

# CompTIA Security+

## What is it?

CompTIA Security+ is an international, vendor-neutral certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

## Why is it different?

- No other certification that assesses baseline cybersecurity skills has performance-based questions on the exam. Security+ emphasizes hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of issues.
- More choose Security+ for DoD 8570 compliance than any other certification.
- Focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection.
- The new Security+ certification covers the Junior IT Auditor/Penetration Tester job role, in addition to the previous job roles for Systems Administrator, Network Administrator, and Security Administrator

## About the exam

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.



### Exam #

SY0-501

### Release Date

October 2017

### List Price

\$330

### Languages

English, Japanese, Portuguese, & Simple Chinese

### CE Required?

Yes

### Accreditation





Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.

## What's in this version?

The new exam has been updated to better reflect today's best practices for risk management and risk mitigation including the following:

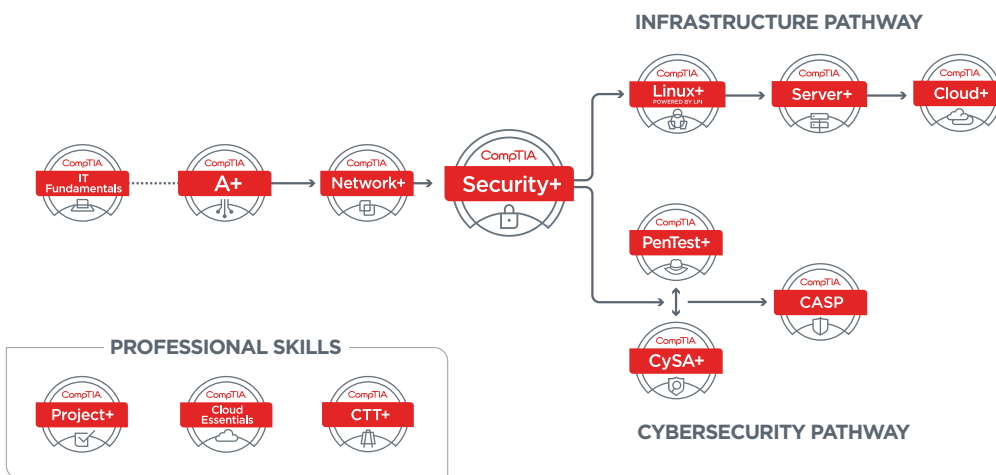
- More emphasis on the practical and hands-on ability to both identify and address security threats, attacks and vulnerabilities.
- Skills covered in Security+ have become a baseline for all cybersecurity jobs and the new version has been updated to reflect how cybersecurity jobs are becoming more specialized, like security analytics. Because of this, the importance of and demand for Security+ has increased for a broader variety of job roles.

## How does Security+ Compare to Alternatives?

| Certification               |  Security+ |  CCNA Security |  EC-Council Certified Ethical Hacker (CEH) |  GIAC Security Essentials (GSEC) |
|-----------------------------|---|---|---|---|
| Performance-based Questions | Yes   | No  | No<br>A second exam, CEH (Practical) offers performance-based questions   | No  |
| Exam Length                 | 1 exam, 90 min  | 1 exam, 90 min  | 1 exam, 4 hrs   | 1 exam, 5 hrs   |
| Experience Level            | Entry-level cybersecurity   | Intermediate  | Intermediate  | Entry-level cybersecurity   |
| Pre-requisites              | CompTIA A+ and Network+ recommended   | CCENT, CCNA Routing and Switching, OR CCIE certification  | CEH Training, 2 years information security experience, Endorsement  | None  |
| Price                       | \$330   | \$250   | \$950   | \$1699  |

## 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.



“When I got out of the Marine Corps, I realized a lot of potential employers require CompTIA Security+. You need more than just job training – you need certifications.”

