Independent Tests of
Anti-Virus Software

AV
comparatives

VPN - Virtual Private Network

35 VPN services put to test

LANGUAGE:	ENGLISH
LAST REVISION:	20TH MAY 2020

WWW.AV-COMPARATIVES.ORG

Contents

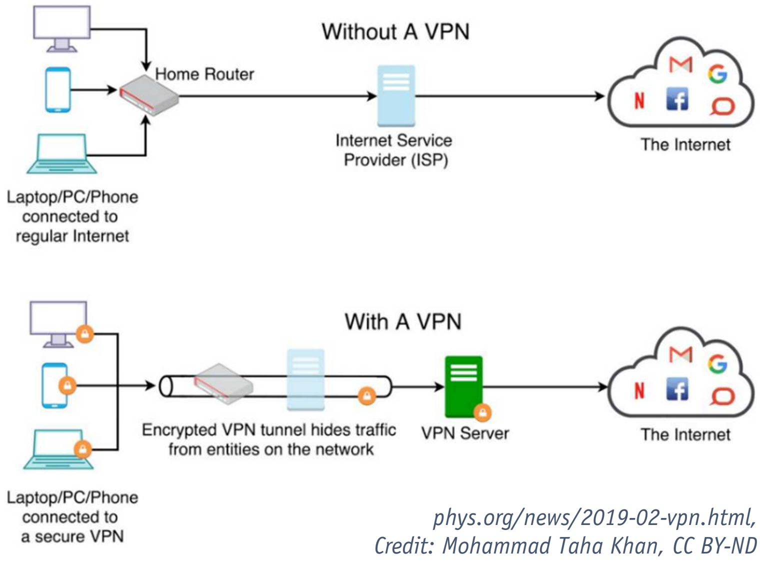
Introduction

The aim of this test is to compare VPN services for consumers in a real-world environment by assessing their security and privacy features, along with download speed, upload speed, and latency. This report starts with an extensive discussion of VPNs in general, the different applications that are available nowadays, plus the advantages and possible risks of using a VPN. We will further explain why VPN providers should have a strict *no-logs policy*. The report is intended to help readers find a VPN program that fits their individual requirements.

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. First, the request is encrypted and sent to the VPN server, which is responsible for resolving the domain name (DNS), and routing it to the target server.


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

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. The traffic forwarded from the VPN server to the target server and back is anonymised, but the possibility of encryption varies from product to product.

Why use a VPN?

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 the same Wi-Fi. It is relatively straightforward for a cybercriminal to intercept your Internet communications and gain access to your private data; with the encryption provided by a VPN, this is no longer possible. Furthermore, one may involuntarily expose information such as IP address and client software to other peers when using P2P technologies and torrent services.

For most consumers, security might no longer be the number one reason for using a VPN. 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. This can make it possible to access specific movies and TV shows from online video streaming services such as Netflix, Amazon Prime Video, Disney+, or the BBC iPlayer, which are not accessible from outside their respective country locations. VPNs can be also used to purchase game titles earlier and more cheaply.

Additionally, there are some VPN programs that are optimised for gaming, as they offer high-speed servers with better connections to popular gaming servers. We note that many consumers associate the name "VPN" with these features alone. There are consumer programs available, mostly free, that provide geo-unlocking functionality without any encryption, yet still describe themselves as VPNs. Bear in mind that in this case, a hacker who intercepts such communications will be able to read everything transmitted.

Vague Privacy

Using a VPN should not be seen as a guarantee of anonymization but viewed rather as a step in this direction. Indeed, though a user's ISP has no access to the traffic sent over a secured connection, it can tell if a VPN is being implemented. This may arouse suspicion, especially if the user has e.g. a criminal history. Furthermore, the VPN provider has access to the user's requests, and how well their privacy is guarded depends on the trustworthiness of the company offering the product. Recently, there has been a surge of interest in online privacy, as ISPs have been legally allowed to collect and sell anonymized user data to third parties (e.g. advertisers) in the USA.[1]

Even more concerning news came from the revelations of Edward Snowden in 2013. He provided evidence that the USA, UK, Canada, Australia and New Zealand gather and share intelligence about one another's citizens in order to circumvent national surveillance laws that prevent them from spying on their own citizens, as well as enabling global surveillance.[2] This co-operation is known as *Five Eyes*, and the revealed documents have shown that intelligence-sharing activities are already taking place on the Internet. In addition, the *Five Eyes* nations co-operate with other countries in matters of international surveillance, leading to the creation of the *Nine Eyes* (Five Eyes + France, Denmark, Norway and the Netherlands) and *Fourteen Eyes* (Nine Eyes + Germany, Italy, Spain, Belgium, and Sweden) alliances. It is also confirmed that further countries such as Israel, Japan, Singapore, and South Korea exchange information with these alliances as well.

Potential Risks

It is safe to say that any of these nations has the power and opportunity to force VPN providers to grant access to data about a user, and to share this with other countries. 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 provider has registered its business; and thirdly, the country where the relevant VPN server is located (regardless of the VPN provider's business location). However, it is not always clear who owns a VPN service or where the company is headquartered.[3] This makes it harder for governments to pressurise VPNs into handing over user data, as they may not have the necessary authority. In several countries, the use of VPNs is either completely banned or allowed only if the VPN is approved by the government. In fact, many people try to bypass blocked content or 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 monitoring their citizens' online activities. This is the reason why VPNs are very popular in countries where they are outlawed.

[1] https://arstechnica.com/tech-policy/2017/03/senate-votes-to-let-isps-sell-your-web-browsing-history-to-advertisers/

[2] https://en.wikipedia.org/wiki/UKUSA_Agreement

[3] https://slate.com/technology/2019/02/best-vpn-companies-trust-privacy.html

The Relevance of No-Logs Policies

Because of international intelligence-sharing agreements, as well as the national laws and surveillance programs already mentioned, many VPN providers offer a strict no-logs policy. In other words, they do not retain any information that could identify users or track their online activities. This means that they cannot provide authorities with such data under any circumstances, because it was never recorded in the first place.

We suggest that readers might like to analyse the privacy policies of VPN providers before buying a product. Many of them claim to not log any traffic, e.g. the websites the user has visited. However, some service providers save connection logs, for both regulatory and technical reasons. These might include timestamps of service logon/logoff, usernames, partial IP addresses, and the temporary IP address assigned by the VPN.

In the past, some VPN vendors who had claimed to have a strict no-logs policy revealed themselves by providing authorities with user information they had collected.[4] In fact, there are various reasons that could be deemed as legitimate for the government/authorities to request information, e.g. to counter terrorism and stop the spread of child pornography. Finally, a strict no-logs policy is very desirable when the headquarter is based in a member country of the Five, Nine, and Fourteen Eyes alliances.

Using VPNs to Spoof Geolocation

As already mentioned, VPNs are now widely used to access e.g. content of video-streaming services that are only available in specific geographical locations. We note that this may violate the terms and conditions of many such service providers, who may take technical steps to prevent the use of VPNs to stream videos to unauthorised locations. For example, specific IP addresses or address ranges known to be used by VPN providers may be blacklisted, or measures to detect masquerading techniques may be taken.[5]

In some cases, the VPN may simply leak the genuine IP address. A constant game of cat and mouse ensues, in which one side constantly tries to identify and circumvent the measures employed by the other. A VPN product that unlocks a particular streaming service one day may fail to do so the next, and vice versa. Clearly, a VPN service that provides a number of servers in a particular country is more likely to unlock a streaming service in that country than one that offers only a single server, although this is not a given.

Due to this situation, users who want to access streaming services that are only available in other countries could (whilst taking full responsibility for their own actions) take advantage of the free trial periods or money-back guarantees offered by many of the VPN providers.

[4] https://torrentfreak.com/ipvanish-no-logging-vpn-led-homeland-security-to-comcast-user-180505/, https://torrentfreak.com/purevpn-explains-how-it-helped-the-fbi-catch-a-cyberstalker-171016/

[5] https://help.netflix.com/en/node/277

Test Procedure

We tested and reviewed 35 popular VPNs, whereby we mimicked the behaviour of a user residing in Europe who wanted to connect to a VPN server located in the USA, and vice versa. Our test assessed the two important features of privacy and speed. Hence, we divided the test into three parts:

- The *Leak Test*, where we evaluated the degree of the 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-out.
- The *Performance Test*, where we measured the VPN's download and upload speeds and latency (response time).

