CCSP® Certified Cloud Security Professional

An (ISC)² Certification

10 REASONS
Why Demand for Cloud Security Is Sky-High

Inside

The State of Cloud Security

Organizations are migrating data, applications and services from on-premises data centers to the cloud, seeking to innovate, disrupt their markets and reap the benefits the cloud delivers: flexible capacity, scalability, improved availability and increased agility.

The migration process is not without concerns, however. In fact, it's a balancing act, where organizations need to plan the most effective migration scenarios.

Many have opted to migrate to multiple cloud environments to avoid vendor lock-in. Recent research by Thales shows multicloud adoption is widespread not only among large-scale organizations but also in small and medium businesses. SaaS usage is the most pervasive, with 64% of the global respondents having 26 or more SaaS applications. At the same time, 74% of organizations are using two or more PaaS vendors, and 56% are using at least two IaaS providers.

Source: 2021 Thales Global Cloud Security Study
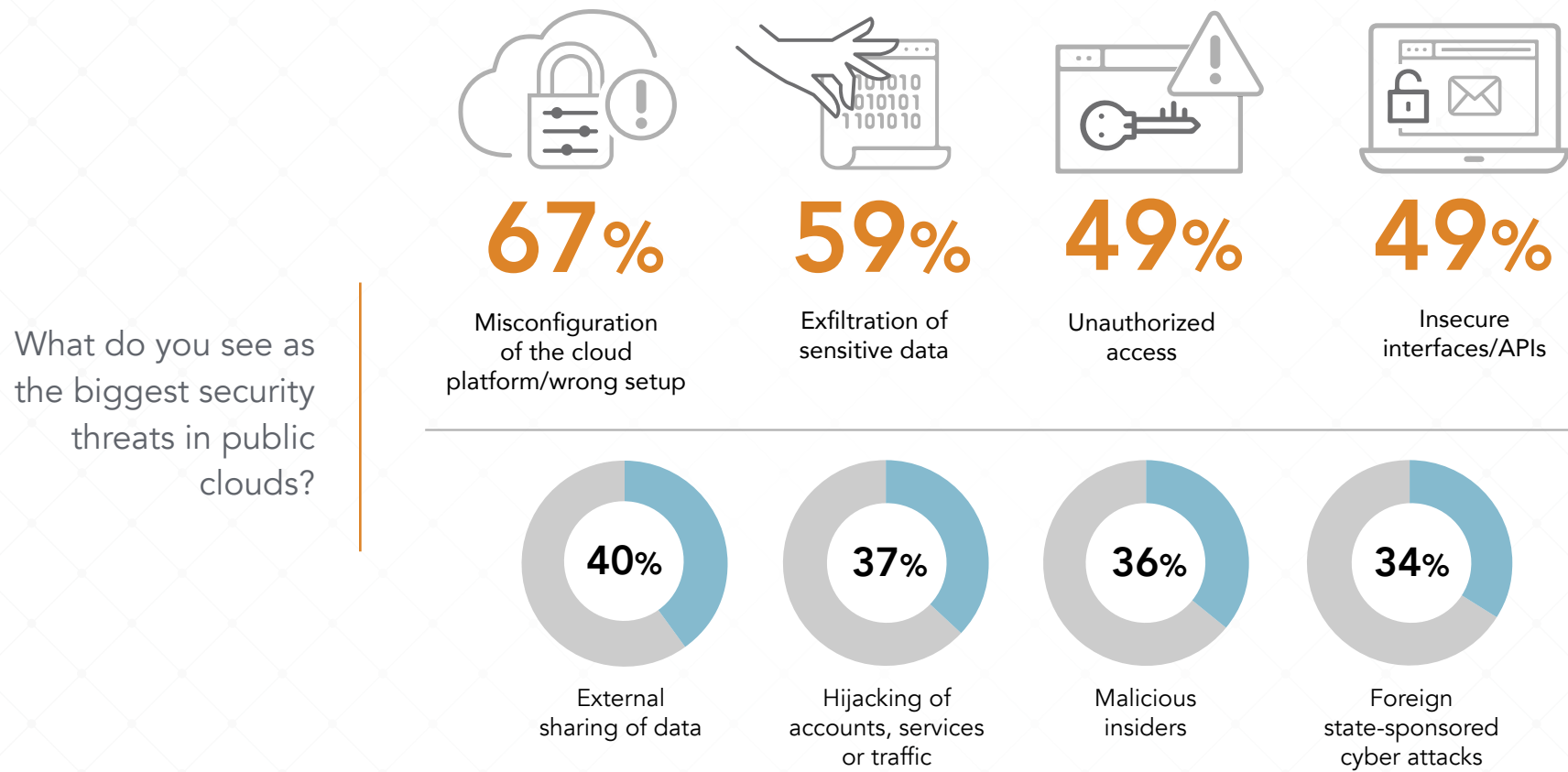
SaaS USAGE IS THE MOST PERSVASIVE with

64%

of global respondents having 26 or more Saas applications.

