CompTIA

Security+ For Government Agencies and Contractors

Protect Your Agency with the Leading Cybersecurity Cert

Staffing Security+ certified IT workers safeguards your network against cybersecurity threats

WHAT IS SECURITY+?

CompTIA Security+ is a vendor-neutral IT certification that validates successful candidates have knowledge and skills of network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management and cryptography.

WHY CHOOSE SECURITY+?

Nearly 600,000 have earned the Security+ credential, far and away making it the most sought after cybersecurity certification. Many pursue Security+ as their first cybersecurity certification and as a steppingstone to additional cyber certifications.

CompTIA continually updates Security+ to reflect how cybersecurity job roles are becoming more specialized. As new skills (like security analytics) grow in importance, the skills covered in Security+ have become a baseline for all cybersecurity jobs. The importance of and demand for Security+ has increased in recent years for a broader variety of job roles.

DoD DIRECTIVE 8140/8570

For Information Assurance Technician (IAT) Level II and for Information Assurance Manager (IAM) Level I, the U.S. Department of Defense recognizes Security+ certification validates the knowledge and skills of IT workers under DoD Directive 8140/8570. More choose Security+ for DoD 8140/8570 compliance than any other IT certification.

REDUCED VULNERABILITY

Cybersecurity breaches can wreak havoc with an agency's reputation. Security+ certified staff increase the odds that your organization will be able to defend against cybersecurity threats.

RETURN ON INVESTMENT

Compromised data can do serious financial damage to an agency. U.S. organizations have the highest average total cybersecurity costs at $21 million annually*. Agencies that invest in CompTIA Security+ certified staff efficiently limit their risks and keep their systems protected.

Security+ 501, released in October 2017, places a greater emphasis on the practical and hands-on ability to both identify and address security threats, attacks and vulnerabilities.

WHO IS SECURITY+ FOR?

A very wide variety of people pursue the Security+ certification. Some job titles of candidates include:

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

> "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

DoD Approved IA 8140/8570 Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
A+ Network+ SSCP	**Security+** CySA+ GSEC SSCP	CASP CISA CISSP (or Associate) GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
Security+ CAP GSLC	CASP CAP GSLC CISM CISSP (or Associate)	GSLC CISM CISSP (or Associate)
IASAE Level I	**IASAE Level II**	**IASAE Level III**
CASP CISSP (or Associate)	CASP CISSP (or Associate)	CISSP - ISSEP CISSP - ISSAP

CompTIA Security+® Certification for Government Agencies

Additional Benefits of a Security+ Certified Staff

- Demonstrates compliance with government regulations under the Federal Information Security Management Act (FISMA)
- Comprehends security risks within virtualization, cloud computing and wireless platforms
- Creates uniform cybersecurity processes

Verified Cybersecurity Skills

The CompTIA Security+ certification exam includes both multiple choice and hands on performance-based questions that require each individual to perform in a simulated environment. Successful candidates will demonstrate the following skills:

Threats, Attacks and Vulnerabilities
Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts.

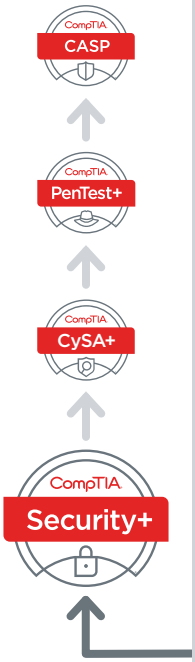
Technologies and Tools
Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security.

Architecture and Design
Implement secure network architecture concepts and systems design.

Identity and Access Management
Install and configure identity and access services, as well as management controls.

Risk Management
Implement and summarize risk management best practices and their business impact.

Cryptography and PKI
Install and configure wireless security settings and implement public key infrastructure.



"Compliance is very important to Avaya. CompTIA Security+ ensures that our security technicians have an understanding of the best way to implement a secure network."

- **ARMANDO RODRIGUEZ**, REGIONAL SOLUTIONS ENGINEER, AVAYA

CompTIA Security+ Exam Prerequisites: *It is recommended that CompTIA Security+ candidates have CompTIA Network+ certification and at least two years of technical networking experience, with an emphasis on security.*

HOW TO GET YOUR EMPLOYEES Security+ CERTIFIED

1. Choose a training option
- CompTIA CertMaster
- Instructor-Led
- Self-Study
- Visit **Certification.CompTIA.org/training**

2. Get familiar with the exam
- Download the exam objectives
- Review sample questions from the exam
- Visit **Certification.CompTIA.org/certifications/security**

3. Test
- Locate a Pearson VUE testing center near you and take the Security+ exam
- Visit **Certification.CompTIA.org/testing**

Learn more: **Certification.CompTIA.org/securityplus**

CompTIA is the world's largest provider of vendor-neutral certifications. CompTIA certifications are developed with the support of leading technology companies and organizations, and validated by industry experts around the world.

* Ponemon Institute, Cost of Cyber Crime, 2017