Lab Setup

We utilized Microsoft's Azure cloud infrastructure in order to perform the test, with locations in the UK and USA. As the aim of this test is to compare VPNs in an environment that is close to a real-world scenario, we limited the available bandwidth to 100/100 Mbps (download/upload speeds respectively), which is a realistic value for Internet connections in (sub-)urban areas. Moreover, the enormous bandwidth of the cloud infrastructure ensured that the relatively small bandwidth of 100/100 Mbps was always available, so that the Internet connection itself was never the limiting factor in our tests.

The latest version of each VPN product available at the time of testing (March 2020) was bought from the vendor's website, downloaded, and installed on the test system in accordance with the instructions provided. Where product settings allowed it, we configured the program to launch and connect automatically 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 Washington, D.C. for the USA, and London for the UK, in so far as these were available.

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 the following instances:

- Public IP address: The external IP address of the test system that is visible on the Internet.
- DNS address: The IP address of the DNS server resolving DNS requests on behalf of the test system.
- Torrent IP address: The IP address of the Torrent client used that is visible when sharing files via a P2P network.
- Torrent DNS address: The IP address of the DNS server resolving DNS requests on behalf of the Torrent client used.
- Web Real-Time Communication (WebRTC): WebRTC provides audio/video communication and P2P file sharing from within the browser, which might expose the true local or public IP address.
- HTTP request: HTML elements embedded in a web page can send requests to external sources, and thus leak the true IP address.

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, in a so-called *kill-switch* test. The VPN should provide a mechanism that prevents the genuine public IP address from being leaked to the Internet in the period between the 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 connection loss by deactivating and reactivating the Ethernet network adapter (and thus the network connection) and recording the system's public IP address before and after this.

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, share files in a P2P network, or run a gaming server on their PC. 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 each mouse click or key press.

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 get a broad overview of the traffic during different times of day and days of the week, we repeated the tests every two hours for one week, including the weekend.

We used one set of test systems in the UK, which connected to VPN servers in Washington, D.C. (USA), and one set of test systems in the USA that connected to VPN servers in London (UK), in so far as these locations were available. Having established a transatlantic VPN connection from the UK to the USA or vice versa, we measured the download and upload speed, as well as the latency, between the test system and three speed-testing servers. Of these three servers, two were specific: both were in the destination country and geographically close to the exit point of the VPN server the test system was connected to. The third server was selected automatically, on the basis that it should be the one closest to the VPN server and thus provide the fastest connection.

In addition, we set up reference systems without a VPN product installed. In that case, we only used the two specified servers on the respective other side of the Atlantic Ocean. We did not use the automatically selected server, as this would be in the same country as the reference system and thus irrelevant.

Tested Products

We tested and reviewed 35 popular VPN products for Windows. For each product, the latest version available at the time of testing (March 2020) was used.

For the test, we used the paid version of the products and their default protocol.

Product	Version	Vendor	Headquarter
Avast SecureLine VPN	5.5	Avast Software s.r.o.	Czech Republic
AVG Secure VPN	1.10	Avast Software s.r.o.	Czech Republic
Avira Phantom VPN	2.32	Avira Operations GmbH & Co. KG	Germany
Bitdefender VPN	24.0	Bitdefender	Romania
BullGuard VPN	1.3	BullGuard Ltd.	UK
CyberGhost VPN	7.2	CyberGhost S.A.	Romania
ExpressVPN	7.8	Express VPN International Ltd.	British Virgin Islands
F-Secure Freedome	2.32	F-Secure Corp.	Finland
hide.me VPN	3.2	eVenture Ltd.	Malaysia
HMA VPN	5.0	Privax Ltd.	UK
Hotspot Shield	9.6	AnchorFree Inc.	USA
IPVanish	3.4	Mudhook Media Inc.	USA
Ivacy	5.3	PMG Pte. Ltd.	Singapore
Kaspersky Secure Connection	20.0	AO Kaspersky Lab	Russia
McAfee Safe Connect	2.6	McAfee LLC	USA
mySteganos Online Shield VPN	2.0	Steganos Software GmbH	Germany
Nord VPN	6.27	Tefincom & Co. S.A.	Panama
Norton Secure VPN	1.9	NortonLifeLock Inc.	USA
Panda Dome VPN	20.00	Panda Security S.L.	Spain
Private Internet Access	1.8	Private Internet Access Inc.	USA
Private Tunnel	2.8	OpenVPN Technologies Inc.	USA
PrivateVPN	2.3	Privat Kommunikation Sverige AB	Sweden
ProtonVPN	1.13	Proton Technologies AG	Switzerland
PureVPN	7.1	GZ Systems Ltd.	Hong Kong
SaferVPN	5.0	Safer Social Ltd.	Israel
StrongVPN	2.4	Strong Technology LLC	USA
Surfshark	2.6	Surfshark Ltd.	British Virgin Islands
TorGuard	3.98	VP Networks LLC	USA
Trust.Zone VPN	1.1.	Trusted Solutions Ltd.	Seychelles
TunnelBear	4.1	TunnelBear Inc.	Canada
VPNSecure	2.1	VPNSecure Pty Ltd.	Australia
VPN Unlimited	7.0	KeepSolid Inc.	USA
VyprVPN	3.3	Golden Frog GmbH	Switzerland
Windscribe	1.83	Windscribe Ltd.	Canada
ZenMate VPN	5.0	ZenGuard GmbH	Germany

Additional Product Information

Consolidations & Collaborations

Over the past few years, many small companies have entered the VPN market with their own solutions for protecting the user's privacy, anonymizing the online activities, and accessing geo-restricted content.

Many of these VPN services are actually owned by bigger companies, but might still operate independently. Here, we would like to list interesting collaborations/acquisitions relating to the tested VPN products within the past few years.[6]

- **Avast SecureLine VPN** and **AVG Secure VPN** are owned by Avast. **Privax Ltd.**, the company behind **HMA VPN**, has been a subsidiary of Avast since 2016.
- The **Gaditek** company owns **Ivacy** and **PureVPN**.
- **J2 Global** acquired **IPVanish** and **StrongVPN** from StackPath, along with **SaferVPN,** in 2019. It also owns several other VPN brands which are not listed in this report.[7]
- **Kape Technologies** bought **CyberGhost VPN**, **Private Internet Access**, and **ZenMate VPN** between 2017 and 2019.
- **TunnelBear** was acquired by **McAfee** in March 2018.[8]
- The VPN solutions of **Bitdefender**, **Kaspersky**, and **Panda** are powered by **AnchorFree Inc.** (Hotspot Shield).
- **BullGuard** announced a partnership with **Nord VPN** in November 2018.[9]

While testing and reviewing products for this report, we found some products that had very similar websites and terminology to other VPN products. It would be reasonable to assume that there might be business connections between these providers. Readers who are interested to know the background of the products they purchase might like to do their own research into this.

As a marketing incentive, many antivirus (AV) vendors have integrated third-party VPN technology into their security solutions. Users who are concerned about privacy might like to consider that AV programs are able to access to most parts of the operating system, as well as the user data, and might log many actions the user takes. We note that **Bitdefender** and **Panda** currently appear to offer their VPN products only in combination with their respective AV solutions.

[6] https://thenextweb.com/tech/2019/01/23/youd-be-surprised-how-many-vpns-are-owned-by-the-same-company/
[7] https://www.techradar.com/news/ign-owner-j2-global-snaps-up-major-vpn-brands
[8] https://venturebeat.com/2018/03/08/mcafee-acquires-vpn-company-tunnelbear/
[9] https://www.techradar.com/news/bullguard-and-nordvpn-announce-new-partnership

Supported Protocols

In the upcoming table, we present an overview of important encryption, network, and communication protocols as well as popular VPN applications, supported by the tested products. We list these protocols for the Windows platform only (IKEv2 and L2TP only in combination with IPSec). **Bitdefender**, **Kaspersky**, and **Panda** leverage the proprietary VPN protocol *Catapult Hydra* by **Hotspot Shield**.
For more details about the pros and cons of each protocol, please visit this website.