Prove Your Cloud Security Expertise. Get The Ultimate Guide to the CCSP and learn how.

3

Cloud adoption blurs traditional corporate boundaries and renders traditional security controls inappropriate. Most legacy security tools are not designed for the dynamic, distributed, virtual environments of the cloud. In fact, 81% of organizations say traditional security solutions don't work at all in cloud environments or have only limited functionality, according to the 2021 Cloud Security Report.

Lack of adequate security protections creates holes and threats, which bad actors are eager to exploit. The biggest security threats are misconfiguration of the cloud platform (67%), exfiltration of sensitive data (59%), unauthorized access (49%), insecure interfaces/APIs (49%), external sharing of data (40%) and hijacking of accounts, services or traffic (37%).

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

40%
External sharing of data

37%
Hijacking of accounts, services or traffic

36%
Malicious insiders

34%
Foreign state-sponsored cyber attacks

Source: 2021 Cloud Security Report

Prove Your Cloud Security Expertise. Get The Ultimate Guide to the CCSP and learn how.
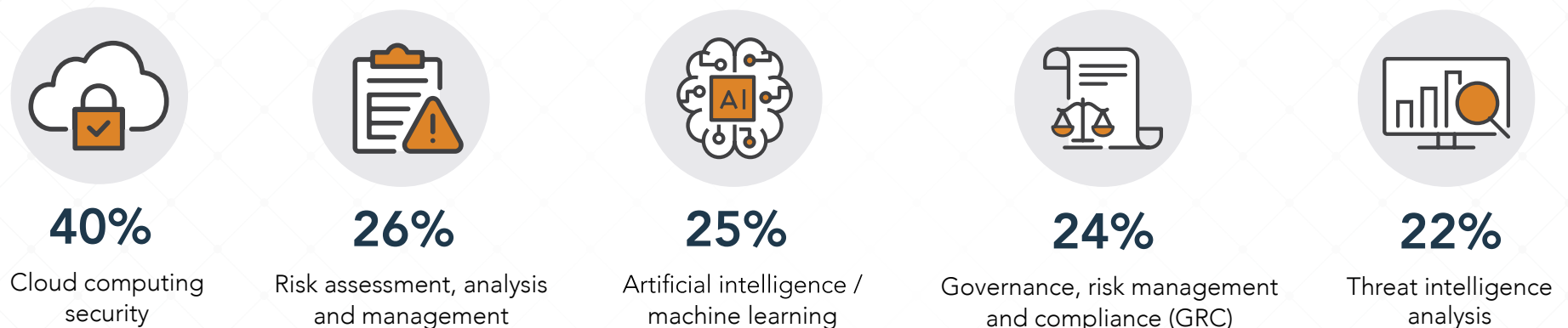
4

Adoption of effective cloud security doesn't come without barriers. Complexity is a significant factor to consider and is self-inflicted by the dominance of multicloud environments. The 2021 Cloud Security Report reveals that the biggest challenge organizations face is the lack of staff expertise and training. According to Global Knowledge, 75% of IT decision-makers say their teams lack the skills they need.

Because of the skills gap, organizations are scrambling to fill cloud security positions. Organizations are seeking to train and certify IT team members to ensure their evolving security needs are met. As a result, 40% of industry professionals plan to pursue cloud security training within the next two years, according to the 2021 Cybersecurity Workforce Study. This trend will continue to grow as organizations turn to cloud-based solutions versus on-premises legacy ones.

Top Areas of Professional Development Participants are Pursuing

40%	**26%**	**25%**	**24%**	**22%**
Cloud computing security	Risk assessment, analysis and management	Artificial intelligence / machine learning	Governance, risk management and compliance (GRC)	Threat intelligence analysis

Source: 2021 Cybersecurity Workforce Study

Demand for cloud security talent has produced ample opportunities for careers in the field. Cloud security tops the list of technical concepts and systems those seeking a career in cybersecurity should pursue, according to the 2021 Cybersecurity Workforce Study.

