

CompTIA CASP+

What is it?

CompTIA Advanced Security Practitioner (CASP+) is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness.

Why is it different?

- **CASP+ is the only hands-on, performance-based certification for advanced practitioners** — not managers — at the advanced skill level of cybersecurity. While cybersecurity managers help identify what cybersecurity policies and frameworks could be implemented, CASP+ certified professionals figure out how to implement solutions within those policies and frameworks.
- **Unlike other certifications, CASP+ covers both security architecture and engineering** — CASP+ is the only certification on the market that qualifies technical leaders to assess cyber readiness within an enterprise, and design and implement the proper solutions to ensure the organization is ready for the next attack.

About the exam

CASP+ is an advanced-level cybersecurity certification covering technical skills in security architecture and senior security engineering in traditional, cloud, and hybrid environments, governance, risk, and compliance skills, assessing an enterprise's cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions. Successful candidates will have the knowledge required to:

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise
- Use monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environment
- Apply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniques
- Consider the impact of governance, risk, and compliance requirements throughout the enterprise



Exam

CAS-004

Release Date

August 2021

Languages

English

CE Required?

Yes

Accreditation





Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved for the U.S. Department of Defense Directive 8140.03-M.

What's in this version?

Information security threats are on the rise globally. Organizations are increasingly concerned over the lack of adequately trained senior IT security staff's ability to effectively lead and manage the overall cybersecurity resiliency against the next attack. Updates to CASP+ qualify advanced skills required of security architects and senior security engineers to effectively design, implement, and manage cybersecurity solutions on complex enterprise networks.

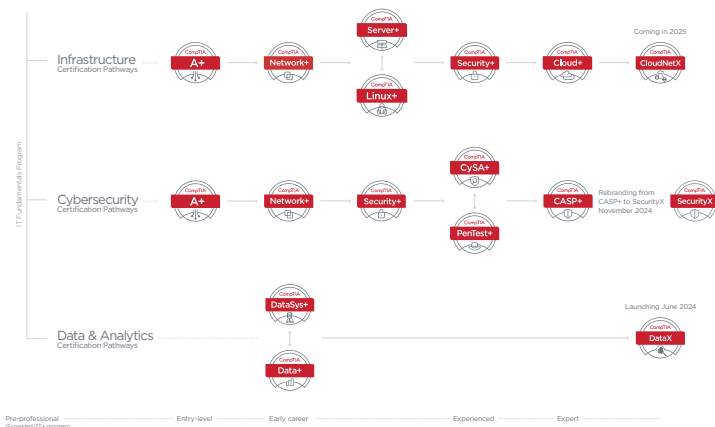
- **Security Architecture** – Expanded coverage to analyze security requirements in hybrid networks to work toward an enterprise-wide, zero trust security architecture with advanced secure cloud and virtualization solutions.
- **Security Operations** - Expanded emphasis on newer techniques addressing advanced threat management, vulnerability management, risk mitigation, incident response tactics, and digital forensics analysis.
- **Security Engineering and Cryptography** – Expanded to focus on advanced cybersecurity configurations for endpoint security controls, enterprise mobility, cloud/hybrid environments, and enterprise-wide PKI and cryptographic solutions.
- **Governance, Risk, and Compliance** - Expanded to support advanced techniques to prove an organization's overall cybersecurity resiliency metric and compliance to regulations, such as CMMC, PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

How does CASP+ Compare to Alternatives?

		 Certified Information Systems Security Professional		
Certification	CASP+	(ISC)2 Certified Information Systems Security Professional (CISSP)	GIAC Certified Enterprise Defender (GCED)	ISACA Certified Information Security Manager (CISM)
Performance-based Questions	Yes	No	No	No
Exam Length	90 questions, 165 minutes	100-150 questions, 3 hours	115 questions, 3 hours	150 questions, 4 hours
Experience Level	Advanced	Advanced	Advanced	Advanced
Exam Focus	Cybersecurity Practitioner Skills, Architect & Engineer	Cybersecurity Management Skills	Cybersecurity Practitioner Skills, Engineer	Cybersecurity Management Skills
Prerequisites	Recommend 10 years of IT administration, including 5 years hands-on, technical security experience.	Documented proof of minimum 5 years full-time IT work experience in two or more of the eight domains.	None. However, students should be aware of the technical level required for the certification.	Documented proof of minimum 5 years IS work experience in three or more of the job practice analysis areas.