Product	OpenVPN	IKEv2/ IPSec	L2TP/ IPSec	PPTP	SOCKS	SSTP	SSH	WireGuard
Avast SecureLine VPN	✓	✗	✗	✗	✗	✗	✗	✗
AVG Secure VPN	✓	✗	✗	✗	✗	✗	✗	✗
Avira Phantom VPN	✓	✗	✗	✓	✗	✗	✗	✗
Bitdefender VPN	✓	✗	✗	✗	✗	✗	✗	✗
BullGuard VPN	✓	✓	✓	✗	✗	✗	✗	✗
CyberGhost VPN	✓	✓	✓	✓	✗	✗	✗	✗
ExpressVPN	✓	✓	✓	✓	✗	✗	✗	✗
F-Secure Freedome	✓	✗	✗	✗	✗	✗	✗	✗
hide.me VPN	✓	✓	✗	✗	✓	✓	✗	✗
HMA VPN	✓	✗	✓	✓	✗	✗	✗	✗
Hotspot Shield	✗	✗	✗	✗	✗	✗	✗	✗
IPVanish	✓	✓	✓	✓	✓	✓	✗	✗
Ivacy	✓	✓	✓	✓	✗	✓	✗	✗
Kaspersky Secure Connection	✓	✓	✓	✓	✗	✗	✗	✗
McAfee Safe Connect	✓	✗	✗	✗	✗	✗	✗	✗
mySteganos Online Shield VPN	✓	✓	✗	✗	✗	✗	✗	✗
Nord VPN	✓	✓	✗	✗	✓	✗	✗	✗
Norton Secure VPN	✓	✗	✗	✗	✗	✗	✗	✗
Panda Dome VPN	✗	✗	✗	✗	✗	✗	✗	✗
Private Internet Access	✓	✗	✓	✓	✓	✗	✗	✓
Private Tunnel	✓	✗	✗	✗	✗	✗	✗	✗
PrivateVPN	✓	✓	✓	✓	✓	✗	✗	✗
ProtonVPN	✓	✓	✗	✗	✗	✗	✗	✗
PureVPN	✓	✓	✓	✓	✗	✓	✗	✗
SaferVPN	✓	✓	✓	✓	✗	✗	✗	✗
StrongVPN	✓	✓	✓	✗	✗	✓	✗	✓
Surfshark	✓	✓	✗	✗	✓	✗	✗	✗
TorGuard	✓	✓	✓	✓	✓	✓	✓	✓
Trust.Zone VPN	✓	✗	✓	✗	✗	✗	✗	✗
TunnelBear	✓	✓	✗	✗	✓	✗	✗	✗
VPNSecure	✓	✗	✗	✓	✓	✗	✓	✗
VPN Unlimited	✓	✓	✗	✗	✓	✗	✗	✓
VyprVPN	✓	✓	✓	✓	✗	✗	✗	✗
Windscribe	✓	✓	✗	✗	✓	✗	✗	✗
ZenMate VPN	✓	✓	✓	✗	✗	✗	✗	✗

✓ Protocol supported ✗ Protocol not supported

Logging

The following table summarises information from the privacy policy of each product. By “traffic” we mean the monitoring and recording of browsing activities (privacy implications), whereas the remaining columns, such as “No Dates/Timestamps” merely relate to keeping track of how one connects to a VPN service, and so fall under the category of “connection” logs. In some cases, there may be different levels of logging for different versions of the same product. For example, data transfer limits applied to the restricted version of a product might only be practicable if data usage is monitored; for the full version of the same program, such monitoring might not be required. Even though traffic logs are certainly considered to be the most privacy invasive, one should also be wary of connection logs, as they might reveal more information than one expects. For instance, from an IP address, one might be able to obtain an approximate geolocation of the corresponding user. However, minimal connection logs that just keep track of bandwidth usage, timestamps, and VPN-assigned IP addresses can be justified on technical grounds, as they help the vendor to manage the service, e.g. by avoiding server overloads.

Please note that the information in this table relates solely to the use of the VPN services (not to other areas such as use of cookies on their websites). It was obtained from the respective vendors’ websites at the time of writing. Therefore, we cannot take any responsibility for the accuracy or truthfulness of these statements. Also, factors such as the applicable law in the country where the headquarters is located, the degree to which third parties are involved in the data process, and additional restrictions when using the free version of the same product, should all be considered. For a more detailed overview, we encourage the reader to examine the corresponding privacy policies.

Product	No Traffic Logs	No Dates / Timestamps	No Bandwidth Logs	No IP Address Logs	Transparency Report / Warrant Canary
Avast SecureLine VPN	✓	✗	✗	✗[10]	Yes
AVG Secure VPN	✓	✗	✗	✗[10]	Yes
Avira Phantom VPN	✓	✓	✗	✓	Yes
Bitdefender VPN	?	?	?	⊘	None
BullGuard VPN	✓	✓	✓	✓	None
CyberGhost VPN	✓	⊘	✓	✓	Yes
ExpressVPN	✓	✗	✓	✓	None
F-Secure Freedome	⊘	✗	✗	✗	None
hide.me VPN	✓	✓	⊘	✓	Yes
HMA VPN	✓	⊘	⊘	✓	Yes
Hotspot Shield	⊘	✓	✗	⊘	Yes
IPVanish	✓	✓	✓	✓	None
Ivacy	✓	✓	✓	✓	None
Kaspersky Secure Connection	?	?	?	?	None
McAfee Safe Connect	?	?	?	?	None
mySteganos Online Shield VPN	✓	?	⊘	✓	None
Nord VPN	✓	✓	✓	✓	Yes
Norton Secure VPN	✓	✓	⊘	⊘	None
Panda Dome VPN	?	?	?	?	None

[10] Collects VPN-assigned IP address and subnet only of originating IP address

Private Internet Access	✓	✓	✓	✓	Yes
Private Tunnel	✓	✗	✗	✗	None
PrivateVPN	✓	✓	✓	✓	None
ProtonVPN	✓	✗	✓	✓	Yes
PureVPN	✓	✗	✗	✓	None
SaferVPN	✓	✗	✗	✓	None
StrongVPN	✓	✓	✓	✓	None
Surfshark	✓	✓	✓	✓	None
TorGuard	✓	✓	✓	✓	None
Trust.Zone VPN	✓	⊘	✓	✓	Yes
TunnelBear	✓	✓	✗	✓	Yes
VPNSecure	✓	✓	✓	✓	None
VPN Unlimited	✓	✓	✓	✓	None
VyprVPN	✓	✓	✓	✓	None
Windscribe	✓	✗	✗	✓	Yes
ZenMate VPN	✓	✓	✓	✓	None

✓ No data logged ✗ Data logged
? Not explicitly stated, unclear policy ⊘ Data logged but anonymised

"Data logged but anonymised" means that the vendor explicitly states in its privacy policy that the collected data is anonymised.

Please note that **IPVanish**, **PrivateVPN**, **StrongVPN**, **TorGuard**, and **ZenMate** provide only short statements with limited information about their respective logging policies. Whilst we have stated "No data logged" in all four categories for these vendors in the table, we would prefer to see more detailed privacy policies from them, listing exactly what is and is not logged.

Payment Information

The following table shows relevant information regarding trial versions, freemium restrictions, the refund period, and the most common payment options for each product. Some providers offer more anonymous payment methods. The information listed below is based on what was available on the German and US websites of each VPN provider in April 2020. It is subject to change in the future, and may vary depending on the number of devices included in the subscription, country/region, deal size or term, and discounts applied. Users should pay careful attention to details of initial prices, renewal prices, special offers and validity periods when buying a product. For example, the price for the initial purchase might be discounted, meaning the user might have to pay considerably more for the (auto-)renewal of their subscription. Moreover, users should inform themselves whether the auto-renewal function is activated on the initial purchase, and if they will receive any notification prior to the expiration of the subscription. In fact, it might in some cases be cheaper to cancel the current subscription before it runs out and make a completely new purchase rather than extending the existing one for another term. More details can be found in the individual review of each product.

