Independent Tests of
Anti-Virus Software

VPN Certification Test Report
Kaspersky VPN Secure Connection

PLATFORM: WINDOWS

TEST PERIOD: NOVEMBER 2024

LAST REVISION: 12TH DECEMBER 2024

WWW.AV-COMPARATIVES.ORG

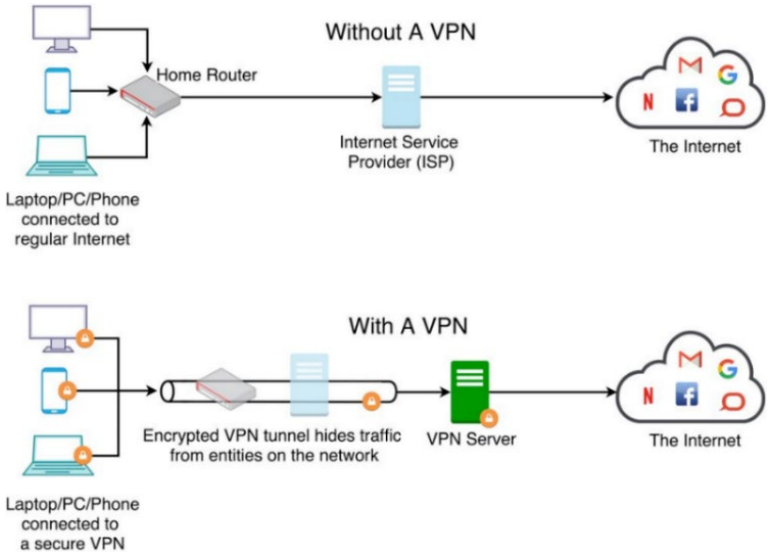
Introduction

AV-Comparatives conducts a certification test for VPN products, subjecting them to rigorous evaluation to assess their performance in key areas such as security, privacy, download speed, upload speed, and latency. Certification is granted only to products that undergo the testing process and meet the required standards.

What is a VPN?

A Virtual Private Network (VPN) is a technology originally designed to allow remote workers secure access to their company's local networks. Today, VPNs are widely used to enhance online privacy and security.

A VPN provides the following two benefits. First, while a user's Internet traffic still passes through their Internet Service Provider (ISP), the VPN encrypts the data, hiding the content of the communication. Second, it replaces the user's public IP address with one from the VPN server, masking their true geographic location and providing greater privacy.



Why use a VPN?

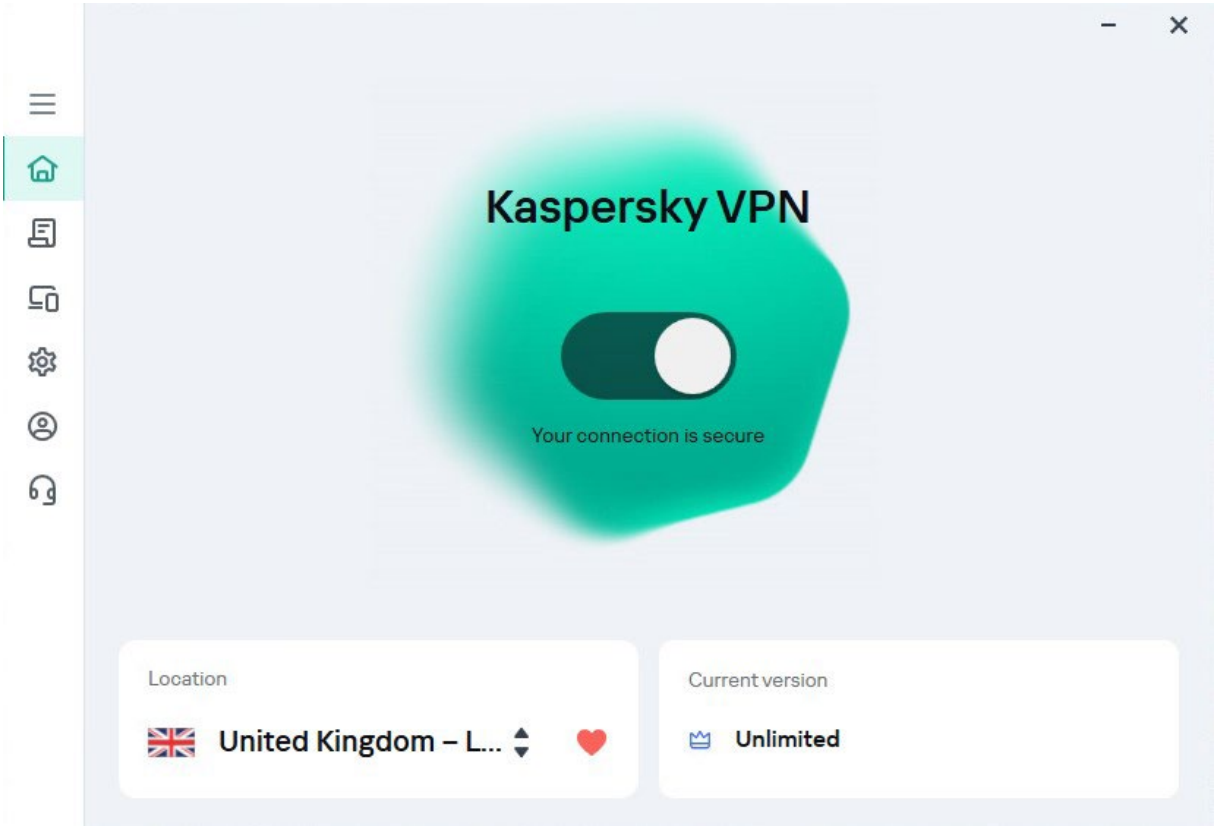
VPNs offer numerous benefits, making them essential tools for many users. Common use cases include enhanced security, access to geo-restricted content, and improved privacy.

