials and incident response (tied at 44% and up from 29% last year).

What are your biggest cloud security concerns?

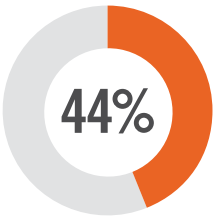


69%

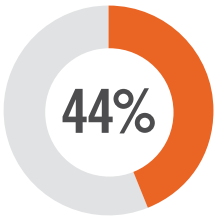
Data loss/leakage

66%

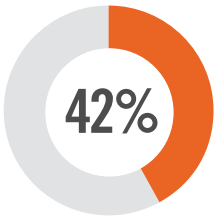
Data privacy/ confidentiality



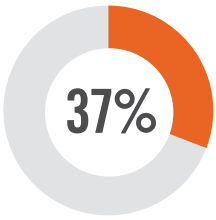
Accidental exposure of credentials



Incident response



Legal and regulatory compliance



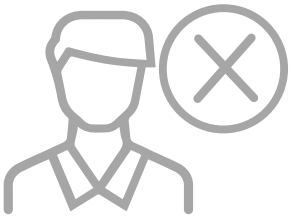
Data sovereignty/ residency/control

Visibility & transparency 30% | Availability of services, systems and data 28% | Lack of forensic data 27% | Business continuity 26% Liability 24% | Fraud (e.g., theft of SSN records) 24% | Disaster recovery 23% | Having to adopt new security tools 21% | Performance 19% | Not sure/other 8%

OPERATIONAL SECURITY HEADACHES

As more workloads continue to move to the cloud, cybersecurity professionals are increasingly realizing the complications with protecting these workloads. Lack of qualified security staff (47%) has risen to the number one spot on the list of day-to-day headaches, up from the third spot on last year's survey. This is followed by compliance (40%) and setting consistent security policies across cloud and on-premises environments (36%).

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



47%

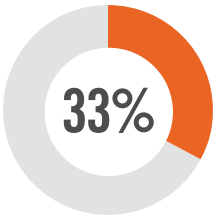
Lack of qualified staff

40%

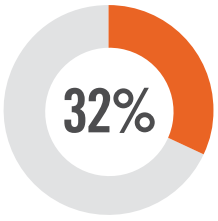
Compliance

36%

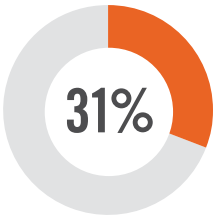
Setting consistent security policies



Visibility into infrastructure security



Can't identify misconfigurations quickly



Security can't keep up with pace of change in applications

Lack of integration with on-premises security technologies

Securing traffic flows 27% | Understanding network traffic patterns 27% | Justifying more security spend 25% | Securing access from personal and mobile devices 25%

BARRIERS TO CLOUD ADOPTION

Cloud computing is still not without challenges. Among the barriers to cloud adoption, organizations mention lack of qualified staff (37%) as the biggest impediment to faster adoption – up from the fifth spot on last year's survey. This is followed by challenges regarding integration with existing IT environments, and data security issues (tied at 35%).

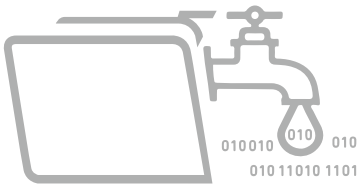
What are the biggest barriers holding back cloud adoption in your organization?

37%

Lack of staff resources or expertise

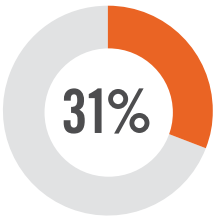
35%

Integration with existing IT environment

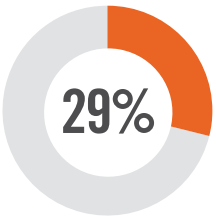


35%

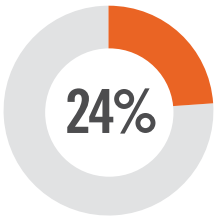
Data security, loss & leakage risks



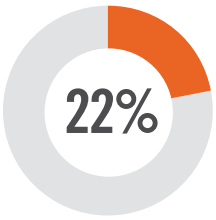
Legal & regulatory compliance



General security risks



Lack of budget



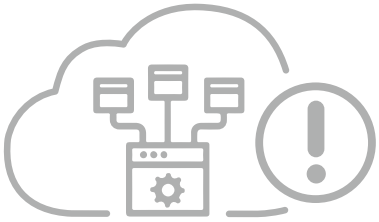
Fear of vendor lock-in

Loss of control 20% | Complexity managing cloud deployment 19% | Internal resistance and inertia 18% | Cost/lack of ROI 16%
Lack of management buy-in 14% | Lack of transparency and visibility 13%