					Approx. Price for 5 Devices / 1 Year	
Product	Free Trial	Trial Period / Freemium Restrictions	Refund Period	Common Payment Options	USD	EUR
Avast SecureLine VPN	✓	7 days	30 days	Credit/Debit card, PayPal, Wire transfer	90	90
AVG Secure VPN	✓	7 days	30 days	Credit/Debit card, PayPal, Wire transfer	90	90
Avira Phantom VPN	Freemium	No UK location, 500 MB data per month	30 days	Credit/Debit card, PayPal	78	60
Bitdefender VPN	✓	30 days	30 days	Credit/Debit card, PayPal, Wire transfer	85	65
BullGuard VPN	✗	n/a	30 days	Credit/Debit card, PayPal, Wire transfer	83	73
CyberGhost VPN	✗	n/a	45 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	72	72
ExpressVPN	✗	n/a	30 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	100	n/a
F-Secure Freedome	✓	30 days	30 days	Credit/Debit card, PayPal, Wire Transfer, Digital wallets	90	80
hide.me VPN	Freemium	Fewer locations, 10 GB data per month	30 days	Credit/Debit card, PayPal, Wire transfer Cryptocurrency	100	100
HMA VPN	✓	7 days	30 days	Credit/Debit card, PayPal	84	72

Hotspot Shield	Freemium	1 US location only, 500 MB data per month, no streaming optimization	45 days	Credit/Debit card, PayPal	96	96
IPVanish	✗	n/a	30 days	Credit/Debit card, PayPal	78	n/a
Ivacy	✓	7 days	30 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	42	55
Kaspersky Secure Connection	Freemium	Automatic location selection, 200 MB per day	30 days	Credit/Debit card, PayPal, Wire transfer	30	30
McAfee Safe Connect	Freemium	250 MB data per month	30 days	Credit/Debit card, PayPal, Wire transfer, Digital wallets	48	48
mySteganos Online Shield VPN	✓	7 days	30 days	Credit/Debit card, PayPal, Wire transfer	50	50
Nord VPN	✗	n/a	30 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	84	89
Norton Secure VPN	✗	n/a	60 days	Credit/Debit card, PayPal, Wire transfer	100	70
Panda Dome VPN	Freemium	Automatic location selection, 150 MB data per day	30 days	Credit/Debit card, PayPal	77	62
Private Internet Access	✗	n/a	30 days	Credit/Debit card, PayPal, Cryptocurrency, Digital wallets	40	37
Private Tunnel	✓	7 days	60 days	Credit/Debit card, PayPal, Digital wallets	48	n/a
PrivateVPN	✗	n/a	30 days	Credit/Debit card, PayPal, Cryptocurrency	50	n/a
ProtonVPN	Freemium	3 locations, 1 device, speed limit	30 days	Credit/Debit card, PayPal, Cryptocurrency	96	96
PureVPN	✗	n/a	31 days	Credit/Debit card, PayPal	70	70
SaferVPN	✗	n/a	30 days	Credit/Debit card, PayPal, Cryptocurrency	66	54
StrongVPN	✗	n/a	30 days	Credit/Debit card, PayPal, Digital wallets	70	n/a
Surfshark	✗	n/a	30 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	72	60
TorGuard	✓	7 days	7 days	Credit/Debit card, Wire transfer, Cryptocurrency, Digital wallets	60	n/a
Trust.Zone VPN	✗	n/a	10 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	94	88
TunnelBear	Freemium	500 MB data per month	✗	Credit/Debit card, Cryptocurrency	60	n/a

VPNSecure	✓	30 days, 1 US location only, 2GB during test period	7 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	80	n/a
VPN Unlimited	✓	7 days	7 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	60	n/a
VyprVPN	✗	n/a	30 days	Credit/Debit card, PayPal	45	45
Windscribe	Freemium	10 locations, 2 GB data per month	3 days	Credit/Debit card, PayPal, Wire transfer, Cryptocurrency, Digital wallets	49	n/a
ZenMate VPN	Freemium	4 locations, 2 MB/s speed limit, Browser extension only	30 days	Credit/Debit card, PayPal, Wire transfer	40	40

✓ Offered ✗ Not offered

Test Results

Leak & Kill-Switch Tests

The table below shows the results of the various elements of the Leak Test and Kill-Switch Test. For each component of the Leak Test, a product is deemed to have failed if the IP address of the original network was leaked. In the Kill-Switch Test, a product fails if it does not block the Internet connection in the time between the VPN dropping out and being re-established.

Not all VPNs implement a *visible* kill-switch option whose settings can be changed in the VPN client. The test determines whether there is a kill-switch *function* in practice. A product that does not block the Internet connection when the VPN drops out will inevitably leak the user's genuine IP address, thus compromising security and privacy.

Product	Public IP	DNS Server	WebRTC Local IP	WebRTC Public IP	Torrent IP/DNS	HTTP Request	Kill Switch
Avast SecureLine VPN	✓	✓	✓	✓	✓	✓	✓
AVG Secure VPN	✓	✓	✓	✓	✓	✓	✓
Avira Phantom VPN	✓	✓	✓	✓	✓	✓	✓
Bitdefender VPN	✓	✓	✓	✓	✓	✓	✗
BullGuard VPN	✓	✓	✓	✓	✓	✓	✓
CyberGhost VPN	✓	✓	✓	✓	✓	✓	✓
ExpressVPN	✓	✓	✓	✓	✓	✓	✓
F-Secure Freedome	✓	✓	✓	✓	✓	✓	✓
hide.me VPN	✓	✓	✓	✓	✓	✓	✓
HMA VPN	✓	✓	✓	✓	✓	✓	✓
Hotspot Shield	✓	✓	✓	✓	✓	✓	✓
IPVanish	✓	✓	✓	✓	✓	✓	✓
Ivacy	✓	✓	✓	✓	✓	✓	✓
Kaspersky Secure Connection	✓	✓	✓	✓	✓	✓	✗
McAfee Safe Connect	✓	✓	✓	✓	✓	✓	✗
mySteganos Online Shield VPN	✓	✓	✓	✓	✓	✓	✓
Nord VPN	✓	✓	✓	✓	✓	✓	✓
Norton Secure VPN	✓	✓	✓	✓	✓	✓	✗
Panda Dome VPN	✓	✗	✓	✓	✓	✓	✗
Private Internet Access	✓	✓	✓	✓	✓	✓	✓
Private Tunnel	✓	✓	✓	✓	✓	✓	✓
PrivateVPN	✓	✓	✓	✓	✓	✓	✓
ProtonVPN	✓	✓	✓	✓	✓	✓	✓
PureVPN	✓	✓	✓	✓	✓	✓	✓
SaferVPN	✗	✗	✓	✗	✗	✓	✓
StrongVPN	✓	✓	✓	✓	✓	✓	✓
Surfshark	✓	✓	✓	✓	✓	✓	✓
TorGuard	✓	✓	✓	✓	✓	✓	✓

Trust.Zone VPN	✓	✓[11]	✓	✓	✓	✓	✓
TunnelBear	✓	✓	✓	✓	✓	✓	✓
VPNSecure	✓	✓	✓	✓	✓	✓	✓
VPN Unlimited	✓	✓	✓	✓	✓	✓	✓
VyprVPN	✓	✓	✓	✓	✓	✓	✓
Windscribe	✓	✓	✓	✓	✓	✓	✓
ZenMate VPN	✓	✓	✓	✓	✓	✓	✓

✓ Test passed ✗ Test failed

[11] The setting "DNS leak protection" is disabled by default, which results in a DNS leak. If enabled, no leak was observed.

Performance Test

In the following section, we present the results of the Performance Test, starting with the results for the download and upload speeds, as well as the latency. To make comparing the tested products easier, we provide a table where we assign each test result to a cluster, rating the VPN's performance from "very fast" to "very slow" for the download/upload speed and "very low" to "very high" for the latency results.

All the sub-tests were performed every two hours for a week, including the weekend. The maximum bandwidth was limited for each test system to 100/100 Mbps, which is a realistic value for Internet connections in (sub-)urban areas. Different measurement methods have been used get more balanced results and to improve statistical accuracy. For each VPN, over one thousand measurements points were taken over the course of one week. In the charts, the results without a VPN connection are shown as a vertical line.

During testing, we also looked at how the results changed over the course of the week. For this, the test results have been grouped by weekday and into two-hour time slots for each day. No obvious correlation between time and VPN performance was observed, i.e. even during high-peak times, the VPNs delivered consistent performance.