By encrypting Internet traffic, VPNs provide a significant security advantage, particularly when using public Wi-Fi networks in places such as cafés, hotels, or airports. These networks are often targeted by cybercriminals who can intercept unprotected data. A VPN protects sensitive information, making it much harder for hackers to access your online activities.

Another major reason for the growing popularity of VPNs is their ability to spoof the user's geographic location. This feature allows access to content that may be restricted in certain regions, such as streaming services, websites, or social media platforms. Additionally, VPNs are invaluable for individuals in countries with strict government censorship, helping them bypass restrictions and safeguard their online activities from surveillance.

Tested Product

The most recent, paid-for version of **Kaspersky VPN Secure Connection** for Windows (21.19), available at the time of testing (November 2024), was used in this test.



AV-Comparatives' Approved VPN Product Award

To be certified and receive AV-Comparatives' **Approved VPN Product Award**, VPN solutions must undergo rigorous evaluation and meet the certification criteria regarding privacy and performance as outlined in this report (see Appendix).

Only products that passed the 2024 VPN Certification Test have their reports published. Kaspersky submitted Kaspersky VPN Secure Connection for evaluation in 2024. **Kaspersky VPN Secure Connection for Windows** met all the requirements and was awarded the certification.

Test Procedure

In this test, the primary objective was to assess both the privacy features and performance of the tested product. The test was divided into three parts:

- The *Leak Test*, where we evaluated the degree of privacy the VPN provides by performing IP leak tests.
- The *Kill-Switch Test*, where we checked the VPN's ability to protect the genuine public IP address from being leaked in the event of an unexpected connection drop.
- The *Performance Test*, where we measured the VPN's download and upload speeds, as well as its latency (response time).

Lab Setup

We conducted the test using Microsoft's Azure cloud infrastructure. All tests were performed on a fully patched 64-bit Microsoft Windows 10 system. To simulate a real-world scenario, we limited the available bandwidth to 250/250 Mbps (download/upload speeds), a realistic value for Internet connections in (sub-)urban areas. Additionally, the enormous bandwidth of the cloud infrastructure ensured that the 250/250 Mbps limit was consistently available, meaning the Internet connection itself was never the limiting factor in our tests.

The latest version of the VPN product available at the time of testing (November 2024) was downloaded from the vendor's website and installed on the test system following the provided instructions. The product was tested using its default settings, including the default protocol or "Automatic" if that was the selected default option. If not, we used the VPN protocol listed first in the program, as outlined in the Certification Report. Where applicable, we configured the program to launch and connect automatically both on system start-up and after an unexpected connection drop.

Leak Test

We assessed the product's resilience against potential data and information leaks. The test was performed using various web testing methods, which allowed us to evaluate the product for leaks in several areas, including public IP address, DNS server, WebRTC local/public IP, and Torrent IP/DNS. The test was considered failed if an IP address belonging to the original network was detected while the VPN was active.