BIGGEST CLOUD SECURITY THREATS

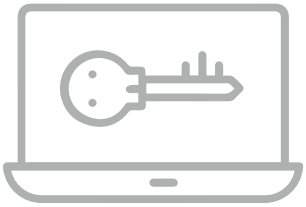
When asked about what are the biggest security threats facing public clouds, organizations ranked misconfiguration of the cloud platform (68%) highest, up from the third spot on last year's survey. This is followed by unauthorized access (58%), insecure interfaces (52%), and hijacking of accounts (50%).

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



68%

Misconfiguration of the cloud platform/ wrong setup



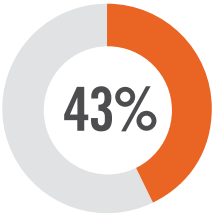
58%

Unauthorized access

52%

Insecure interfaces /APIs

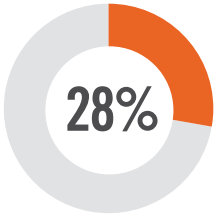
Hijacking of accounts, services or traffic



External sharing of data

Malicious insiders

Foreign state-sponsored cyber attacks

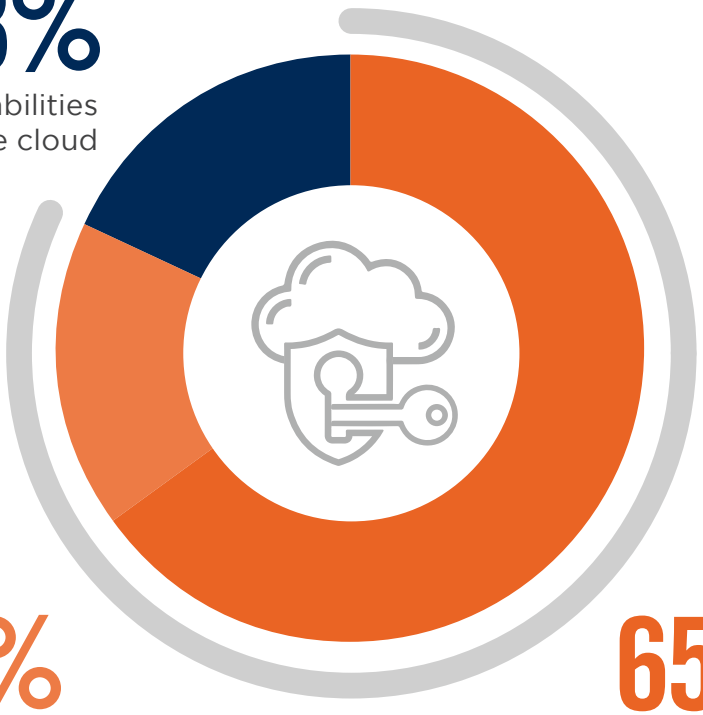


Denial of service attacks

TRADITIONAL TOOLS IN THE CLOUD

As workloads continue to move to the cloud, organizations are faced with unique security challenges presented by cloud computing. Most legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. Eighty-two percent of respondents say traditional security solutions either don't work at all in cloud environments or have only limited functionality – a marked deterioration from last year's survey (66%).

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



18%
All capabilities work in the cloud

82%
Claim traditional security solutions either don't work at all or have limited functionality.

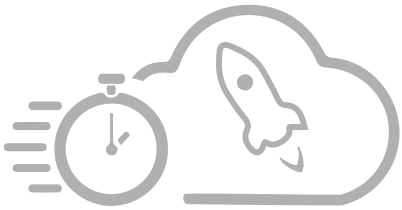
17%
Our traditional network security tools don't work in the cloud

65%
Limited functionality

DRIVERS OF CLOUD-BASED SECURITY SOLUTIONS

The rapid adoption of cloud computing is driven by a number of undeniable advantages. Organizations recognize several key drivers of deploying cloud-based security solutions, including faster time to deployment and cost savings (tied at 41%). This is followed by reduced efforts around patches and software updates (40%).