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage cybersecurity. Enter where appropriate for you. Consider your experience and existing certifications or course of study.



Top CASP+ Job Roles

- Security Architect
- Senior Security Engineer
- SOC Manager
- Security Analyst
- IT Cybersecurity Specialist/INFOSEC Specialist
- Cyber Risk Analyst

Technical Areas Covered in the Certification

Security Architecture 29%

- Analyze security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network and to provide the appropriate authentication and authorization controls
- Analyze organizational requirements to determine the proper infrastructure security design
- Integrate software applications securely into an enterprise architecture
- Implement data security techniques for securing enterprise architecture and implement secure cloud and virtualization solutions
- Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements

Security Operations 30%

- Given a scenario, perform threat management and vulnerability management activities and analyze those vulnerabilities to recommend risk mitigations
- Use appropriate vulnerability assessment and penetration testing methods and tools
- Analyze indicators of compromise and formulate an appropriate response
- Given a scenario, use processes to reduce risk
- Given an incident, implement the appropriate response
- Explain the importance of forensic concepts

Security Engineering and Cryptography 26%

- Given a scenario, apply secure configurations to enterprise mobility or configure and implement endpoint security controls
- Explain security considerations impacting specific sectors and operational technologies
- Explain how cloud technology adoption impacts organizational security
- Given a business requirement, implement appropriate PKI solution or implement appropriate cryptographic protocols and algorithms
- Given a scenario, troubleshoot issues with cryptographic implementations

Governance, Risk and Compliance 15%

- Given a set of requirements, apply appropriate risk strategies
- Explain the importance of managing and mitigating vendor risk
- Understand compliance frameworks and legal considerations, and their organizational impact
- Explain the importance of business continuity and disaster recovery concepts

Organizations that have contributed to the development of CASP+

- AT&T Cybersecurity
- Lockheed Martin
- Exxon Mobil
- Archdiocese of Philadelphia
- RxSense
- SecureWorks
- U.S. Dept. of State
- U.S. Army
- U.S. Marine Corps
- U.S. Navy Center for Information Dominance
- East Tennessee State University
- Target Corp.
- General Dynamics IT (GDIT)
- Ricoh
- Splunk
- Johns Hopkins University Applied Physics Laboratory

Research and Statistics

Fastest-Growing Job Category Burning Glass predicts that over the next ten years, positions aligned to CASP+ will experience an **18 percent growth rate.**

Growing Value CASP+ is named as one of the top 10 certifications paying the highest premiums, earning IT professionals a **14 percent increase above base salary.**¹

CompTIA Certification Exams



* What does it mean to be a “high stakes” exam?

An extraordinarily high level of rigor is employed in developing CompTIA certifications. Each question created for a CompTIA exam undergoes multiple layers of quality assurance and thorough psychometric statistical validation, ensuring CompTIA exams are highly representative of knowledge, skills and abilities required of real job roles. This is why CompTIA certifications are a requirement for many professionals working in technology. Hiring managers and candidates alike can be confident that passing a CompTIA certification exam means competence on the job. This is also how CompTIA certifications earn the ANSI/ISO 17024 accreditation, the standard for personnel certification programs. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.



* What does it mean to be a “vendor-neutral” exam?

All CompTIA certification exams are vendor-neutral. This means each exam covers multiple technologies, without confining the candidate to any one platform. Vendor-neutrality is important because it ensures IT professionals can perform important job tasks in any technology environment. IT professionals with vendor-neutral certifications can consider multiple solutions in their approach to problem-solving, making them more flexible and adaptable than those with training in just one technology.



* What is a Performance Certification?

CompTIA performance certifications validate the skills associated with a particular job or responsibility. They include simulations that require the test taker to demonstrate multi-step knowledge to complete a task. CompTIA has a higher ratio of these types of questions than any other IT certifying body.

1. Foote Partners, 10 IT certs paying the highest premiums today, 2020