Download speed

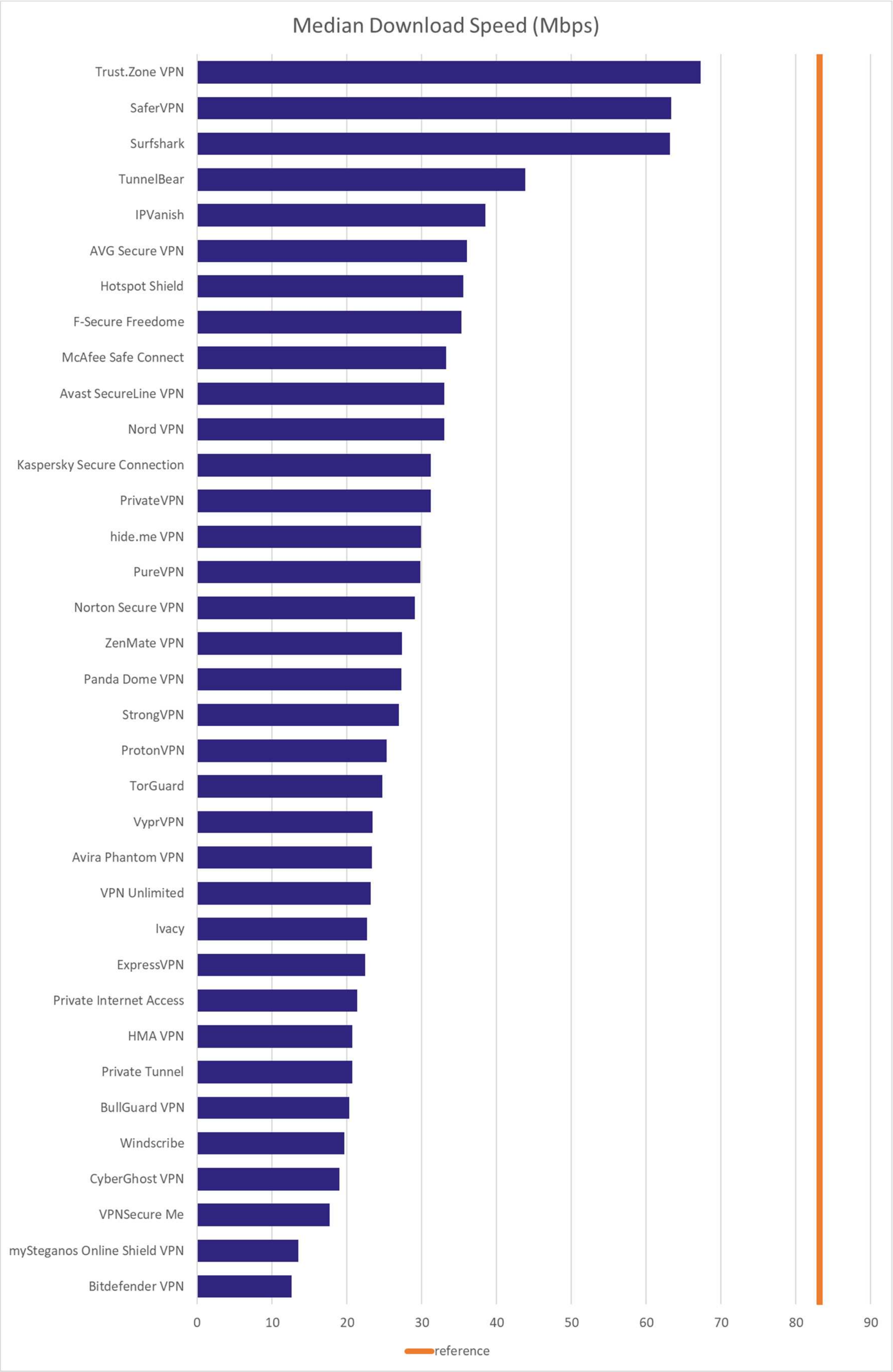


Figure 1: Median download speed in Mbps, speed without VPN indicated by the vertical line (higher is better)

Upload speed

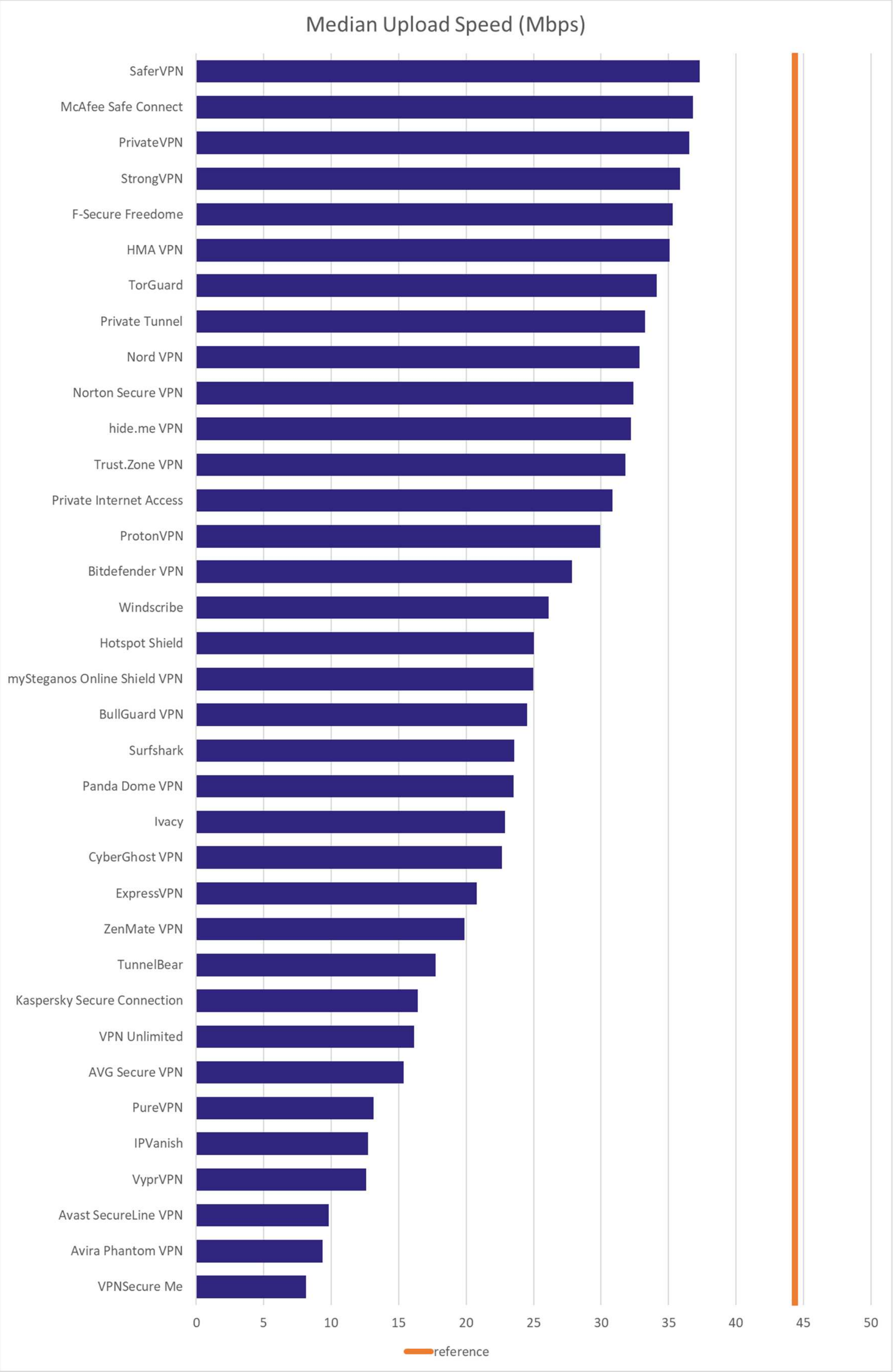


Figure 2: Median upload speed in Mbps, speed without VPN indicated by the vertical line (higher is better)