Kill-Switch Test

We evaluated the product's ability to protect the user's public IP address during an unexpected connection drop. The VPN should include a mechanism, a so-called *kill switch*, that prevents the genuine public IP address from being exposed while the VPN connection is lost and until it is re-established. Ideally, the VPN should completely disable or suspend the Internet connection until a secure connection is restored. We simulated a connection loss by deactivating and reactivating the Ethernet network adapter and recorded the system's public IP address before and after the event.

Performance Test

We evaluated the performance of the product based on two key aspects: the bandwidth or maximum data transfer rate in terms of the *download speed* and *upload speed*, and the delay of the network connection in terms of the *latency*.

For most users, download speed is the most critical factor, as it determines how quickly a browser or application can load web pages, files, video streams, or other online resources. Conversely, upload speed is crucial for activities such as uploading or streaming videos to platforms like YouTube or sharing files in a peer-to-peer (P2P) network. Latency, often referred to as "reaction time", measures the time it takes for a request to travel from the source to a destination and back. Low latency is particularly important for fast-paced online games, as it directly affects how quickly the game responds to user inputs.

To obtain accurate and reliable results, we employed multiple measurement methods. This approach not only increased the statistical significance of our results but also provided a more balanced evaluation. To account for potential bandwidth fluctuations, we conducted tests at different times each day over the course of one week.

We simulated a scenario in which a user in Germany downloads and uploads content from and to servers in different countries. To ensure comprehensive results, we tested VPN servers located in three countries: Germany, the United Kingdom, and the United States. We measured download and upload speeds, as well as latency, between the test system and three target servers. Two of these servers were in the destination country and geographically close to the VPN server's exit point. The third server was selected automatically based on its proximity to the VPN server, providing the fastest possible connection.

Kaspersky VPN Secure Connection Certification Report (November 2024)

Website: https://www.kaspersky.com/vpn-secure-connection

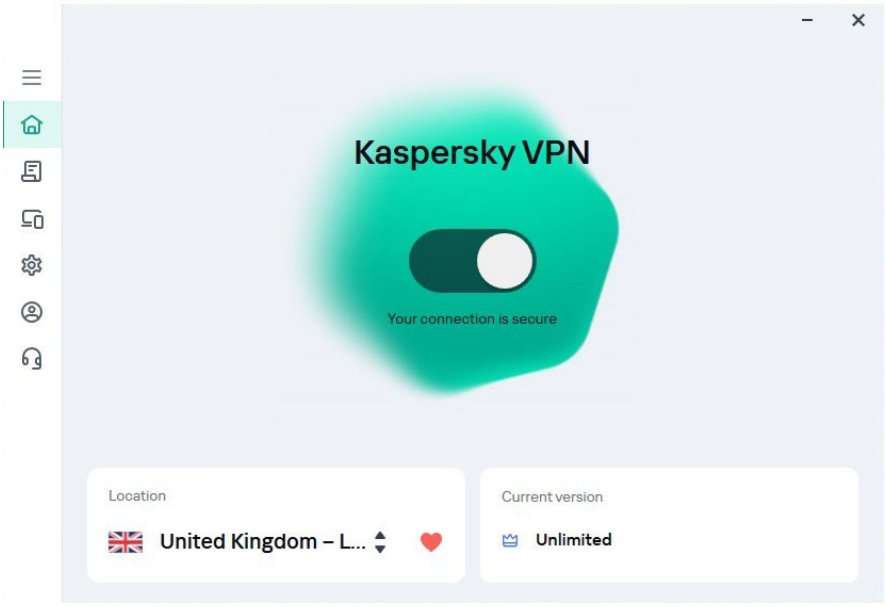
To be certified and receive AV-Comparatives' **Approved VPN Product Award**, VPN solutions must undergo rigorous evaluation and meet the certification criteria regarding privacy and performance as outlined in this report (see Appendix). **Kaspersky VPN Secure Connection** for Windows met all the requirements and was awarded the certification.

