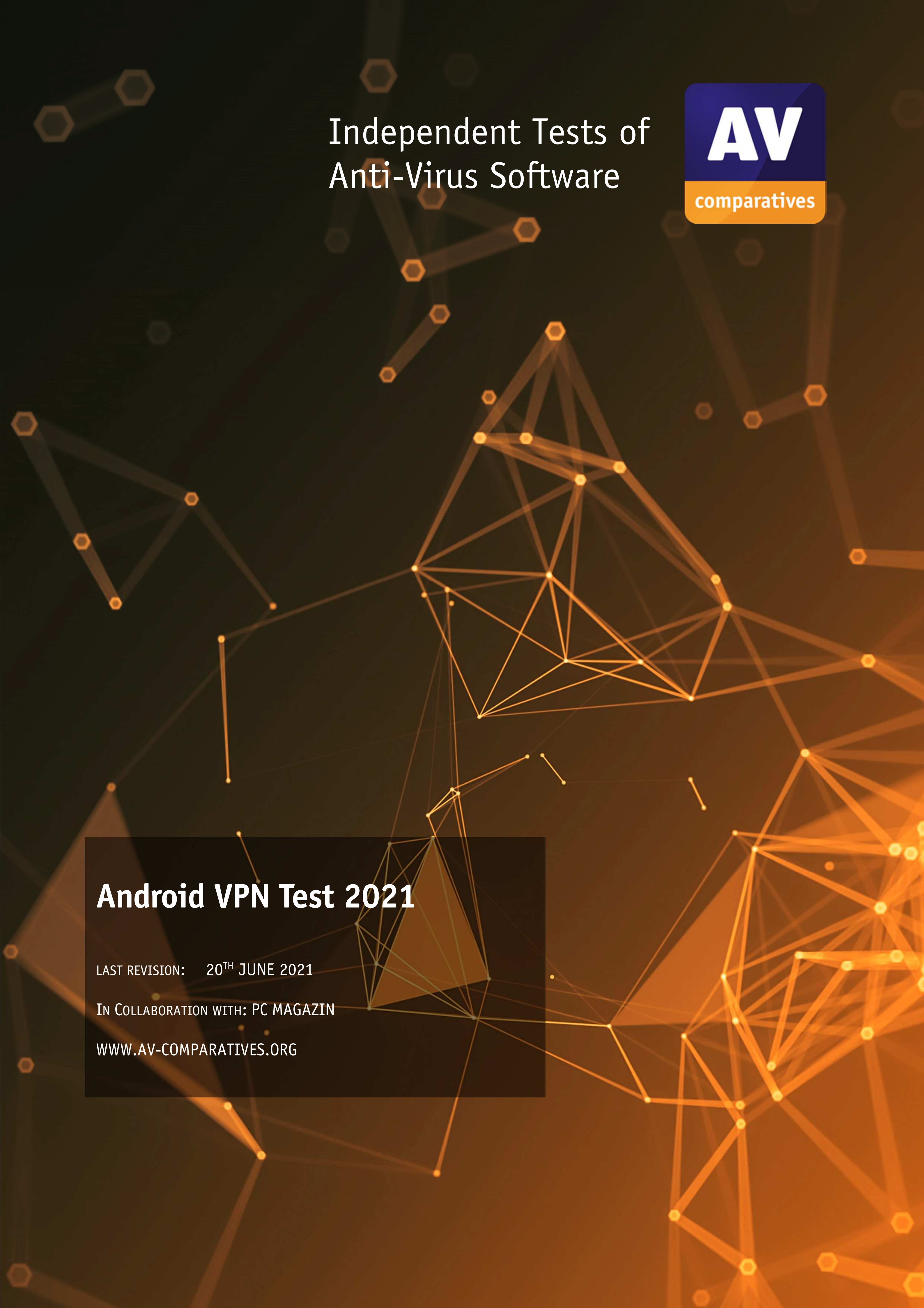


Independent Tests of
Anti-Virus Software

Android VPN Test 2021

LAST REVISION: 20TH JUNE 2021

IN COLLABORATION WITH: PC MAGAZIN

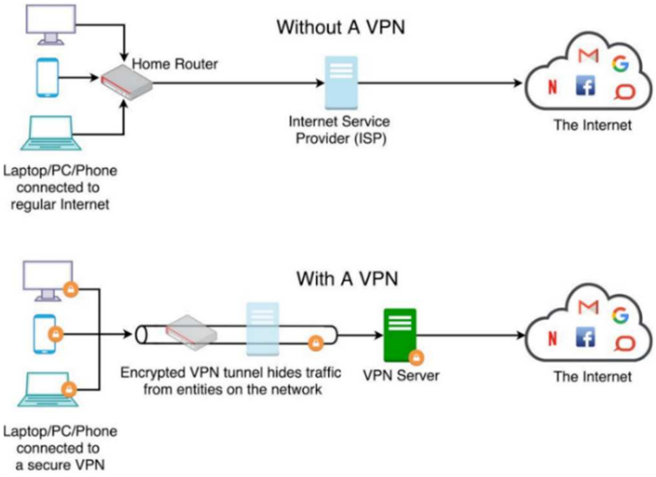
WWW.AV-COMPARATIVES.ORG

Introduction

The purpose of this test is to assess whether 6 popular VPN apps for Android perform appropriately in terms of security, privacy, download speed, upload speed, and latency. The test was performed in collaboration with PC Magazin. You can look forward to seeing more reports of this type. This project starts a new series of certification tests for a range of IT-security-related products like VPNs (for different platforms), and also security of IoT devices (such as routers and IP cameras). Vendors who would like to take part in these certification tests can contact us via the contact form at www.av-comparatives.org.

What is a VPN?

Virtual Private Networks (VPNs) were originally developed as a means of allowing remote workers to access resources on their company's local area networks in a secure manner. Nowadays they are also used globally to help anonymise a user's online experience. There are two important aspects here: firstly, although the traffic still goes through the user's Internet service provider (ISP), the VPN hides the content of the request by encrypting it; secondly, the public IP address is provided by the VPN server, thus ensuring the user's privacy, and allowing their real geographical location to be hidden.


Without A VPN
Home Router
Internet Service Provider (ISP)
The Internet
