CompTIA Security+ 701

How the world's most popular cert is changing in 2024 (and how it affects you)

INFOSEC™

What is the CompTIA Security+?

More than 700,000 cybersecurity professionals have earned CompTIA's Security+, making it the most popular cybersecurity certification in the world. It's designed to validate knowledge across a wide range of entry-level cybersecurity roles, so it provides a clear path for individuals to build the baseline skills required to transition into security. It's also why so many organizations either require or recommend a Security+ in their job openings.

Employers want Security+ holders

Simply saying you have skills and expertise in cybersecurity will not earn you a job. Employers want your skills validated, and the easiest way for them to do that is to rely on certifications.

"Employers are listing Security+ in about 13% of all the job ads," said Patrick Lane, Director of Product Management at CompTIA, in our Security+ webcast. "The reason is that Security+ provides those baseline skills needed to get into a cybersecurity career."

The Security+ certification has simply become a requirement for many hiring managers as they attempt to bring in entry-level candidates and close their organization's cybersecurity skills gap.

Benefits of earning your Security+:

- Globally recognized certification
- Created by a vendor-neutral, non-profit certification body
- Regularly updated to align with the latest trends and techniques
- Validates a baseline of industry-recommended cybersecurity skills
- Proven way to help break into a junior cybersecurity role

32% growth

Expected increase in roles like information security analyst from 2022-2032

700,000+ certified

Number of Security+ certification holders

$95,472

Average Security+ holder salary in the U.S.

Learn More About Security+

Security+: 5 in-demand cybersecurity skills

In November 2023, CompTIA updated the Security+ exam (from SY0-601 to SY0-701), to align with the most in-demand entry-level cybersecurity skills and trends heading into 2024. The updated exam evaluates the skills required to:

- **Assess the security posture** of an enterprise environment and recommend and implement appropriate security solutions
- **Monitor and secure hybrid environments,** including cloud, mobile, Internet of Things (IoT) and operational technology (OT)
- **Operate with an awareness of applicable regulations and policies,** including principles of governance, risk and compliance
- **Identify, analyze and respond** to security events and incidents

This is done by testing against five core sets of cybersecurity skills that employers are looking for:

1. General security concepts

Includes key cybersecurity terminology and concepts to provide a foundation for security controls discussed throughout the exam.

2. Threats, vulnerabilities and mitigations

Focuses on responding to common threats, cyberattacks, vulnerabilities and security incidents and appropriate mitigation techniques to monitor and secure hybrid environments.

3. Security architecture

Includes security implications of different architecture models, principles of securing enterprise infrastructure and strategies to protect data.

4. Security operations

Includes applying and enhancing security and vulnerability management techniques, as well as security implications of proper hardware, software and data management.

5. Security program management and oversite

Updated to better reflect the reporting and communication skills required for Security+ job roles relating to governance, risk management, compliance, assessment and security awareness.

Security+ 701 vs. 601: What changed?

“The cybersecurity industry is becoming more refined and more focused,” said Lane in our Security+ webcast. “Now we know better than ever the job roles and the skills that we need to focus on — and what we don’t need to focus on.”

As a result, the new Security+ exam has seven fewer exam objectives. The 25 objectives in the SY0-701 exam align with the knowledge and skills employers expect from those in a security administrator-type role.

Security+ 701		Security+ 601 equivalent	
1. General security concepts	12%	---	---
2. Threats, vulnerabilities and mitigations	22%	1. Attacks, threats and vulnerabilities	24%
3. Security architecture	18%	2. Architecture and design	21%
---	---	3. Implementation	25%
4. Security operations	28%	4. Operations and incident response	16%
5. Security program management and oversight	20%	5. Governance, risk and compliance	14%

5 changes to the new exam

1. Fewer exam objectives (28 vs. 35) due to more focused job roles in a maturing industry
2. Security administrator skills are identified more accurately, and NICE work roles have increased
3. Exam domains and objectives were re-ordered and re-named to address instructional design improvements
4. More focus on the application of skills and slightly less focus on the analysis
5. GRC tasks focused on reporting and communication versus minutia of regulatory standards and processes

Security+ related job roles

The primary job roles for Security+ holders remain security administrator and systems administrator. However, one big change is the mapping to NICE Work Roles, said Lane. The new Security+ maps to 80% of the core objectives for 18 NICE Work Roles. This is helpful for companies using the Workforce Framework for Cybersecurity (NICE Framework).

Nearly one in four (24%) employed U.S. cybersecurity professionals are Security+ certified, mostly in the following roles:

New Security+ 701 job roles	Old Security+ 601 job roles
Primary job roles:	**Primary job roles:**
» Security administrator	» Security administrator
» Systems administrator	» Systems administrator
Secondary job roles:	**Secondary job roles:**
» Help desk analyst	» Help desk manager / analyst
» Security engineer	» Security engineer / analyst
» Security analyst	» Network / Cloud engineer
» NICE Work Roles (18)	» DevOps / Software developer
	» IT auditors
	» IT project manager

Security+ NICE Work Roles

Security+ 701 maps to 80%+ of the core objectives for the following NICE Work Roles:

- Technical support specialist
- Database administrator
- Knowledge manager
- Network operations specialist
- System administrator
- System requirements planner
- System testing and evaluation specialist
- Cyber defense analyst
- Cyber defense infrastructure support specialist
- Cyber defense incident responder
- Vulnerability assessment analyst
- Security control assessor
- Secure software assessor
- Information systems security manager
- Cyber policy and strategy planner
- IT project manager
- IT program auditor
- Systems security analyst

Security+ exam details

The updated version (SY0-701) of the Security+ exam was released in November 2023. The previous version (SY0-601) remains available through July 2024, so those taking the exam prior to then can choose either version. Both versions follow the same format and will earn your CompTIA Security+ certification, so you should take the version you studied for.