Latency

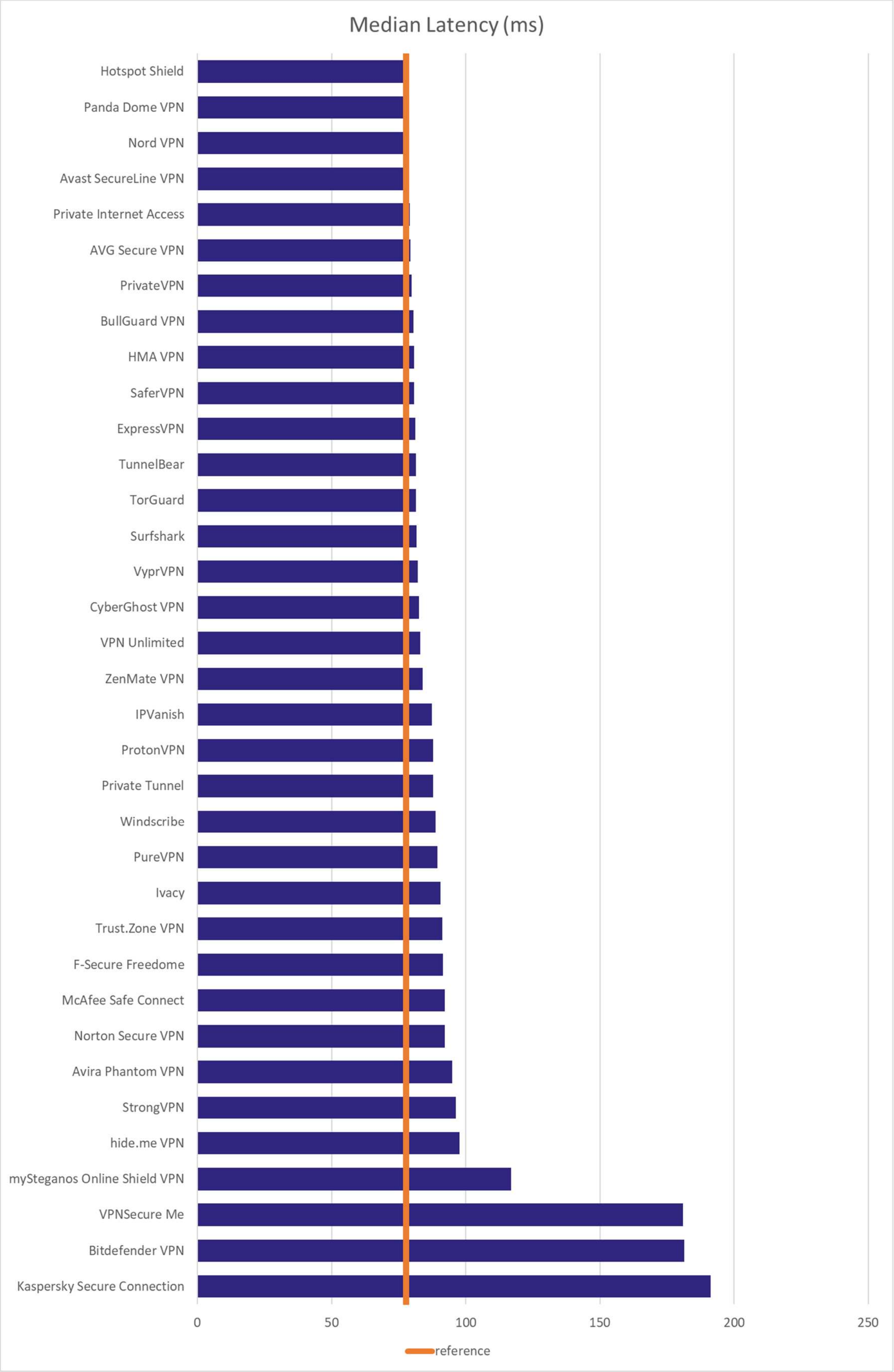


Figure 3: Median latency in ms, latency without VPN indicated by the vertical line (lower is better)

As can be seen, using a VPN always results in a decrease in the connection speed. This is because the bandwidth is limited not only by the ISP but also by the VPN server.

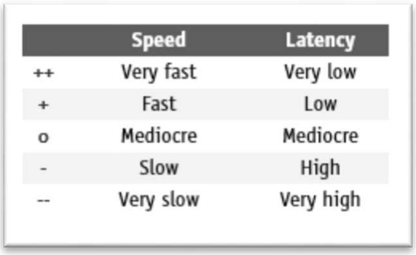
Typically, the median download speed with an activated VPN is only slightly above one third (36%) of the download speed without a VPN. However, the top three VPNs **Trust.Zone VPN**, **SaferVPN**, and **Surfshark** achieve between 75% and 80% of the reference download speed.

The upload speeds show less of a difference between an active VPN connection and the direct connection, with VPN upload speeds averaging 56% of the reference value. In comparison to the download speeds, there is a more linear speed drop-off, with twelve VPNs (**SaferVPN, McAfee Safe Connect, PrivateVPN, StrongVPN, F-Secure Freedome, HMA VPN, TorGuard, Private Tunnel, Nord VPN, Norton Secure VPN, hide.me VPN, Trust.Zone VPN**) achieving more than 70% of the reference upload speed.

For the most part, the latency of VPN connections is similar to the latency of the non-VPN connection, with half of the tested VPNs increasing the latency only by 10% of the reference value. However, **VPNSecure**, **Bitdefender VPN**, and **Kaspersky Secure Connection** had a latency of more than twice the value of a direct connection. While a latency of around 80ms might seem slow, we have to consider that these times are measured for transatlantic connections and are therefore to be expected.

Performance Overview

Here, we provide a table for easy comparison of the performance of all the tested products, which is rated using five categories. The ranges for the categories were defined by the testers after consulting statistical methods and are based on clusters built with the hierarchal clustering method. A key to the symbols is shown on the right.



	Speed	Latency
++	Very fast	Very low
+	Fast	Low
o	Mediocre	Mediocre
-	Slow	High
--	Very slow	Very high

Product	Download Speed	Upload Speed	Latency
Avast SecureLine VPN	+	-	++
AVG Secure VPN	+	o	++
Avira Phantom VPN	o	-	+
Bitdefender VPN	-	+	-
BullGuard VPN	o	+	++
CyberGhost VPN	o	+	++
ExpressVPN	o	o	++
F-Secure Freedome	+	++	+
hide.me VPN	+	++	+
HMA VPN	o	++	++
Hotspot Shield	+	+	++
IPVanish	+	o	+
Ivacy	o	+	+
Kaspersky Secure Connection	+	o	-
McAfee Safe Connect	+	++	+
mySteganos Online Shield VPN	-	+	o
Nord VPN	+	++	++
Norton Secure VPN	+	++	+
Panda Dome VPN	+	+	++
Private Internet Access	o	++	++
Private Tunnel	o	++	+
PrivateVPN	+	++	++
ProtonVPN	o	++	+
PureVPN	+	o	+
SaferVPN	++	++	++
StrongVPN	o	++	+
Surfshark	++	+	++
TorGuard	o	++	++
Trust.Zone VPN	++	++	+
TunnelBear	+	o	++
VPNSecure	o	-	-
VPN Unlimited	o	o	++
VyprVPN	o	o	++
Windscribe	o	+	+
ZenMate VPN	+	o	++

Discussion

In the following section, we will discuss the key points of this report, state interesting observations made during testing, and provide some guidance to readers looking for a VPN[12].

General Security Observations

Most of the tested products support more than one VPN protocol the user can choose from, to allow for different use cases. All of them implement the popular protocol OpenVPN, except for **Hotspot Shield** and **Panda Dome VPN** as they leverage a proprietary VPN protocol. We note that 14 of the products support PPTP, which is known to be insecure due to its weak encryption and non-existent authentication features.

Users who frequently connect to public networks, such as the Wi-Fi at a hotel, restaurant, or other public place, should use a VPN. This is because it provides protection against man-in-the-middle attacks, by encrypting the communication channel and thus the data being transferred. However, obsolete or broken encryption methods do not prevent intruders from accessing and decrypting the intercepted data. Therefore, check in advance if the chosen VPN service implements the latest encryption technologies. Like any other program, VPN services can contain vulnerabilities and other security flaws.[13] Therefore, it is advisable to always keep the software up to date.

Test Results

28 products passed both our Leak Test and Kill-Switch Test flawlessly. **Panda Dome VPN** failed only the DNS server component of the Leak Test, and **Trust.Zone VPN** passed the same test only if we manually enabled its “DNS leak protection” option. It is unclear to us why this is disabled by default. **SaferVPN** showed several deficiencies in our Leak Test, leaking the genuine IP address in four out of six instances. Furthermore, **Bitdefender VPN, Kaspersky Secure Connection, McAfee Safe Connect, Norton Secure VPN,** and **Panda Dome VPN** failed our Kill-Switch Test because they do not provide such a function at all.