Laptop/PC/Phone connected to regular Internet
With A VPN
Encrypted VPN tunnel hides traffic from entities on the network
VPN Server
The Internet
Laptop/PC/Phone connected to a secure VPN

phys.org/news/2019-02-vpn.html,
Credit: Mohammad Taha Khan, CC BY-ND

Why use a VPN on Android?

The last decade has seen a tremendous and rapid improvement of mobile devices, both in terms of software and hardware. Nowadays, any user on Android is able to stream videos, do online banking, use torrent services and interact with many other applications, a fact which has motivated VPN vendors to support this platform. There might be various reasons for someone to use a VPN, among which are security, access to geo-restricted content, and privacy. VPNs encrypt the user's Internet traffic, which provides obvious security benefits. If you are using a public Wi-Fi network, such as the one provided by a café, hotel or airport, you are actually connected to the same network as anybody else using that Wi-Fi. It is relatively straightforward for a cybercriminal to intercept your Internet communications and gain access to your private data.

The rise in popularity of VPNs in recent years is partly because they can be used to spoof the user's geolocation, that is, make it appear that he/she is in a different country. The VPN is hence seen by many people as a way to hide their actions in countries where governments try to control the information its citizens have access to (e.g. websites, social media networks, news), as well as to monitor their citizens' online activities.