Certification areas	**Passed?**	**Notes**
All leak tests passed	YES	
Kill-switch test passed	YES	
Minimum download speed reached	YES	241 Mbps[1]
Minimum upload speed reached	YES	190 Mbps[1]
Latency below maximum limit	YES	
Refund period over 27 days	YES	30 days
Uses secure protocols	YES	Catapult Hydra, WireGuard, OpenVPN (only for manual configuration via config file)
Additional information	**Present?**	
Total number of servers exceeds 1,000	YES	2,007*
Servers in over 50 countries	YES	88 countries*
Servers on all continents (except Antarctica)	YES	
Free trial	YES	Free trial for 7 days
Simultaneous use on at least 5 devices	YES	
Split tunnelling	YES	
Transparency report (not older than 2 years)	YES	Link (last update: 2024) Link (last update: 2024)
Warrant canary (not older than 2 years)	YES	Link (last update: 2024)
Vendor claims to have a strict no-log policy	YES	Link
Are traffic logs and/or originating IP address logs collected?	NO	
Free of ads and upselling	NO	Upselling of own protection app within settings
Anonymous payment options	NO	
Are third-party VPN components used?	YES	Catapult Hydra library by Pango
Headquarters location / jurisdiction is known	YES	Switzerland, Russia
Auto-connect	YES	
Dedicated servers / protocol optimizations for streaming/gaming/P2P	YES	Streaming, P2P, Gaming
Trackers included	YES	Self-hosted tracking service
Are legacy protocols supported?	NO	
Different platforms supported	YES	Windows, macOS, Android, iOS
Extra features included	YES	Anti-tracker, Custom DNS, Double VPN/Multihop, 10Gbps servers

*) according to the vendor as of November 2024.

[1] On bandwidth 250 Mbps.

Kaspersky VPN Secure Connection is a reliable, user-friendly VPN service designed for users looking for robust security and privacy while browsing the Internet. It can be downloaded from the vendor's website and requires a My Kaspersky user account. A 7-day free trial with full product functionality and a 30-day refund policy give users ample time to assess the service. However, the lack of anonymous payment options, such as cryptocurrency, may discourage users seeking complete anonymity. The free version offers an automatically chosen server location and imposes a daily data limit.



Installation and Setup

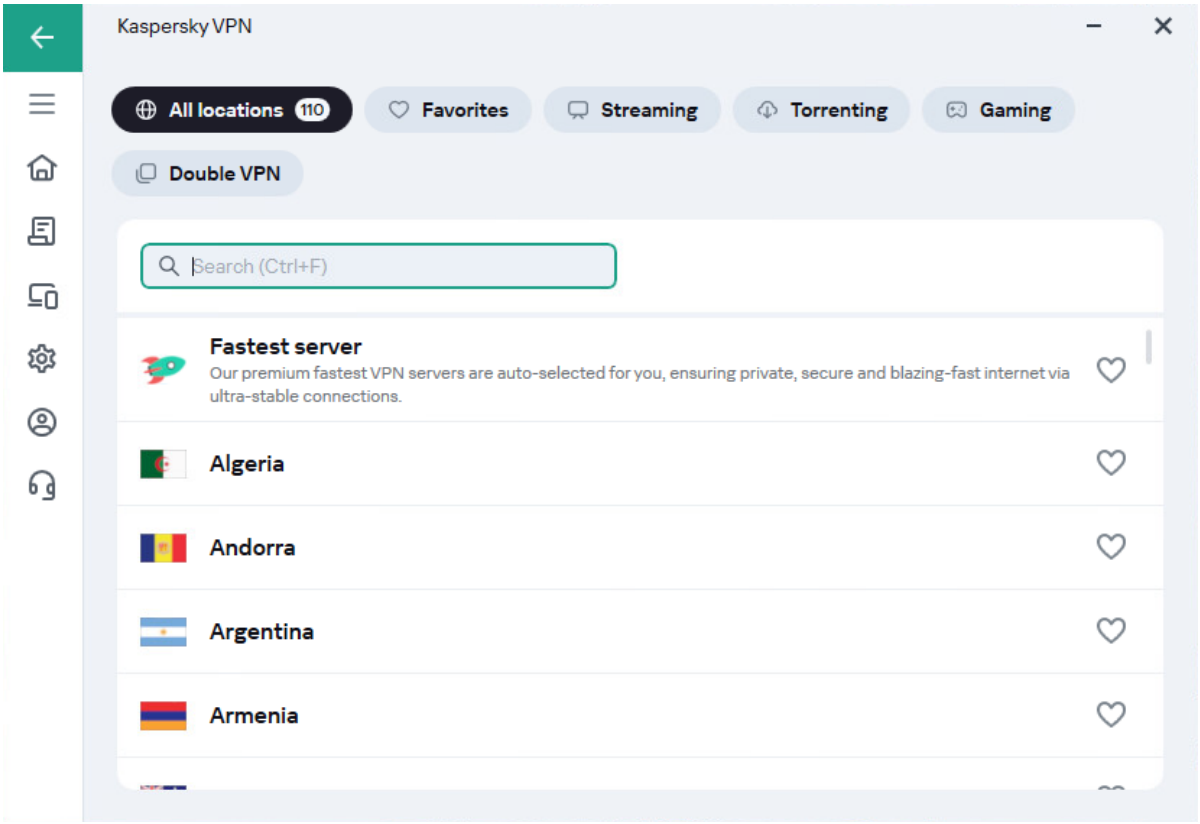
The installation and setup process is straightforward, with clear guidance provided throughout. The program interface is clean and intuitive, featuring a home page where users can select server locations, toggle the VPN on/off, and view the license status. Additional settings and options are neatly organised in a menu on the left side. While there is minor promotion of Kaspersky's protection app within the VPN settings, the service is otherwise free of ads and upselling.