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



41%

Faster time to deployment

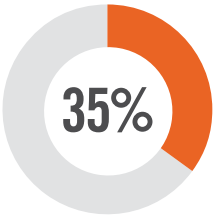
41%

Cost savings

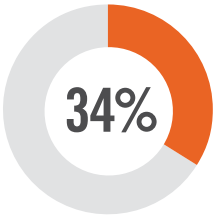
40%

Reduced efforts around patches and upgrades of software

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)

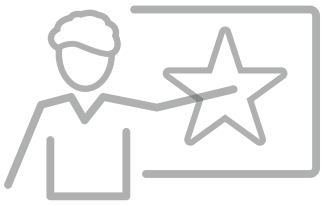
Meet cloud compliance expectations

Better performance 30% | Easier policy management 26% | Reduction of appliance footprint in branch offices 21% | Other 5%

BARRIERS TO CLOUD-BASED SECURITY ADOPTION

Despite the significant advantages offered by cloud-based security solutions, 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 (55%) continues to rank as the highest barrier, followed by budget challenges (46%), data privacy concerns (37%), and lack of integration with on-premises platforms (36%).

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



55%

Staff expertise/ training

46%

Budget

37%

Data privacy

Lack of integration with on-premises security technologies

Solution maturity

Regulatory compliance requirements

Data residency

Sunk cost into on-premises tools 24% | Integrity of cloud security platform (DDoS attack, breach) 17% | Limited control over encryption keys 15% | Scalability and performance 12% | Not sure/other 10%

CLOUD BENEFITS REALIZED

When asked about cloud benefits, the organizations participating in this survey generally confirm that cloud is delivering on its promise of flexible capacity and scalability (51%), improved availability (46%), and increased agility (45%).

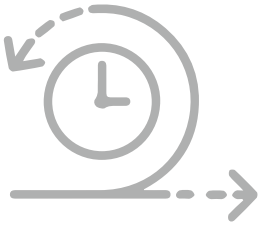
What overall benefits have you already realized from your cloud deployment?