Tested Products

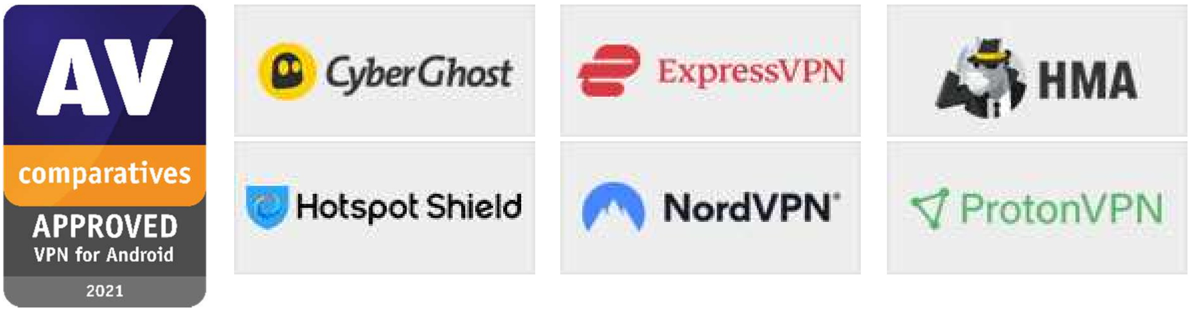
We evaluated 6 of the most popular VPN products for Android. For each product, the latest version available at the time of testing (April 2021) was used. For this report, we used the paid version of the products and their default protocol.

Product	Version	Vendor	Headquarters
CyberGhost VPN	8.3	CyberGhost S.A.	Romania
ExpressVPN	10.2	Express VPN International	British Virgin Islands
HMA	5.29	Privax Limited	UK
Hotspot Shield	8.4	Pango GmbH/Pango Inc.	Switzerland/USA
NordVPN	5.1	NordVPN	Panama
ProtonVPN	2.6	Proton Technologies AG	Switzerland

AV-Comparatives' Approved VPN for Android Award

We are giving our Approved VPN for Android Award to qualifying products. The certification criteria are described at the end of the report.

We congratulate the vendors shown below, whose products met the certification criteria, and are thus given the AV-Comparatives Approved VPN for Android Award[1]:



[1] Certificate usage is subject to a licensing agreement. Please contact us for details.

Test Procedure

In this test, we reviewed six popular VPN Apps for Android. Our main goal was to assess privacy features and performance of the tested products. Therefore, we divided the test 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 a network change (switching from a Wi-Fi to mobile data network, for instance).
- The *Performance Test*, where we measured the VPN's download and upload speeds and latency (response time).

Lab Setup

We performed all tests on Samsung Galaxy S9 devices, running Android 10. Using a Wi-Fi network, the devices were connected to a broadband Internet connection with a bandwidth of 200/50 Mbps (download/upload speeds respectively). We bought the latest version of each (paid) VPN product available at the time of testing and installed the respective apps on the test devices via the Google Play Store. Where product settings allowed it, we configured the program to launch and connect automatically, both on system start-up and after an unexpected connection drop-out. In order to provide a level playing field, we set the server location for all VPNs to Austria.

Test Methodology

Leak Test

We assessed the robustness of the product against possible data and information leaks. The test was performed using various web testing methods, which allowed us to evaluate each product for potential leaks in different instances such as public IP address, DNS server, WebRTC local/public IP, and Torrent IP/DNS. We consider the test as failed if an IP address belonging to the original network appeared during the test while the VPN was active.

Kill-Switch Test

We examined the protection capabilities of the VPN in the event of an unexpected connection drop-out. The VPN should provide a mechanism, a so-called *kill switch*, that prevents the genuine public IP address from being leaked to the Internet in the period between the VPN connection being dropped and it being re-established. Ideally, the Internet connection should be completely deactivated or suspended by the VPN until a secure connection is available again. We simulated a sudden connection loss by turning the Wi-Fi off and on again through the network settings and recording the system's public IP address during this. On Android, some VPNs make use of Android's built-in kill-switch functions, “Always-on VPN” and “Block connections without VPN”.

Performance Test

We focused on two different aspects to evaluate the performance of the connection provided by each VPN product: first, the bandwidth or maximum rate of data transfer in terms of the *download speed* and *upload speed*; second, the delay of the network connection in terms of the *latency*.

For many people, download speed will be the most important of the speed factors, as it is directly related to how fast a browser or any other program can load a web page, file, video stream, or other resources from another location on the Internet. The counterpart is the upload speed which comes into play when users upload videos to YouTube or share files in a P2P network. Latency measures the time it takes for a request to be sent from the originating host to a destination, and for it to be echoed back to the source. It could be described as "reaction time" and is crucial when playing fast-paced online games, as it determines how quickly the game reacts to user inputs.

