

CompTIA Security+ (SY0-501)

CompTIA Security+ Intro

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.

Key Differentiators:

- 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 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.

Resources:

- Average Salary:
 - U.S. Security Administrator: Glassdoor.com (<https://bit.ly/2NXjo0u>)
 - UK Security Administrator: ITJobsWatch.co.uk (<https://bit.ly/35nZP7Z>)
- Security+ Additional Information: [CompTIA.org/certifications/security](https://www.comptia.org/certifications/security)
- Recommended Pathways: [CompTIA.org/certifications/which-certification](https://www.comptia.org/certifications/which-certification)
- Posts: <https://bit.ly/33YY5kB>

VALUE Prop 1 (Career Changer/Student)

Security+ establishes core knowledge and incorporates best practices in hands-on trouble-shooting and problem-solving. IT professionals with Security+ know how to address security incidents – not just identify them.

VALUE Prop 2 (Employer)

CompTIA Security+ validates core knowledge required of any cybersecurity role, and emphasizes hands-on practical skills required by organizations. It better prepares staff to not only identify security risks but address them as well.

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

Skills and Competencies Acquired:

- Understand network security
- Identify and mitigate security threats
- Understand application, data and host security issues
- Implement access control and identity management

Job Roles:

- Systems Administrator
- Security Specialist
- Security Administrator
- Security Engineer

Competitors

Talking Points / Security+ Advantages

CISCO (CCNA Security)	<ul style="list-style-type: none"> • CCNA Security and Security+ are both certifications that are ideal for IT pros who are in entry-level security roles; however, Security+ is vendor neutral and covers a broader security focus. • Security+ has 38% more job ads than CCNA.
EC-Council Certified Ethical Hacker (CEH)	<ul style="list-style-type: none"> • CEH focuses only on penetration testing, the questions are multiple choice with no performance requirement, and it costs nearly 3x more. • Security+ includes performance-based questions to focus on threats, attacks and vulnerabilities, risk management, cloud security and penetration testing basics. • Security+ has 11x more job ads than CEH.
GIAC Security Essentials (GSEC)	<ul style="list-style-type: none"> • CompTIA Security+ and GSEC are both foundational-level, vendor-neutral certifications, but only Security+ includes performance-based questions to test hands-on skills. • Security+ is listed in 12% of all U.S. cybersecurity job ads, while GSEC is listed in fewer than 3%, according to Burning Glass. • GSEC costs nearly 5x more.

Companies that Endorse Security+:

- Northrop Grumman
- Brotherhood Mutual
- The Joint Commission
- Nationwide
- Agile Defense
- Modern Technology Solutions, Inc.

By the Numbers:

- Over **500,000** Security+ certified professionals.
- **62%** of IT professionals who hold at least one CompTIA certification are Security+ certified, according to Global Knowledge.

CompTIA Security+ (SY0-501)

How does CompTIA Compare?



Certification	Security+	CCNA Security	EC-Council Certified Ethical Hacker (CEH)	GIAC Security Essentials (GSEC)
Performance-based Questions	Yes	No	No 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	Entry	Intermediate	Entry
Prerequisites	CompTIA A+ and Network+ recommended	CCENT, CCNA Routing and Switching, OR CCIE certification	CEH Training, 2 years information security experience, Endorsement	None