Category	Rating
Cloud Security	4.46
Malware Analysis	4.44
Data Analysis	4.42
Threat Assessment	4.42
Intrusion Dectection	4.42
Risk Assessment/Management	4.37
Encryption	4.37
Secure Software Development	4.37
Networking	4.34
Database	4.32
Penetration Testing	4.27
Backup and Storage	4.26
Coding/Programming	4.26
Access Management	4.22
Alert and Event Management	4.22
Hardware	4.21
Compliance	4.19
Forensics	4.08
Administration	4.03
Architecture	3.97

Source: 2021 Cybersecurity Career Pursuers Study

10 REASONS
Why Demand for Cloud Security Is Sky-High

With more cyberattacks targeting cloud workloads, organizations are becoming less confident about their cloud security posture. They need to ensure a holistic and effective approach to cybersecurity, and they're turning to cloud security professionals to play a major role. Robust cloud security teams benefit organizations in a multitude of ways. Here are 10 top reasons demand for cloud security is sky-high.

1. To Minimize the Impact of a Security Event

The damages that follow cyber-related incidents are detrimental. Organizations need cloud security professionals to defend against breaches and prevent these repercussions of falling victim to a cyberattack:

- Loss of revenue
- Reputation damage
- Loss of clients
- Operational disruptions
- Lawsuits
- Intellectual property cyber theft
- Theft of personally identifiable information
- Compromised client data, sensitive business information and equipment

2. To Build a Culture of Security

A comprehensive awareness program led by cloud security professionals sets clear expectations across the organization. It educates team members about how to recognize attack vectors, help prevent cyber-related incidents and respond to potential threats. Training teams about safe online computing, strong authentication and social engineering is critical to ensuring the confidentiality of sensitive business data.

3. To Ensure Business Resiliency

Building a strong, knowledgeable, resilient cloud security team that isn't dependent on a few irreplaceable employees helps ensure organizational continuity and financial stability. A team of individuals with a variety of cloud security skills also has a positive impact on business decision-making and innovation.

4. To Meet the Challenge of Regulatory Compliance

Organizations operate under specific regulatory environments. While there are industry-specific standards and regulations, such as PCI DSS or HIPAA, that dictate how organizations should protect sensitive data, there are also cross-industry, national or transnational regulations that safeguard the confidentiality and integrity of personal data. Regulations like GDPR or CCPA have strict data security requirements and impose costly fines when breaches occur.

Cloud security professionals trained in these regulatory requirements help maintain compliance. This legal background allows them to effectively configure cloud platforms and select the controls that are appropriate for safeguarding assets in the cloud.

5. To Accelerate Innovation

IT leaders recognize the importance of retaining cloud security professionals who fully understand complex and quickly changing cloud environments. Their organizations function more effectively with a uniformly shared foundation of cloud security knowledge, which also benefits the time-to-value for new products and services.

6. To Strengthen Employee Retention

Experienced cloud team members who work with early-career cloud security professionals have more time to take on the high-value facets of projects. They're able to do the initial planning, then focus on more complex tasks, such as strategy and design. This is an advantage not only for the teams but for the organization. As team member tasks are better-aligned to their abilities, they remain with the organization longer.

7. To Foster Confidence and Minimize Stress

Security teams are often overwhelmed by the volume of incidents they need to mitigate daily, and they may experience stress caused by news of data breaches. Cloud security professionals help mitigate anxiety caused by cybersecurity uncertainty by minimizing risky actions and instilling security best practices across the organization.

8. To Save Time and Resources

Hiring newly certified cloud security professionals is critical for small and medium organizations that lack the funds to bring highly experienced specialists on their teams. Rather than hiring for hard-to-find technical skills alone, enhancing the knowledge base of entry-level practitioners with technical aptitude, potential, and enthusiasm is a wise investment for the future.

9. To promote Customer Satisfaction

Data breaches damage reputations and dissolve the confidence their clients and customers hold in the company. Some customers could even pursue legal action. By hiring cloud security professionals to protect assets, organizations foster trust and customer satisfaction.

10. To Stand Out Competitively and Secure Long-Term Success

As organizations move to multicloud platforms, vendor-neutral cloud security professionals help ensure they remain agile and can adapt quickly to changes in the industry. Cloud security professionals are critical to staying on top of the latest technologies, developments and threats.