To measure each of the values mentioned above, we used different measurement methods. This not only gave a greater number of measurements, and hence more statistical relevance, but also provided more balanced results. In order to capture potential variation in bandwidth, we repeated the tests at different times each day for one week. To allow each product to claim the entire bandwidth of our Internet connection, we only ran the speed test on one test device at a time. Furthermore, we disabled automatic updates on the test devices.

For our speed test, we used the scenario of a user in Austria uploading and downloading content to and from a server in Ireland. Download and upload speeds and latency were measured with a connection to the respective VPN service, and then with a direct connection not using a VPN.

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 additional features and privacy aspects.

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[2] 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-out.

Minimum download speed reached: in order to be certified, an Android VPN product must reach a median download speed of 10 Mbps. The minimum speed recommended by Netflix[3] to watch movies in HD is 5 Mbps. For a VPN product on Windows, a median download speed of 25 Mbps must be reached, which is the minimum speed recommended by Netflix to watch movies in 4K.

Minimum upload speed reached: in order to be certified, an Android VPN product must reach a median upload speed of 10 Mbps. The minimum speed recommended by YouTube[4] to stream videos with 1080p @60 fps is 9 Mbps. For a VPN product on Windows, a median upload speed of 18 Mbps must be reached, which is the minimum speed recommended by YouTube to stream videos with 1440p @60 fps.

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.[5] 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.

[2] For example, the VPN Trust Initiative (https://vpntrust.net).
[3] https://help.netflix.com/de/node/306
[4] https://support.google.com/youtube/answer/2853702
[5] 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, both for load balancing purposes, and to provide redundancy.

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 / Freemium: 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 streaming/P2P servers: the VPN vendor provides servers specifically suited and optimized for streaming as well as 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.

Extra features included: we list a few selected features included in the VPN product regarding security and privacy.

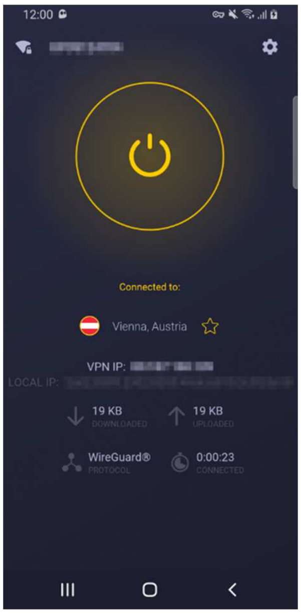
CyberGhost VPN Certification Report (April 2021)

Website: https://www.cyberghostvpn.com/

CyberGhost VPN for Android reached the minimum certification requirements for 2021, and so receives AV-Comparatives' Approved VPN Product Award.

CyberGhost is owned by Kape Technologies and was founded in Romania in 2011. It makes VPN products for Windows, macOS, Linux and iOS, in addition to Android. The vendor claims to have a no-log policy and provides a transparency report.

Anonymous payment is possible. The Android VPN includes additional features: tracking protection, a dedicated IP address, and blocks malicious-domain blocking.



Certification areas		**Notes**
All leak tests passed	YES	
Kill-Switch test passed	YES	Not visible, but built into app
Minimum download speed reached	YES	37 Mbps
Minimum upload speed reached	YES	26 Mbps
Latency below maximum limit	YES	
Refund period over 27 days	YES	45 days
Uses secure protocols	YES	WireGuard (default), OpenVPN
Additional information		
Total number of servers exceeds 1,000	YES	7,053*
Servers in over 50 countries	YES	91*
Servers on all continents (except Antarctica)	YES	
Free trial / Freemium	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: February 2021)
Warrant canary (not older than 2 years)	NO	
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	YES	
Anonymous payment options	YES	Cryptocurrency
Are third-party VPN components used?	NO	
Headquarters location / jurisdiction is known	YES	Romania
Auto-connect	NO	
Dedicated streaming/P2P servers	YES	Streaming
Trackers included	YES	3rd-party tracking service
Are legacy protocols supported?	YES	L2TP/IPSec
Extra features included	YES	Tracking protection, block malicious domains, dedicated IP