**Michael Bays**  
Security+  
Certified

## Technical Areas Covered in the Certification

### Threats, Attacks and Vulnerabilities

**21%**

- Analyze indicators of compromise and determine types of malware
- Compare and contrast types of attacks
- Explain threat actor types and attributes
- Explain penetration testing and vulnerability scanning concepts
- Explain the impact of various types of vulnerabilities

### Technologies and Tools

**22%**

- Install and configure network components, both hardware and software-based, to support organizational security
- Use appropriate software tools to assess the security posture of an organization
- Troubleshoot common security issues
- Analyze and interpret output from security technologies
- Deploy mobile devices securely
- Implement secure protocols

### Architecture and Design

**15%**

- Explain use cases and purposes for frameworks, best practices and secure configuration guides
- Implement secure network architecture concepts, secure systems design, and explain the importance of physical security controls
- Explain the importance of secure staging deployment concepts and the security implications of embedded systems
- Summarize secure application development, deployment, cloud and virtualization concepts
- Explain how resiliency and automation strategies reduce risk

### Identity and Access Management

**16%**

- Compare and contrast identity and access management concepts
- Install and configure identity and access services
- Implement identity and access management controls
- Differentiate common account management practices

### Risk Management

**14%**

- Explain the importance of policies, plans and procedures related to organizational security
- Summarize business impact analysis concepts and basic concepts of forensics
- Explain risk management processes and concepts, as well as disaster recovery and continuity of operations concepts
- Follow incident response procedures
- Carry out data security and privacy practices

### Cryptography and PKI

**12%**

- Compare and contrast basic concepts of cryptography
- Explain cryptography algorithms and their basic characteristics
- Install and configure wireless security settings
- Implement public key infrastructure

## Organizations that have contributed to the development of Security+

- Northrop Grumman
- State of Minnesota
- Nationwide
- Southeastern Louisiana University
- Norfolk University
- Office of the Comptroller of the Currency
- Agile Defense, Inc.
- The Johns Hopkins University Applied Physics Laboratory
- Modern Technology Solutions, Inc. (MTSI)
- Archdiocese of Philadelphia
- Fayetteville Technical Community College
- Brotherhood Mutual
- The Joint Commission

## Research and Statistics

### Security Even Higher Priority

About 8 in 10 managers responsible for security at their firms across 12 countries covered in CompTIA's *International Trends in Cybersecurity* **expect security to become an even higher priority** over the next two years.<sup>†</sup>

### Serious Breaches Common

While nearly three-quarters of organizations report experiencing at least one security incident, about 6 in 10 had **one or more serious breaches**.<sup>†</sup>

### Certified Salary

The mean salary for Security+ certified professionals in the United States and Canada is **\$87,666** (overall mean is \$81,165).<sup>2</sup>

### Risk of Human Error

58% of organizations report **human error a major contributor to security risk**. Top sources of human cybersecurity error include (1) general carelessness, (2) failure to get up to speed on new threats, (3) lack of expertise with websites and applications, (4) end user failure to follow policies and procedures, (5) lack of expertise with networks, servers and other infrastructure, and (6) IT staff failure to follow policies and procedures.<sup>†</sup>

## Top Security+ Job Roles

- Systems Administrator
- Network Administrator
- Security Administrator
- Junior IT Auditor/ Penetration Tester
- Security Specialist
- Security Consultant
- Security Engineer

“I needed to establish my career. In this profession, a person who has certifications is more recognized in the market.”

**Wanderley  
Martins**  
Security+  
Certified

## Learn with CompTIA

Official CompTIA Content is the only study material exclusively developed by CompTIA for the CompTIA certification candidate; no other content library covers all exam objectives for all certifications. CompTIA eBooks and CertMaster Products have been developed with our Official CompTIA Content to help you prepare for your CompTIA certification exams with confidence. Learners now have everything they need to learn the material and ensure they are prepared for the exam and their career.

*Whether you are just starting to prepare and need comprehensive training with CertMaster Learn, need a final review with CertMaster Practice, or need to renew your certification upon expiration with CertMaster CE, CertMaster's online training tools have you covered.*

## ✱ 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 International Trends in Cybersecurity – CompTIA, April 2016  
2 <https://www.globalknowledge.com/us-en/content/salary-report/it-skills-and-salary-report/>