Prove Your Cloud Security Expertise. Get The Ultimate Guide to the CCSP and learn how.

10
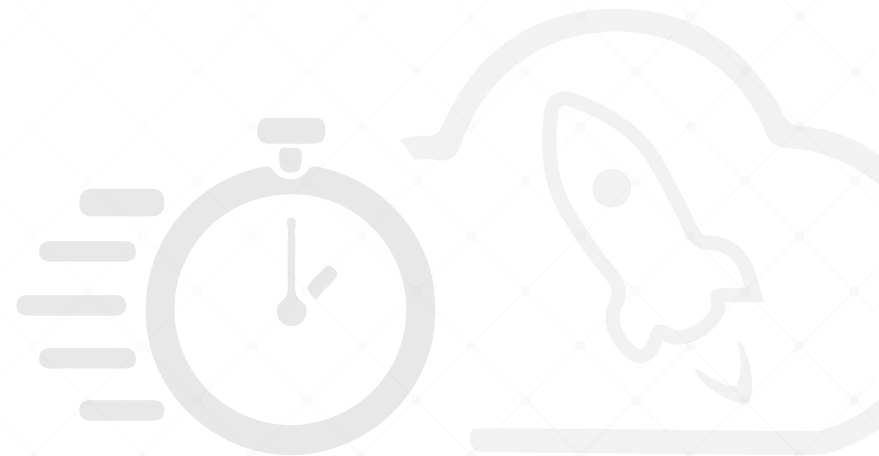
Why Why Vendor Neutral Matters

As more businesses opt for multicloud environments, vendor-neutral certification is highly desirable for cloud security team members.

Vendor-neutral certification broadens operational knowledge and provides professionals with the big picture about cloud computing and security. A vendor-agnostic cloud certification helps in understanding concepts like legal compliance, roles and responsibilities and alignment of security objectives with business goals.

In contrast, vendor-native certifications offered by cloud providers focus only on configuring and operating in the specific platforms, limiting the scope and the applicability of the knowledge gained.

Certified Cloud Security Professional
An **(ISC)²** Certification

CCSP®

What Role CCSP Certification Plays

(ISC)² Certified Cloud Security Professional (CCSP) demonstrates that you have the advanced knowledge and technical skills to design, manage and secure data, applications and infrastructure in the cloud. It positions you as an authority in cloud security, highly proficient in staying on top of the latest technologies, developments and threats.

CCSP is a vendor-neutral certification that shows you have the knowledge and skills to successfully secure any cloud environment. Vendor-neutral certification gives you a balanced approach and knowledge base of all aspects of cloud security, including the advantages and limitations of technologies.

If you already hold a vendor-specific certification, CCSP builds the end-to-end foundational knowledge needed for effective cloud security. It extends your skills and allows you to apply your security expertise to multiple cloud environments.

The knowledge and skills gained with CCSP certification are valuable for professionals in any stage of their career.

Entry-Level

CCSP allows entry-level professionals to leverage the training offered by cloud providers and apply it to multicloud environments. They're able to translate and implement cloud security policies into well-established, robust practices and solutions to protect the corporate data.

Middle Management

Middle management professionals complement their business experience with CCSP by gaining technical foundational knowledge about the risks and challenges of cloud computing. They're able to advise senior executives, aligning business objectives with security goals and contributing to defense in depth.

Senior Management

CCSP helps senior managers develop strategies that drive the business journey to innovation and success. Understanding how secure cloud computing increases revenue empowers them to make the right decisions.
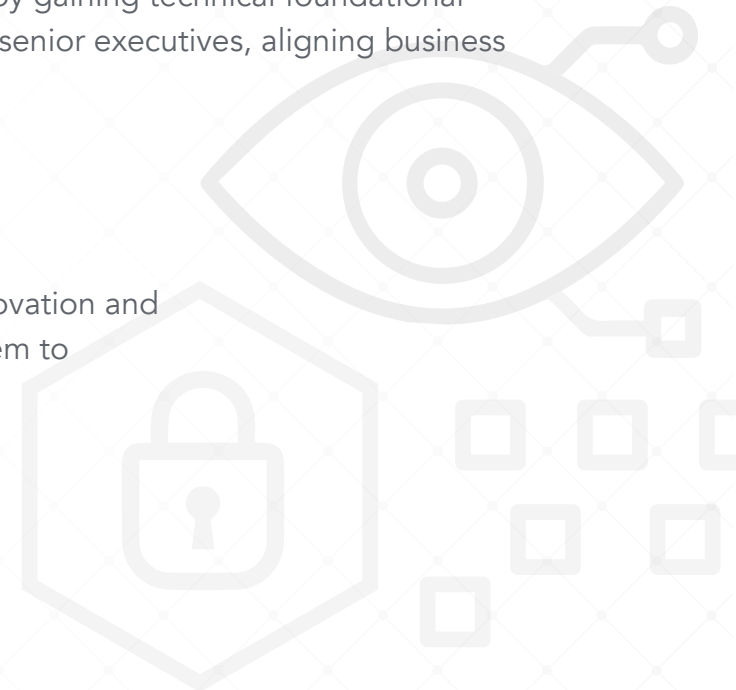
Flexible Training for CCSP