*) according to vendor's website, as of April 2021

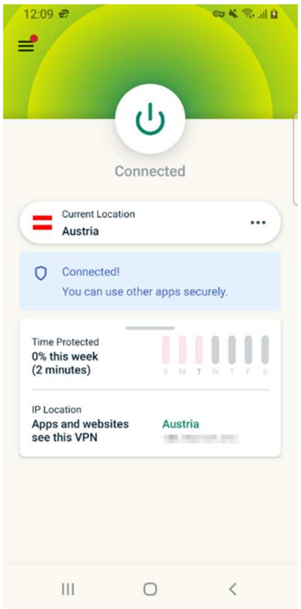
ExpressVPN Certification Report (April 2021)

Website: https://www.expressvpn.com/

ExpressVPN for Android reached the minimum certification requirements for 2021, and so receives AV-Comparatives' Approved VPN Product Award.

ExpressVPN is based in the British Virgin Islands and was founded in 2009. The company makes VPN products for Windows, macOS, Linux and iOS, in addition to Android. It also provides services for routers and other Internet-connected devices. The vendor claims to have a no-log policy.

Anonymous payment options are provided.



Current Location
Austria

Connected!
You can use other apps securely.

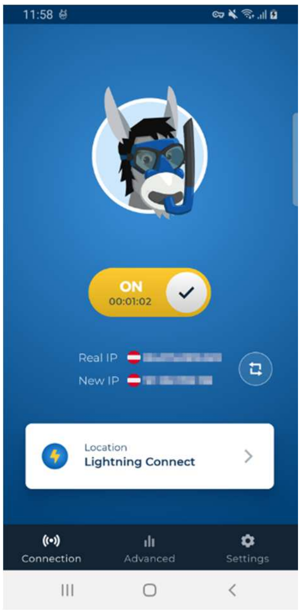
Time Protected
0% this week
(2 minutes)

IP Location
Apps and websites see this VPN
Austria
[redacted]

Certification areas		Notes
All leak tests passed	YES	
Kill-Switch test passed	YES	Leverages Android kill switch, but also provides in-app kill switch
Minimum download speed reached	YES	84 Mbps
Minimum upload speed reached	YES	35 Mbps
Latency below maximum limit	YES	
Refund period over 27 days	YES	30 days
Uses secure protocols	YES	OpenVPN (default), Lightway
Additional information		
Total number of servers exceeds 1,000	YES	3,000*
Servers in over 50 countries	YES	94*
Servers on all continents (except Antarctica)	YES	
Free trial / Freemium	YES	Free trial for 7 days
Simultaneous use on at least 5 devices	YES	
Split tunnelling	YES	Not in combination with Android kill switch
Transparency report (not older than 2 years)	NO	
Warrant canary (not older than 2 years)	NO	
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	YES	
Anonymous payment options	YES	Cryptocurrency
Are third-party VPN components used?	NO	
Headquarters location / jurisdiction is known	YES	British Virgin Islands
Auto-connect	YES	
Dedicated streaming/P2P servers	NO	
Trackers included	YES	3rd-party tracking service
Are legacy protocols supported?	YES	L2TP/IPSec
Extra features included	NO	

*) according to vendor's website as of April 2021

HMA Certification Report (April 2021)



Website: https://www.hidemyass.com/

HMA for Android reached the minimum certification requirements for 2021, and so receives AV-Comparatives' Approved VPN Product Award.

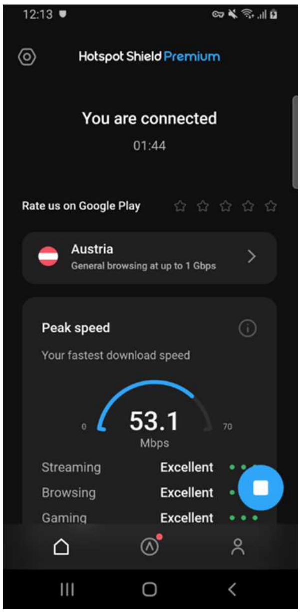
HMA is based in the UK, owned by Avast and was founded in 2005. It makes VPN products for Windows, macOS, Linux and iOS, in addition to Android. HMA claims to have a no-log policy, and publishes both a warrant canary and a transparency report.

The Android VPN includes tracking protection.