In the Performance Test, **Trust.Zone VPN**, **SaferVPN**, and **Surfshark** performed very well overall, especially in the download speed test. Of the remaining products, 18 had fast or very fast download speeds, 23 had fast or very fast upload speeds, and only 7 had a mediocre or high latency for a transatlantic connection.

Users who want to hide their location in order to access geo-blocked articles, news, or other websites, need a secure and reliable VPN connection, and might not be concerned about the speed. On the other hand, gamers typically look for VPNs with a very low latency (hence fast reaction times) but will primarily not be so interested in privacy. For streaming geo-blocked videos in particular, both privacy (hiding the genuine IP address) and speed are essential factors. As mentioned previously, streaming services work hard to identify and block access via VPNs. Therefore, users might want to check if their intended VPN actually works with the desired streaming services, or be ready to switch VPN providers.

[12] https://ssd.eff.org/en/module/choosing-vpn-thats-right-you
[13] https://www.techadvisor.co.uk/news/vpn/vpn-apps-fake-updates-3787350/

Logging & Privacy Policies

Most of the tested VPN products explicitly state in their privacy policies that they do not collect any data at all, or only do so anonymously (e.g. omit the last octet of the IP address). **IPVanish**, **PrivateVPN**, **StrongVPN**, **TorGuard**, and **ZenMate VPN** limit themselves to very short statements about their logging policy, rather than listing all the information they do or do not retain. For **Bitdefender VPN, Kaspersky Secure Connection, McAfee Safe Connect, mySteganos Online Shield VPN,** and **Panda Dome VPN**, either the privacy policy as a whole, or the information regarding collection of specific data categories, was unclear to us. We would welcome it if all VPN vendors made their logging and data-sharing policies clear, even to non-technical users.

Although many VPN providers state that they do not keep any logs, there is no way for us to verify this, and it is up to the user to choose which service they trust their data with. 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.

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 statement, called *Warrant Canary*, stating that they have NOT had any such requests.[14] For users valuing their privacy, it is important to stay up to date about changes in the VPN policies, possible data breaches, and any changes in ownership of the VPN provider.

Privacy-conscious users who want to mask their identity should pay special attention to the VPN's logging policy, as well as who manages the business, where the company is based, and where the VPN-server exit points are located (with respect to the jurisdictions). Where VPNs operate from is especially important considering the intelligence-sharing agreements between the Five, Nine, and Fourteen Eyes alliances. As previously mentioned, there have been cases in the past of VPN providers co-operating with law enforcement agencies to uncover the identity of users, even when based in a country that is not performing the investigation.[15] Finally, as antivirus programs might potentially have a high level of system access, users with major privacy concerns might want to use AV software from vendors unrelated to the vendor that makes their VPN software.

[14] https://www.eff.org/deeplinks/2014/04/warrant-canary-faq

[15] https://torrentfreak.com/ipvanish-no-logging-vpn-led-homeland-security-to-comcast-user-180505/, https://torrentfreak.com/purevpn-explains-how-it-helped-the-fbi-catch-a-cyberstalker-171016/

Further Recommendations

It is always worth doing a quick search on the Internet for information about the reputation of a product or company associated with it. Look for serious news articles on trustworthy websites, or posts in the information security community, in order to get a better picture of the product.

For readers who are thinking about purchasing a VPN, we suggest looking for a trial version, restricted free version, or unconditional money-back guarantee, to test out the product first. We also recommend paying close attention to the prices, especially any differences between the initial purchase price and renewal price (e.g. if initial discounts are applied), and conditions attached to the refund policy, if there is one. It might also be worth comparing the prices for different countries. To experience more anonymity, some VPNs (about half of the tested products) offer cryptocurrency payment options.

There is no universally best VPN, because everyone has their own requirements and preferences. We suggest that users choose the VPN which is best suited to their own use case and budget. We have gathered some important questions that users should ask themselves when they are considering choosing a VPN:

- What are the main reasons for me to use a VPN?
- How much do I care about privacy?
- Is a high connection speed or low latency important to me?
- Can I test whether the product will unlock specific geo-blocked content, without losing a lot of money if it does not?
- Is there a free product that would serve my needs?
- If I need to buy a product, how much am I willing to pay?
- Do I want anonymous payment options?
- How trustworthy does the VPN provider appear to be?
- Is it important to prevent law enforcement agencies from accessing my data?

Individual VPN Product Reviews

On the following pages, we provide individual reviews of all the tested products. For each product, we have given the vendor's name and the location of their headquarter. There is a screenshot of the main program window.

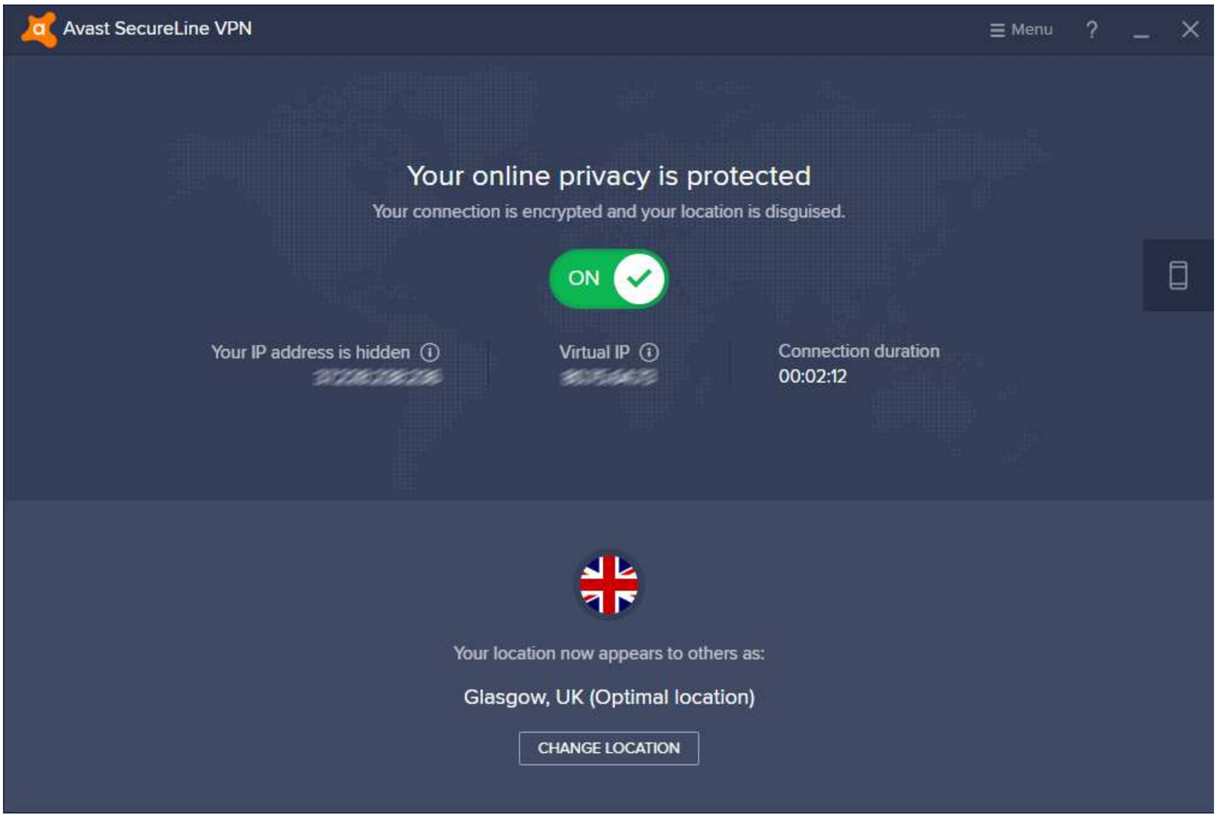
We state whether there is a free trial period and/or money-back guarantee, so that it can be tested out at no financial risk to the user. With regard to prices, we assume the user wants to use the product on a minimum of 5 devices for 1 year, and so provide the minimum cost for this. We give prices in US dollars for users buying from the USA website, and prices in Euro for users buying from the German website. Common payment options are listed, including cryptocurrencies where available. We also note whether a boxed version may be available, as this might provide a de facto anonymous payment option.