51%

More flexible capacity/scalability

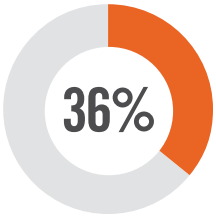
46%

Improved availability and business continuity



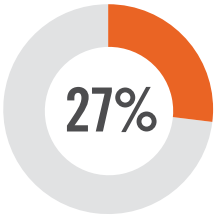
45%

Increased agility

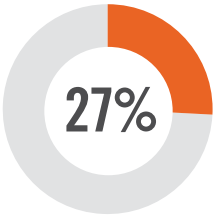


Accelerated deployment and provisioning

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



Reduced cost



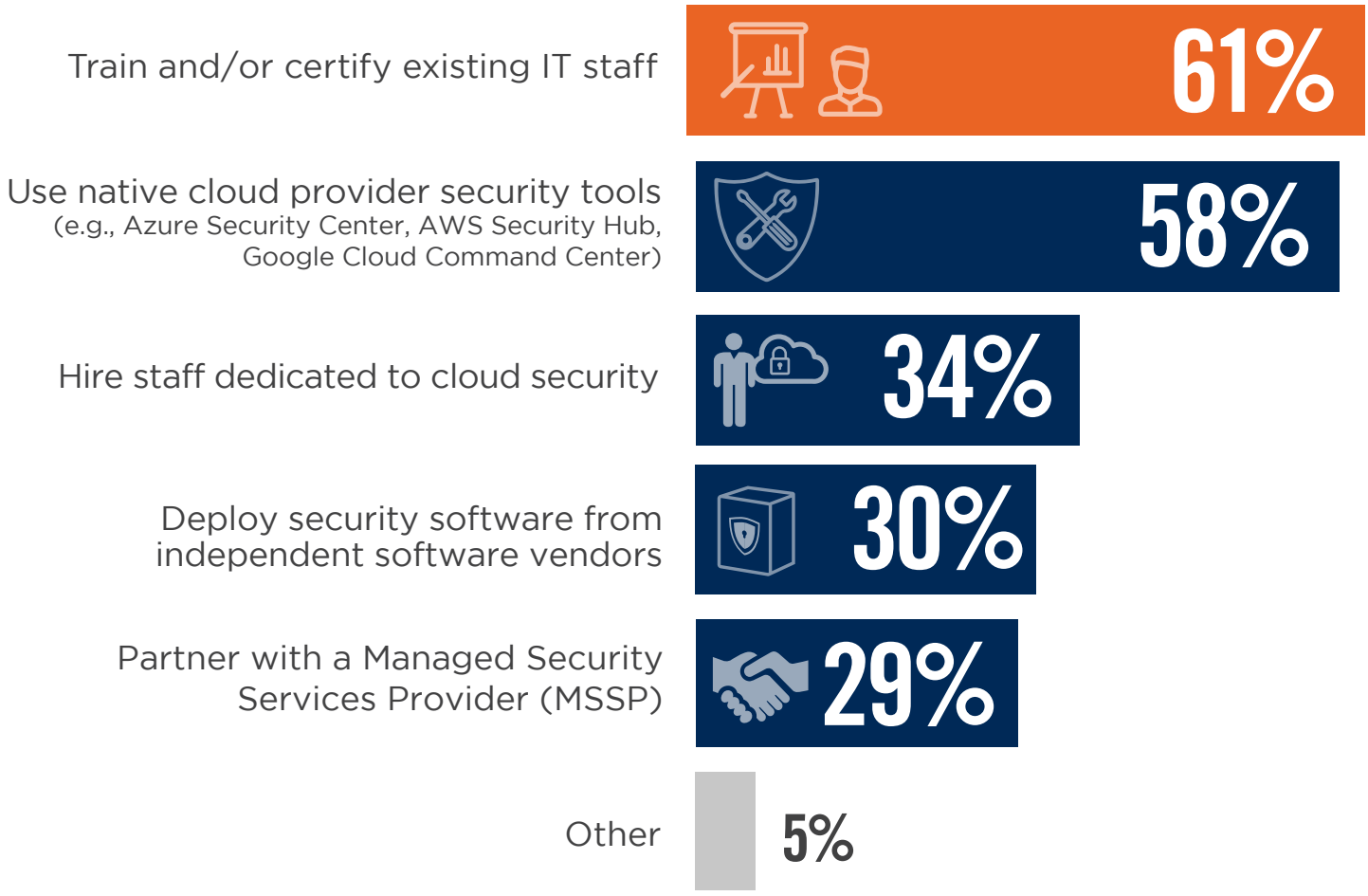
Increased geographic reach

Accelerated time to market 26% | Improved security 23% | Improved performance 23% | Reduced complexity 21%
Increased employee productivity 20% | Improved regulatory compliance 13% | Not sure/other 13%

PATHS TO STRONGER CLOUD SECURITY

For the fourth year in a row, training and certifying IT staff (61%) ranks as the primary tactic organizations deploy to assure their evolving security needs are met. Fifty-eight percent of respondents rely on their cloud provider's native security tools, and 34% are looking to hire more staff dedicated to cloud security.