Certification areas		**Notes**
All leak tests passed	YES	
Kill-Switch test passed	YES	Leverages Android kill switch
Minimum download speed reached	YES	25 Mbps
Minimum upload speed reached	YES	19 Mbps
Latency below maximum limit	YES	
Refund period over 27 days	YES	30 days
Uses secure protocols	YES	OpenVPN
Additional information		
Total number of servers exceeds 1,000	YES	1,060*
Servers in over 50 countries	YES	210*
Servers on all continents (except Antarctica)	YES	
Free trial / Freemium	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: February 2020)
Warrant canary (not older than 2 years)	YES	Link (last update: March 2021)
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	YES	
Anonymous payment options	NO	
Are third-party VPN components used?	NO	
Headquarters location / jurisdiction is known	YES	UK
Auto-connect	YES	
Dedicated streaming/P2P servers	YES	
Trackers included	YES	3rd-party tracking service
Are legacy protocols supported?	YES	IPSec X auth PSK
Extra features included	YES	Tracking protection

*) according to vendor's website as of April 2021

Hotspot Shield Certification Report (April 2021)



Website: https://www.hotspotshield.com/

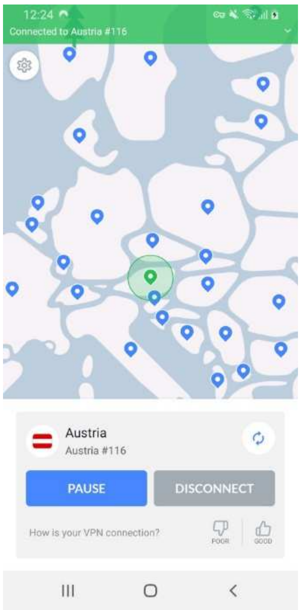
Hotspot Shield VPN for Android reached the minimum certification requirements for 2021, and so receives AV-Comparatives' Approved VPN Product Award.

Hotspot Shield is based in Switzerland and the USA, and was founded in 2008. It is owned by Pango, which was itself acquired by Aura. There are Hotspot Shield VPN products for Windows, macOS, Linux, iOS and routers, in addition to Android.

Certification areas		**Notes**
All leak tests passed	YES	
Kill-Switch test passed	YES	Leverages Android kill switch, but also provides in-app kill switch
Minimum download speed reached	YES	60 Mbps
Minimum upload speed reached	YES	31 Mbps
Latency below maximum limit	YES	
Refund period over 27 days	YES	45 days
Uses secure protocols	YES	Catapult Hydra
Additional information		
Total number of servers exceeds 1,000	YES	1,800*
Servers in over 50 countries	YES	80*
Servers on all continents (except Antarctica)	YES	
Free trial / Freemium	YES	Freemium: 1 US location, 500 MB/month, no optimization for streaming. 7-day premium trial
Simultaneous use on at least 5 devices	YES	
Split tunnelling	YES	
Transparency report (not older than 2 years)	NO	
Warrant canary (not older than 2 years)	NO	
Vendor claims to have a strict no-log policy	NO	
Are traffic logs and/or originating IP address logs collected?	YES	Traffic logs anonymized
Free of ads and upselling	YES	
Anonymous payment options	NO	
Are third-party VPN components used?	NO	
Headquarters location / jurisdiction is known	YES	Switzerland/USA
Auto-connect	YES	
Dedicated streaming/P2P servers	YES	Streaming
Trackers included	YES	3rd-party tracking service
Are legacy protocols supported?	NO	
Extra features included	NO	

*) according to vendor's website as of April 2021

NordVPN Certification Report (April 2021)



Website: https://nordvpn.com/

NordVPN for Android reached the minimum certification requirements for 2021, and so receives AV-Comparatives' Approved VPN Product Award.

NordVPN is based in Panama and was founded in 2012. It claims to have a no-log policy and provides a warrant canary. There are versions of NordVPN for Windows, macOS, Linux, iOS and routers, in addition to Android.

The Android VPN includes the extra features malicious-domain blocking, tap-jacking protection, Dark Web monitor, custom DNS.