After July 31, 2024, SY0-701 will be the only version available until the next update, expected in Fall 2027.

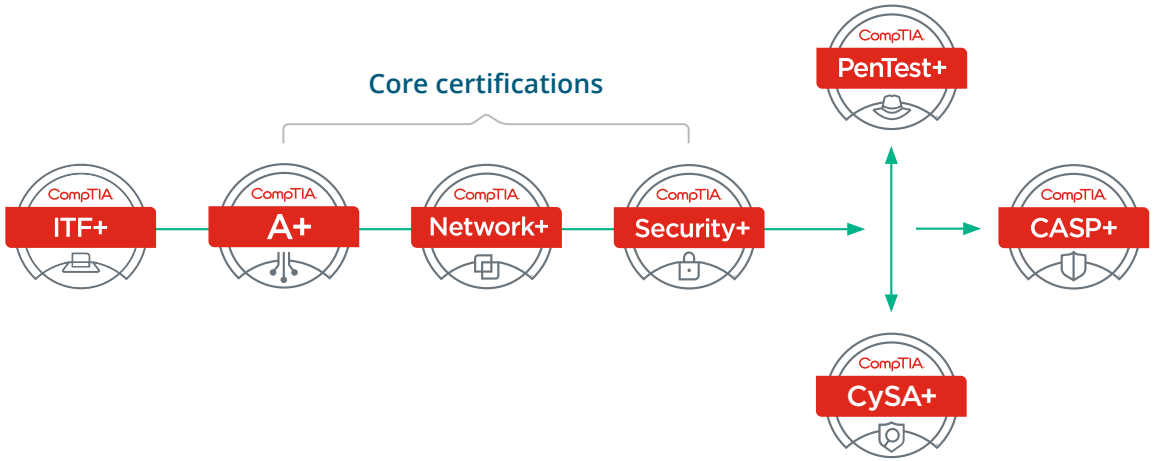
Exam code	SY0-701
Launch date	November 7, 2023
Availability	Worldwide
Testing provider	Pearson VUE testing centers
Format	Online or onsite at Pearson VUE
Total questions	Maximum of 90 questions
Length of test	90 minutes
Question types	Performance-based and multiple-choice
Passing score	750 (on a scale of 100-900)
Languages	English, with Japanese, Portuguese and Spanish to follow
Recommended experience	CompTIA Network+ and two years of experience working in a security/systems administrator job role
Exam retirement of SY0-601	July 31, 2024

Security+ and the CompTIA career path

Although there's no standard way to break into cybersecurity, CompTIA's core three certifications of A+, Network+ and Security+ are likely the most established and repeatable path.

- **CompTIA A+:** Build a foundation of knowledge and skills related to entry-level technical support roles
- **CompTIA Network+:** Expand your skills by learning how to configure, troubleshoot and oversee networks
- **CompTIA Security+:** Establish a baseline of security concepts and practical skills that will aid you throughout your career

Once you build that baseline of cybersecurity skills, you can pursue the PenTest+ to learn more about offensive red team security, or you can pursue the Cybersecurity Analyst (CySA+) to learn more about defensive blue team concepts. The CompTIA Advanced Security Practitioner (CASP+) certification is targeted towards cybersecurity veterans who wish to remain practitioners rather than moving into management.



The big three: A proven path to success

In 2019, we partnered with VetsInTech to help train veterans for cybersecurity roles. CompTIA's core certifications of A+, Network+ and Security+ were the foundation of the program, which included three weeks of intense training focused on building the skills outlined by each certification.

Many who attended began with little or no IT experience; nevertheless, the program has seen a 100% pass rate and 95% employment rate. It's provided a model for individuals looking to jumpstart their cybersecurity careers — and a path forward for individuals and organizations looking to upskill and fill entry-level cybersecurity roles.

VETSINTECH

Security+ training options

There is no right or wrong way to train for your Security+. It depends on your learning style, professional background and schedule. Three popular training methods to consider are:

- Live training with an expert instructor (either in-person or live online)
- Self-paced Security+ training courses
- Self study from books and other resources

Approved CompTIA training partners are recommended, as they will have the latest training materials and follow established best practices. Checking third-party review sites like G2 is also a great way to get an unbiased perspective on different training providers.

Earn your Security+ with Infosec

Infosec is CompTIA's top authorized training partner, and has won numerous awards, including the CompTIA outstanding partner award. You can train for your Security+ with Infosec two ways:

1. Enroll in a Security+ 5-Day Boot Camp
2. Sign up for an Infosec Skills subscription, which includes popular Security+ training from Mike Meyers

Why train with Infosec

- Immediate access to Infosec Skills — including a bonus boot camp prep course — from the minute you enroll to 90 days after your boot camp
- Five days of expert, live Security+ training
- 90-day extended access to all boot camp video replays and materials
- Unlimited Security+ practice exam attempts
- Security+ exam voucher
- Learn by doing with hundreds of additional hands-on courses and labs
- 100% Satisfaction Guarantee
- Exam Pass Guarantee

Learn More About Security+ Training

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. More than 70% of the Fortune 500 have relied on Infosec Skills to develop their security talent, and more than 5 million learners worldwide are more cyber-resilient from Infosec IQ's security awareness training.

Learn more at infosecinstitute.com.

Additional resources

- Security Boot Camp
- Security+ Self-paced Learning Path
- Security+ certification hub
- CompTIA Security+: Everything you need to know about the SY0-701 update (Webcast)
- Security+ exam objectives (PDF)