CompTIA Security+ 601

How the world's most popular cert is changing in 2021

(and how it affects you)

INFOSEC™

What is the CompTIA Security+?

More than half a million 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.

"Security+ appears in nearly 10% of all job ads in the United States," says Patrick Lane, director of product management at CompTIA. "And right now 16% of the entire workforce has Security+."

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

31% growth

Expected increase in cybersecurity jobs from 2019-2029

500,000+ certified

Number of Security+ certification holders

16% of workforce

Cybersecurity professionals with a Security+

Security+: 5 in-demand cybersecurity skills

In November 2020, CompTIA updated the Security+ exam (from SY0-501 to SY0-601), to align with the most in-demand entry-level cybersecurity skills and trends heading into 2021. 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 and IoT
- **Operate with an awareness of applicable laws 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. Attacks, threats & vulnerabilities

Includes the latest trends, such as IoT device weaknesses, newer DDoS attacks and social engineering techniques based on current events.

2. Architecture & design

Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.

3. Implementation

Has been expanded to focus on administering identity, access management, public key infrastructure (PKI), basic cryptography, wireless and end-to-end security.

4. Operations & incident response

Includes organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls and basic digital forensics.

5. Governance, risk & compliance

Has been expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST and CCPA.

Security+ 601 vs. 501: What changed?

"The new Security+ has newer skills, more threats, more entry-level incident response and more governance, risk and compliance (GRC)," says Lane. "But it actually has fewer domains than the previous version, because we're becoming more defined as an industry."

Technologies and tools are still part of the new exam, but those specific objectives are now broken up and placed within the domains where each tool is applied for better instructional design.

Old Security+ 501 domains

1. Threats, attacks and vulnerabilities (21%)
2. Technologies and tools (22%)
3. Architecture and design (15%)
4. Identification and access management (16%)
5. Risk management (14%)
6. Cryptography and PKI (12%)

New Security+ 601 domains

1. Attacks, threats and vulnerabilities (24%)
2. Architecture and design (21%)
3. Implementation (25%)
4. Operations and incident response (16%)
5. Governance, risk and compliance (14%)

6 changes to the new exam

1. More threats, cloud environments, entry-level incident response and GRC
2. Fewer exam domains: reduced from six to five
3. Fewer exam objectives: reduced from 37 to 35
4. More context: 25% more examples under each objective
5. Several exam domains and exam objectives were renamed and re-ordered
6. More emphasis on the application of skills

Security+ related job roles

The primary job roles for Security+ holders are security administrator and systems administrator, which account for approximately 40% of exam takers. However, the number or job roles that are pursuing Security+ is becoming more broad every year.

“It tells an amazing story,” says Lane. “These skills have become more applicable to more and more job roles across the world. It sets IT pros up for success in intermediate and advanced cybersecurity jobs. It really is a springboard into many advanced-level roles.”

Old Security+ 501 job roles

Primary job roles

- Security administrator
- Systems administrator

Related job roles

- Network administrator
- Security specialist
- Security consultant
- Security engineer

New Security+ 601 job roles

Primary job roles

- Security administrator
- Systems administrator

Related job roles

- Helpdesk managers and analysts
- Network and cloud engineers
- IT auditors
- Security officer
- Security manager
- IT project manager
- DevOps team
- Software developer

Springboard for your career

Security+ focuses on the third level of the popular educational model known as Bloom’s Taxonomy: applying knowledge. “It is about hands-on skills,” says Lane. “Security+ gets you employees who get the job done. And employers really, really like that.”

But it also provides a springboard into more advanced analytical roles.

“The analysis level, which is typically at the three- to four-year level of someone’s career, covers more advanced jobs such as security analyst, penetration tester, security engineer, forensics analyst and security architect. Once you have the core baseline cybersecurity skills found in Security+, you can just keep going up and getting higher and higher paying jobs as your cognitive abilities are utilized more.”

Security+ exam details

The updated version (SY0-601) of the Security+ exam was released in November 2020. The previous version (SY0-501) remains available through July 31, 2021, 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 it's recommended you take the version you studied for.

After July 31, 2021, SY0-601 will be the only version available until the next update, which is expected in 2024.

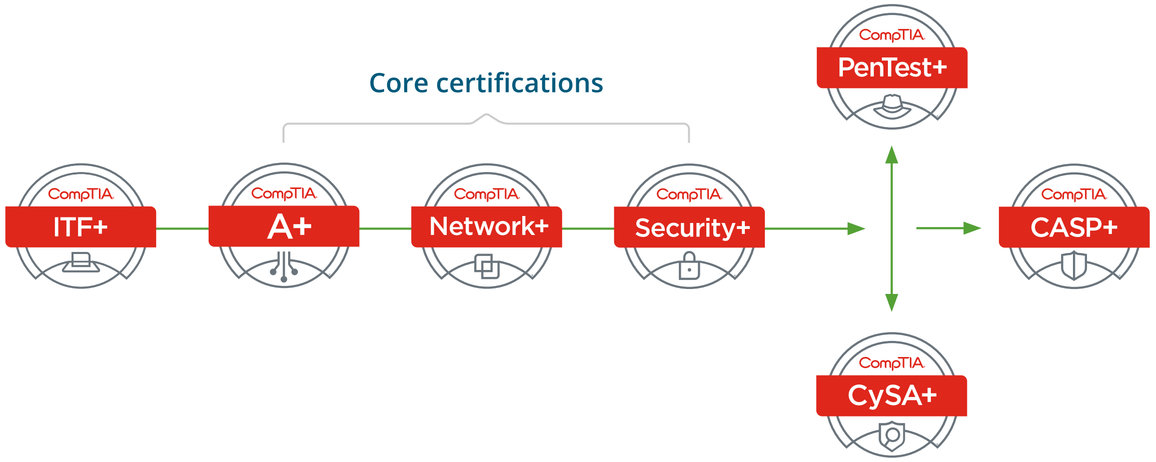
Exam code	SY0-601
Launch date	Mid-November 2020
Availability	Worldwide
Testing provider	Pearson VUE testing centers
Format	Online or onsite at Pearson VUE
Total questions	Maximum of 90 questions
Length of test	90 minutes
Question types	Performance-based and multiple-choice
Passing score	750 (on a scale of 100-900)
Languages	English
Recommended experience	CompTIA Network+ certification and two years of experience in the IT field with a security focus
Exam retirement of SY0-501	July 31, 2021

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.

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)
- On-demand 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 an authorized training partner of CompTIA 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 (online students)

Learn More About Security+ Training

About Infosec

At Infosec, we believe knowledge is power when fighting cybercrime. We help IT and security professionals advance their careers with certifications and skills training. We also empower all employees with security awareness training to stay cybersafe at work and home. Driven by smart people wanting to do good, Infosec educates entire organizations to defend themselves from cybercrime. It's what we do every day — equipping everyone with the latest security skills and confidence to be safe online.

Learn more at infosecinstitute.com.

Additional resources

- Security+ certification training and boot camp
- Infosec Skills Security+ training with Mike Meyers
- Infosec Resources Security+ hub
- CompTIA Security+ certification exam objectives (PDF)