Certification areas		**Notes**
All leak tests passed	YES	
Kill-Switch test passed	YES	Leverages Android kill switch
Minimum download speed reached	YES	99 Mbps
Minimum upload speed reached	YES	33 Mbps
Latency below maximum limit	YES	
Refund period over 27 days	YES	30 days
Uses secure protocols	YES	NordLynx (default), OpenVPN
Additional information		
Total number of servers exceeds 1,000	YES	5,415*
Servers in over 50 countries	YES	59*
Servers on all continents (except Antarctica)	YES	
Free trial / Freemium	YES	Free trial for 7 days
Simultaneous use on at least 5 devices	YES	
Split tunnelling	YES	
Transparency report (not older than 2 years)	NO	
Warrant canary (not older than 2 years)	YES	Link (last update: May 2021)
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	YES	
Anonymous payment options	YES	Cryptocurrency
Are third-party VPN components used?	NO	
Headquarters location / jurisdiction is known	YES	Panama
Auto-connect	YES	
Dedicated streaming/P2P servers	YES	P2P, Onion Over VPN, Obfuscated
Trackers included	YES	3rd-party tracking service
Are legacy protocols supported?	NO	
Extra features included	YES	Block malicious domains, tap-jacking protection, Dark Web monitor, custom DNS

*) according to vendor's website as of April 2021

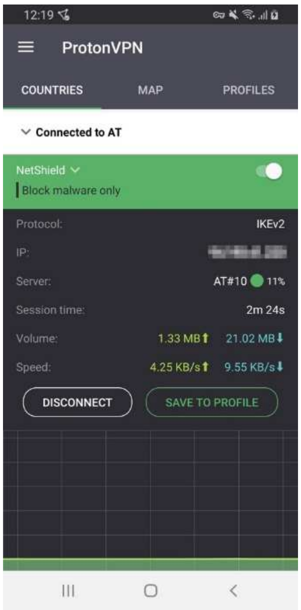
ProtonVPN Certification Report (April 2021)

Website: https://protonvpn.com/

ProtonVPN for Android reached the minimum certification requirements of 2021, and so receives AV-Comparatives' Approved VPN Product Award.

ProtonVPN is based in Switzerland and was founded in 2014. It claims to have a no-log policy. There are ProtonVPN apps for Windows, macOS, Linux, iOS and routers, in addition to Android.

The Android VPN includes extra features: tracking protection, malicious-domain blocking, alternating routing.



Connected to AT

NetShield: Block malware only

Protocol: IKEv2
IP: [redacted]
Server: AT#10 ● 11%
Session time: 2m 24s
Volume: 1.33 MB↑ 21.02 MB↓
Speed: 4.25 KB/s↑ 9.55 KB/s↓

Certification areas		Notes
All leak tests passed	YES	
Kill-Switch test passed	YES	Leverages Android kill switch
Minimum download speed reached	YES	50 Mbps
Minimum upload speed reached	YES	28 Mbps
Latency below maximum limit	YES	
Refund period over 27 days	YES	30 days
Uses secure protocols	YES	IKEv2/IPSec (default), OpenVPN
Additional information		
Total number of servers exceeds 1,000	YES	1,237*
Servers in over 50 countries	YES	55*
Servers on all continents (except Antarctica)	YES	
Free trial / Freemium	YES	Freemium: 3 locations, 1 device, speed limit
Simultaneous use on at least 5 devices	YES	
Split tunnelling	YES	
Transparency report (not older than 2 years)	NO	
Warrant canary (not older than 2 years)	NO	
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	YES	
Anonymous payment options	NO	
Are third-party VPN components used?	NO	
Headquarters location / jurisdiction is known	YES	Switzerland
Auto-connect	YES	
Dedicated streaming/P2P servers	YES	P2P, Plus servers, Secure core, TOR
Trackers included	YES	Self-hosted tracking service
Are legacy protocols supported?	NO	
Extra features included	YES	Tracking protection, block malicious domains, allow alternating routing

*) according to vendor's website as of April 2021

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For inquiries you can contact us via our contact form: https://www.av-comparatives.org/contact/

These results can be used by editors/media/bloggers etc. for free. Please give as source https://www.av-comparatives.org

AV-Comparatives
(June 2021)