Security and Privacy

Kaspersky VPN Secure Connection ensures strong security by utilising secure protocols, including Catapult Hydra (developed by Pango), WireGuard, and OpenVPN (available through manual configuration via a config file, not available in-app). The service's commitment to privacy is reflected in its strict no-log policy, thus not collecting any traffic logs or logs of originating IP addresses. Kaspersky also publishes regular transparency reports detailing how it handles data requests, including the total number of requests received from law enforcement, governments, and users worldwide. Those transparency reports apply to all Kaspersky products and not just the VPN product. The vendor also runs a bug bounty program to identify and fix unknown vulnerabilities.

An anti-tracking feature helps block trackers from collecting data about users' online activities. Users can also configure a custom DNS over HTTPS server as an alternative to the default DNS servers. For those seeking a VPN with integrated malware and phishing protection, upgrading to e.g., Kaspersky Plus or Premium could be an option. Kaspersky Plus and Premium combine Kaspersky VPN Secure Connection with advanced security features, providing good malware and phishing threat detection[2]. Kaspersky VPN Secure Connection passed all leak tests and the Kill-Switch Test.

[2] https://www.av-comparatives.org/vendors/kaspersky/



Performance and Usability

With over 2,000 servers spread across 88 countries worldwide, users have plenty of options when it comes to selecting a server location. Specialized servers are available for streaming, P2P, and gaming, ensuring optimal performance tailored to specific needs. Additionally, a special optimization in the Catapult Hydra protocol reduces latency. For those seeking heightened security, the service includes a "Double VPN/Multihop" feature, adding an extra layer of encryption to maximize privacy and anonymity. All servers are managed by the third-party VPN vendor Pango GmbH and its affiliates, located in Switzerland and the United States.

The VPN supports split tunnelling, allowing users to route specific app traffic through the VPN while leaving other apps unaffected. An auto-connect option activates the VPN automatically at startup and the "Smart Protection" feature prompts or automatically activates the VPN when connecting to insecure Wi-Fi networks, such as those in airports, cafés, hotels, or other public spaces. It is also possible to configure the VPN on routers and other devices using an OpenVPN or WireGuard client and the corresponding configuration files.

Kaspersky VPN Secure Connection easily reached the minimum download speed criteria (the solution demonstrated a median speed of 241 Mbps), minimum upload speed criteria (the solution demonstrated a median speed of 190 Mbps), and stayed below the maximum latency limit (<100 ms) in the Performance Test.

Appendix: Description of Certification Criteria and Additional Information

Compliance with the certification criteria below relates to the time of testing. As e.g. technical standards change as time goes on, we may deem it appropriate to change the certification criteria for future tests. Vendors can apply to have their VPN products certified once a year. Below we have listed Certification Areas, which are required if the product is to be certified. We have also shown additional information, which is not necessary for certification, but which many users will deem important. This relates to privacy aspects and additional features.

Many people use a VPN for reasons of privacy and will thus be concerned about the privacy and security practices of VPN vendors. In this report we have included information on those aspects of VPNs that we consider relevant, but of course there are other organisations[3] that promote good practices for VPN vendors, and these may have differing opinions on this subject.

Certification Areas

All leak tests passed: in order to be certified, a VPN product has to pass all leak tests. We run different leak tests such as public IP address, DNS server, WebRTC local/public IP, and Torrent IP/DNS. A product has failed a test if the IP address of the original network was leaked.

Kill-Switch test passed: in order to be certified, a VPN product must not leak the genuine public IP address during and after re-establishing a secure connection in the event of an unexpected connection drop.

Minimum download speed reached: in order to be certified, an Android VPN product must reach a median download speed of 10 Mbps. For a VPN product on Windows, a median download speed of 25 Mbps must be reached.

Minimum upload speed reached: in order to be certified, an Android VPN product must reach a median upload speed of 10 Mbps. For a VPN product on Windows, a median upload speed of 18 Mbps must be reached.