As the world's largest nonprofit association of certified cybersecurity professionals, we offer Official (ISC)² Training for CCSP. We also work with leading training partners around the world.

When you choose Official (ISC)² Training, you benefit from:

- **Top-notch instruction** from authorized instructors who are (ISC)²-certified, average 15–20 years of industry experience and complete a rigorous process to teach the CBK®

- **Comprehensive exam prep** covering all current exam topic areas with a focus on real-world learning activities and scenarios.

- **Most up-to-date content** for deep awareness and understanding of new threats, technologies, regulations and best practices.

Everyone has their own style of learning. That's why we offer three options to help guide you in CCSP certification. Find Training Today!

1. Self-Paced

Your self-guided tour toward certification

- Learn online at your own pace
- Download videos from an (ISC)[2] Authorized Instructor
- Access instructor support (48-hour email response time)

2. Online Instructor-Led

Your guided group tour toward certification

- Learn live virtually from an (ISC)[2] Authorized Instructor
- Collaborate with team members
- Prepare with the Official (ISC)[2] Student Training Guide

3. Classroom-Based

Your guided small group tour (10 or more students) toward certification

- Learn in-person at your office or a private venue near you
- Interact with an (ISC)[2] Authorized Instructor and students
- Coordinate training around your schedule

Get The Ultimate Guide to the CCSP

Take the next step toward cloud security certification with __The Ultimate Guide to the CCSP__. It covers everything to know about the world's leading cloud security credential. Find out how CCSP and (ISC)² can help you discover your certification path, create your plan and rise to the top in cloud security.

It's All Inside!

- Is CCSP Right for Me?
- CCSPs Around the Globe
- Fast Facts about CCSP
- Benefits of CCSP Certification
- Benefits of (ISC)² Membership
- CCSP Exam Overview
- Official CCSP Training
- Pathway to CCSP Certification
- Free CPE Opportunities

Get Your Guide
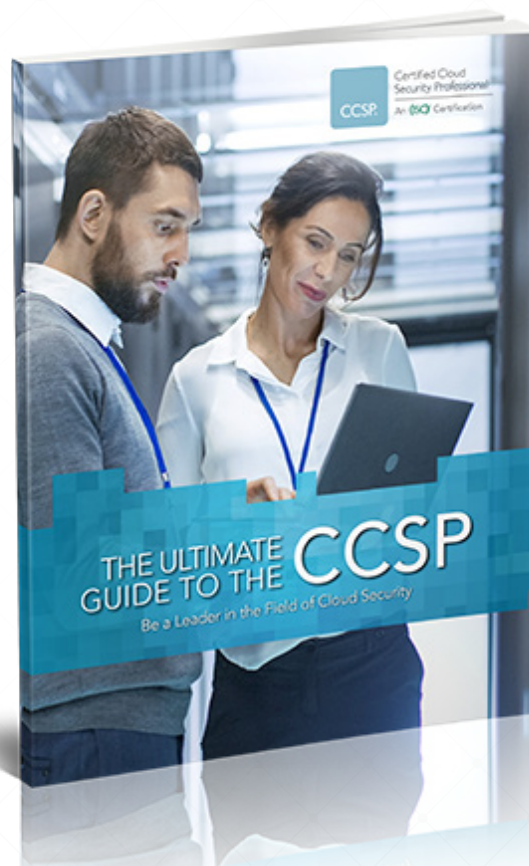
About (ISC)²

(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, programmatic approach to security. 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 – <u>The Center for Cyber Safety and Education</u>™.

Learn more at <u>www.isc2.org</u> or follow us on <u>Twitter</u> or connect with us on <u>Facebook</u> and <u>LinkedIn</u>.