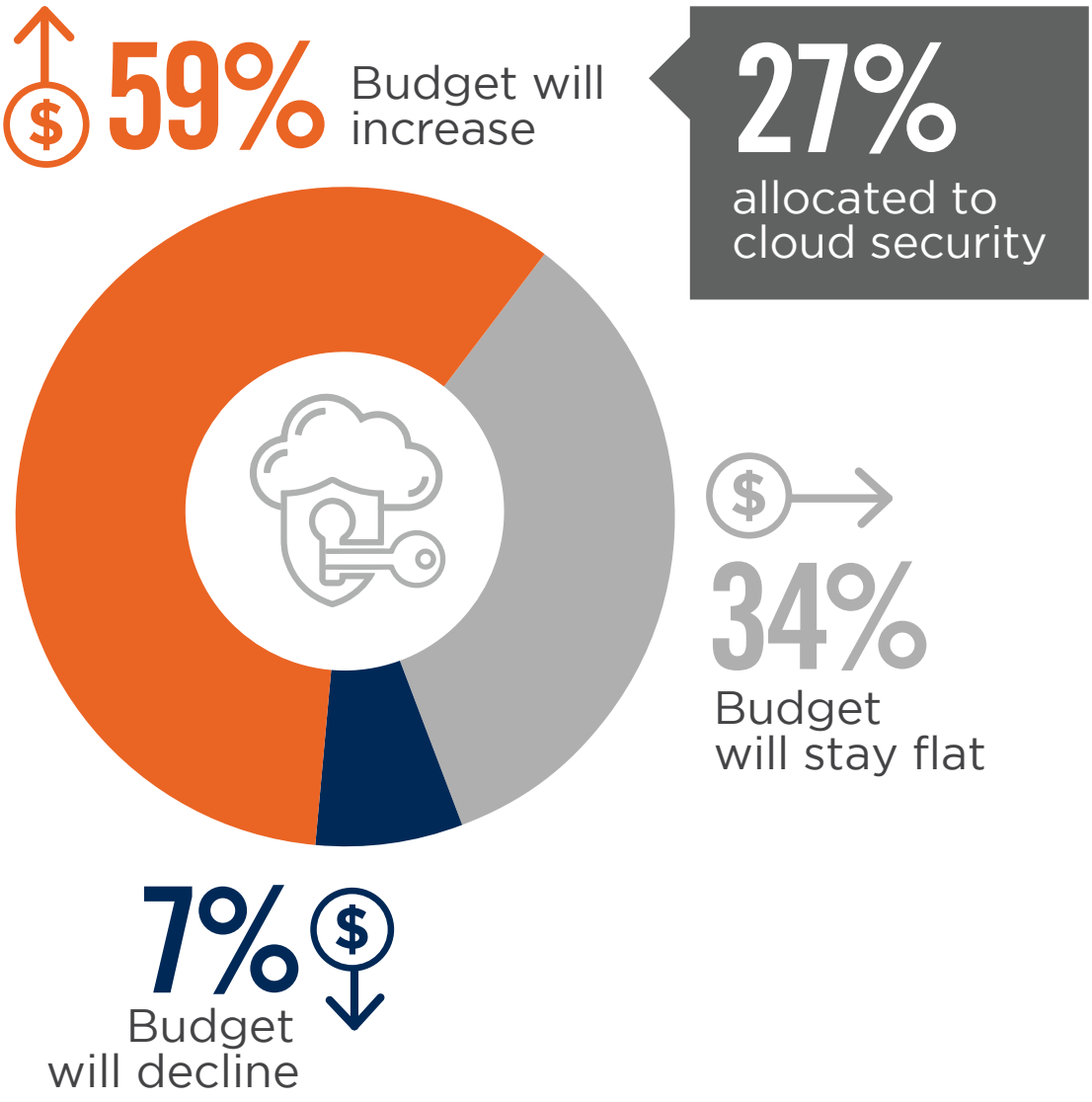
When moving to the cloud, how do you handle your changing security needs?



CLOUD SECURITY BUDGET

A majority, six out of 10 organizations expect their cloud security budget to increase over the next 12 months. On average, organizations allocate 27% of their security budget to cloud security.

How is your cloud security budget changing in the next 12 months?



SECURITY READINESS

When asked how organizations rate their overall security readiness, 69% rate their team's security readiness average or below average. Only half as many say they are above average (31%).