Latency below maximum limit: in order to be certified, a VPN product must have a median latency lower than 100 ms. This is the maximum acceptable latency for gaming on average where delays (or lags) are noticeable.[4] We only mention the latency figure if it is more than 100ms.

Refund period over 27 days: in order to be certified, a VPN product shall offer a refund period of at least 27 days (4 weeks) for 1-year-contracts.

Uses secure protocols: in order to be certified, a VPN product must implement and use secure protocols by default. We have shown which protocol is the default in all cases where this could be determined.

[3] For example, the VPN Trust Initiative (https://vpntrust.net).
[4] https://www.hp.com/us-en/shop/tech-takes/5-reasons-your-ping-is-so-high

Additional Information

Total number of servers exceeds 1,000: a VPN product should offer the widest possible choice of servers, which is ideal for load balancing and ensuring redundancy. However, having more servers does not automatically guarantee better service quality.

Servers in over 50 countries: the user should have a broad choice of country locations, to unlock as many geo-restricted services as possible. Servers in multiple countries can also be beneficial in terms of speed and latency.

Servers on all continents (except Antarctica): as with servers in different countries, servers on different continents can help with performance and access to geo-restricted services.

Free trial: a VPN product should offer a free testing period, or a free version of the product. We feel that users should be able to test a product before buying it.

Simultaneous use on at least 5 devices: a subscription plan for the VPN product should be available that allows it to be installed and used on at least 5 devices at a time. We recommend checking the number of simultaneous devices allowed when purchasing a VPN product.

Split tunnelling: a feature which lets the user decide which apps should or should not use the VPN, thus preventing unnecessary connection slowdowns.

Transparency report (not older than 2 years): although many VPN providers state that they do not keep any logs, there is no way for us to verify this. Publishing a transparency report and generally being open about how user data is dealt with are signs that a VPN provider values a user's privacy.

Warrant canary (not older than 2 years): in some cases, it might be illegal for VPN providers to report that they have had secret requests for user data from government or law-enforcement agencies. Therefore, some providers regularly publish a Warrant Canary stating that they have NOT had any such requests.

Vendor claims to have a strict no-log policy: the vendor states that they have a no-log policy. While this is good, there is no way for us to verify this. Therefore, we assigned this criterion to additional information instead of certification areas.

Are traffic logs and/or originating IP address logs collected: according to the privacy policy and/or analysed network traffic, records such as browsing activities (privacy implications) and/or the original IP address are transmitted.

Free of ads and upselling: we feel that a paid-for VPN product should not include any ads or upselling offers.

Anonymous payment options: providing anonymous payment options is good for buyers who want to stay under the radar even during the purchase. The information was taken from the vendor's German website.

Are third-party VPN components used: whether the VPN technology is developed in-house. If the component is licensed from a third-party, this will be noted here.

Headquarters location / jurisdiction is known: a known headquarters gives the potential buyer the possibility of reviewing the ownership and possible local laws applied to the business. When using a VPN, there are three important factors regarding the jurisdiction over the user's online activity: first, the online regulations of the country the user lives in; secondly, the country where the VPN vendor has registered its business; and thirdly, the country where the relevant, physical VPN server is located (regardless of the VPN provider's business location).

Auto-connect: a feature which lets the user automatically connect to the VPN on system startup, app launch or when connecting to an unsecure Wi-Fi.

Dedicated servers / protocol optimizations for streaming/gaming/P2P: the VPN vendor provides servers or VPN protocols specifically suited and optimized for streaming, gaming, or sharing files in a P2P network.

Trackers included: trackers can be useful for the VPN vendor to diagnose errors, performance issues, and to improve the application. While some trackers might be more privacy-friendly than others depending on the VPN-specific implementation, this is only given as information based on statements in the respective VPN privacy policy, and analysis of the product code and network traffic.

Are legacy protocols supported: although legacy protocols might pose a security risk because of a broken encryption or other vulnerabilities, some VPN products still support such protocols for compatibility reasons. Therefore, users have the choice to pick the protocol which works the best for a specific use case. For more details about the pros and cons of each protocol, please visit this website.

Different platforms supported: a VPN that supports multiple platforms ensures consistent security and flexibility across all devices, enhancing the user experience and providing robust protection regardless of the device or operating system in use. The VPN product is officially supported and can be installed on the listed platforms.

Extra features included: we list a few (up to five) selected features included in the VPN product.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(December 2024)