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

TRAINING AND CERTIFICATION

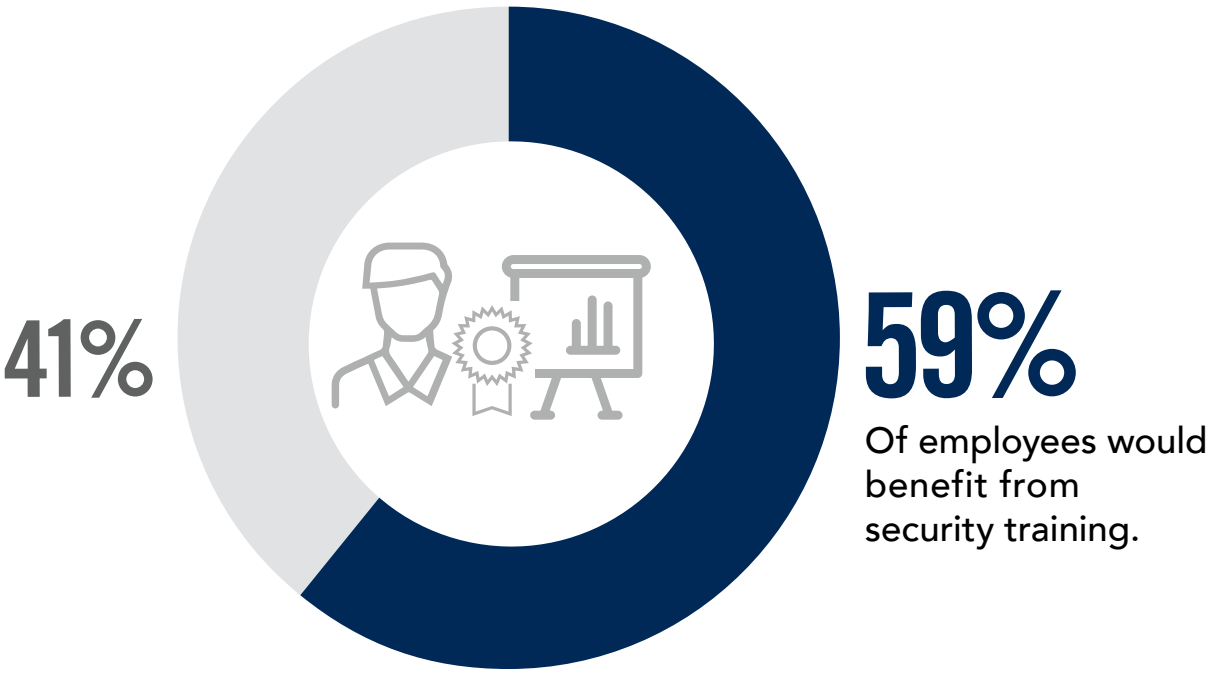
Of those rating their overall security readiness average or below average, 80% believe their teams would benefit from cloud security training and/or certification.

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 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. Cybersecurity professionals agree that 59% of 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?



Top 10 most valued security certifications

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

TRAINING FOCUS

When it comes to prioritizing topics for security training, cybersecurity professionals in our survey selected cloud-enabled cybersecurity (66%), followed by application security (45%), and risk-based frameworks (43%) as the most valuable topics for training and education success.

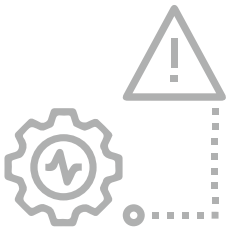
Which of the following topic areas would you find most valuable for ongoing training and education to be successful in your current role?

66%

Cloud-enabled cybersecurity

45%

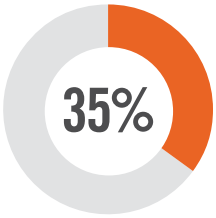
Application security



43%

Risk-based frameworks

Incident response



DevOps

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

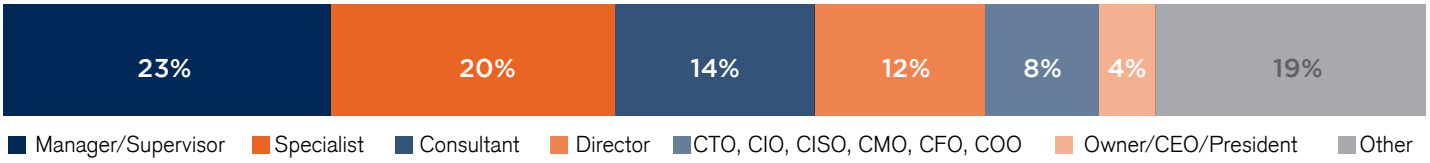
Regulatory compliance

Mobile security 29% | Digital forensics 25% | Open source vulnerabilities 21% | Internet of Things (IoT) 21% | PII 21% | Identifying social engineering/phishing 17% | Not sure/other 6%

METHODOLOGY & DEMOGRAPHICS

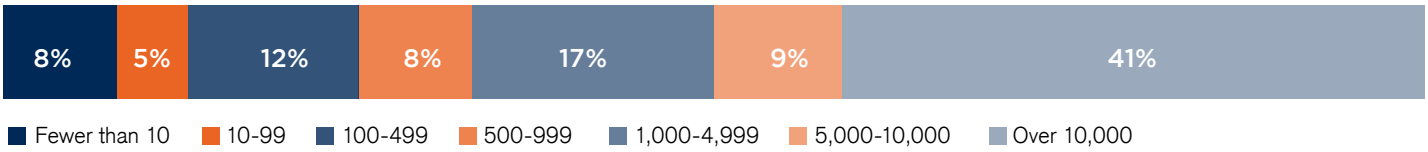
The 2020 Cloud Security Report is based on a comprehensive survey of 653 cybersecurity professionals conducted in May 2020 to uncover how cloud user organizations are responding to security threats in the cloud, and what training, certifications and best practices IT cybersecurity leaders are prioritizing 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

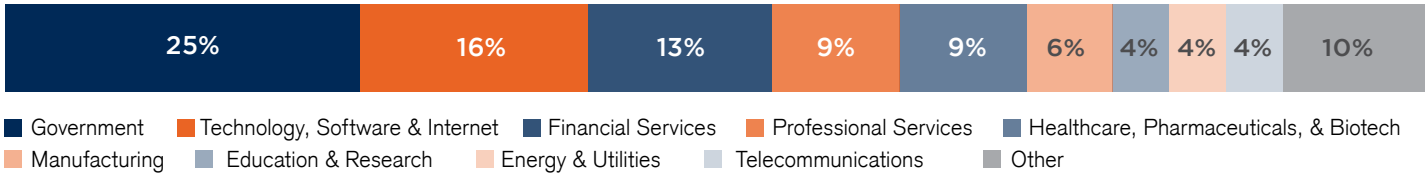


DEPARTMENT

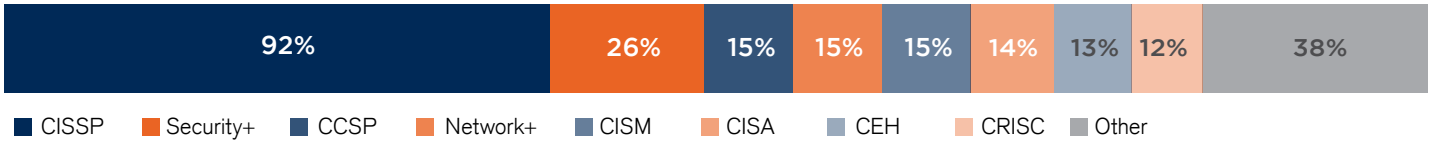
COMPANY SIZE



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 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 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.

The Path to Stronger Cloud Security

CCSP®
Certified Cloud Security Professional
An (ISC)² Certification

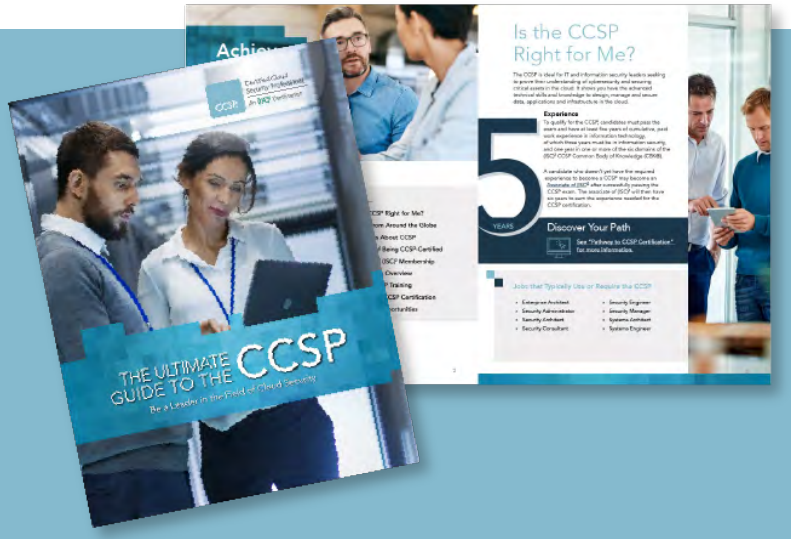
61%

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

34%

want to hire staff dedicated to cloud security.

Start with The Ultimate Guide to the CCSP



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 >