We then say if the product is suitable for non-expert users, i.e. is easy to set up and use. A list of the number of country locations is provided, and whether the USA and UK are included. There is a summary of the Leak Test, Kill-Switch Test, and Performance Test results. We then provide a brief description of the process for installing and using the product. We also list the main configuration options, including whether the program can be set to start/connect automatically when the user logs on to Windows, whether there is a kill-switch setting, and what choice of protocols (if any) is offered.

We then list the countries in which servers were provided at the time of testing. Please note that for any VPN product, the servers provided, and streaming services that can be accessed, can change without warning. We conclude each review with a table showing the pros and cons of each product.

Avast SecureLine VPN

Avast Software s.r.o.
Czech Republic



Your online privacy is protected

Your connection is encrypted and your location is disguised.

Your IP address is hidden [redacted]

Virtual IP [redacted]

Connection duration
00:02:12

Your location now appears to others as:

Glasgow, UK (Optimal location)

At a glance

- Avast SecureLine VPN is a paid-for VPN product
- Website: https://www.avast.com/secureline-vpn
- Free trial: 7 days, 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 90
- Pricing DE: 5 devices / 1 year: EUR 90
- Common payment options: credit/debit card, PayPal, wire transfer
- A boxed version may be available, so the licence key will not be linked to your credit card or email
- Suitable for non-expert users
- Other features: Avast Secure Browser

Summary

Avast SecureLine VPN is very simple to set up and use, so a good choice for non-experts. You can choose from 35 different countries, amongst which are the USA and UK. A range of pricing plans is available, going from 1 PC, 1 year to 5 PCs, 3 years. Both a free trial of 7 days and a 30-day money-back guarantee are provided.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as “fast”, the upload speed as “slow” and the latency as “very low”.

Regarding the privacy policy, Avast clearly states that it stores connection logs, and hence connection timestamps, partial originating IP address, VPN-assigned IP addresses and amount of data transmitted, although no traffic logs are gathered.

Ease of use

The setup process is very quick and easy, with no decisions to make. The program interface is very clear and simple. There is a big *On / Off* button in the upper half of the window, and a *Change Location* button in the lower half. The genuine IP address, virtual IP address and virtual location are also displayed prominently. Settings can be accessed from the Menu button at the top of the window. The main configuration options are: show notifications when the VPN is switched on or off; start the program automatically with Windows; turn on automatically when connected to the Internet; prompt to turn on when connected to the Internet; exclude trusted (private) networks; activate kill switch to block Internet access if the VPN disconnects. Avast SecureLine VPN supports only the OpenVPN protocol.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Belgium, Brazil, Canada (2), China, Czech Republic, Denmark, Finland, France, Germany (2), Hungary, Israel, Italy, Japan, Luxembourg, Malaysia, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Singapore, Russia (2), South Africa, South Korea, Spain (2), Sweden, Switzerland, Taiwan, Turkey, United Kingdom (3), Ukraine, United States (16).

Pros

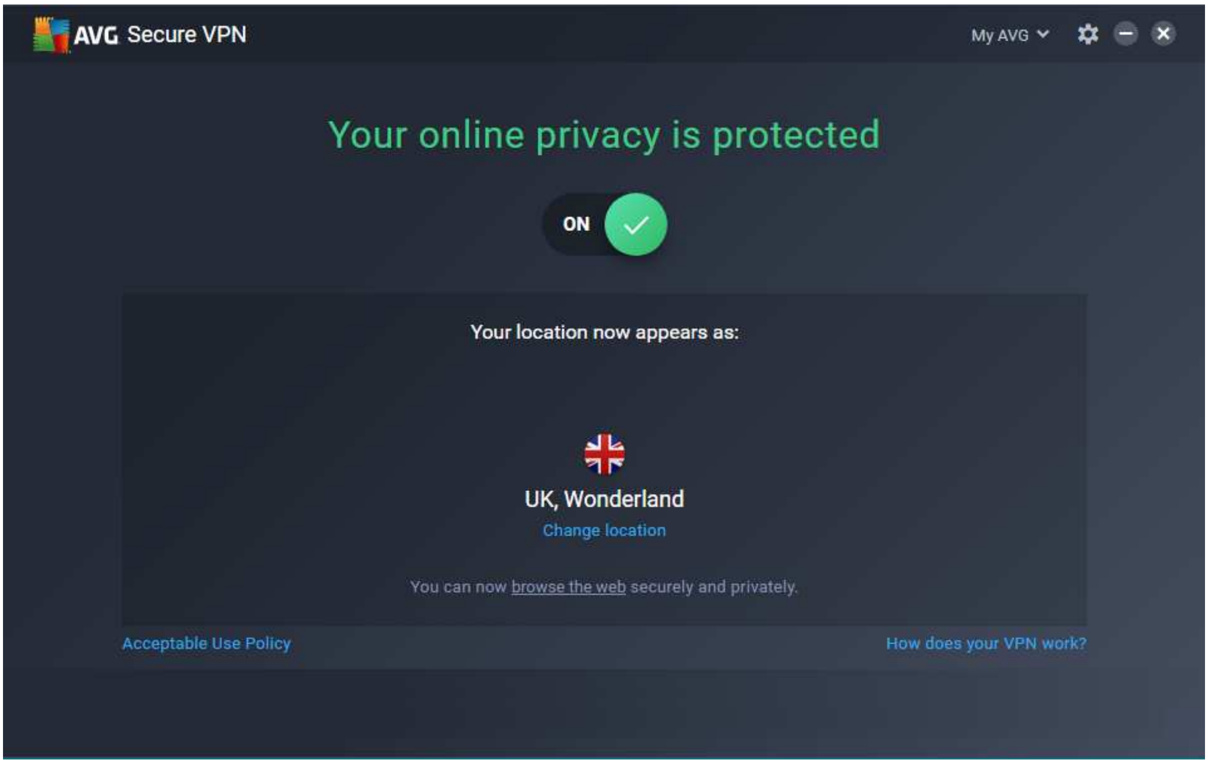
- 7-day free trial
- 30-day money-back guarantee
- Boxed version may be available
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very low latency
- No traffic logging

Cons

- No choice of protocols
- Slow upload speed
- Connection logging

AVG Secure VPN

Avast Software s.r.o.
Czech Republic



Your online privacy is protected

Your location now appears as:

UK, Wonderland

You can now browse the web securely and privately.

At a glance

- AVG Secure VPN is a paid-for VPN product
- Website: https://www.avg.com/en-ww/secure-vpn
- Free trial: 7 days, 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 90
- Pricing DE: 5 devices / 1 year: EUR 90
- Common payment options: credit/debit card, PayPal, wire transfer
- Suitable for non-expert users

Summary

AVG Secure VPN is very easy to set up and use, so it's suited to all users. You can select from 37 countries, including the UK and USA. A range of pricing plans is available, with 1-year, 2-year and 3-year subscriptions. A free trial of 7 days is provided, along with a 30-day money-back guarantee.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "mediocre" and the latency as "very low".

In the product's privacy policy, the company states that for technical reasons connection timestamps, partial originating IP address, the VPN-assigned IP addresses and bandwidth usage are stored, although no traffic logs are gathered.

Ease of use

The program can be set up very simply, by downloading the installer from the AVG website and running it. There are no decisions to make. When the program first starts, a brief explanation of the product is shown. You can select your virtual location. A pop-up appears, prompting you to activate auto-connect. The program is very easy to use. The main window has a prominent On/Off switch, and a *Change Location* button. Settings are found by clicking the cogwheel icon in the top right-hand corner. The main configuration options in the settings dialog are: start program automatically with Windows; connect VPN automatically when connected to the Internet; prompt to connect VPN when connected to the Internet; activate kill switch, to block Internet access if the VPN disconnects. AVG Secure VPN supports only the OpenVPN protocol.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Belgium, Brazil, Canada (2), Hong Kong, Czech Republic, Denmark, Finland, France, Germany (2), Hungary, Iceland, Ireland, Israel, Italy, Japan, Luxembourg, Malaysia, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Singapore, Russia (2), South Africa, South Korea, Spain (2), Sweden, Switzerland, Taiwan, Turkey, United Kingdom (3), Ukraine, United States (16).

Pros

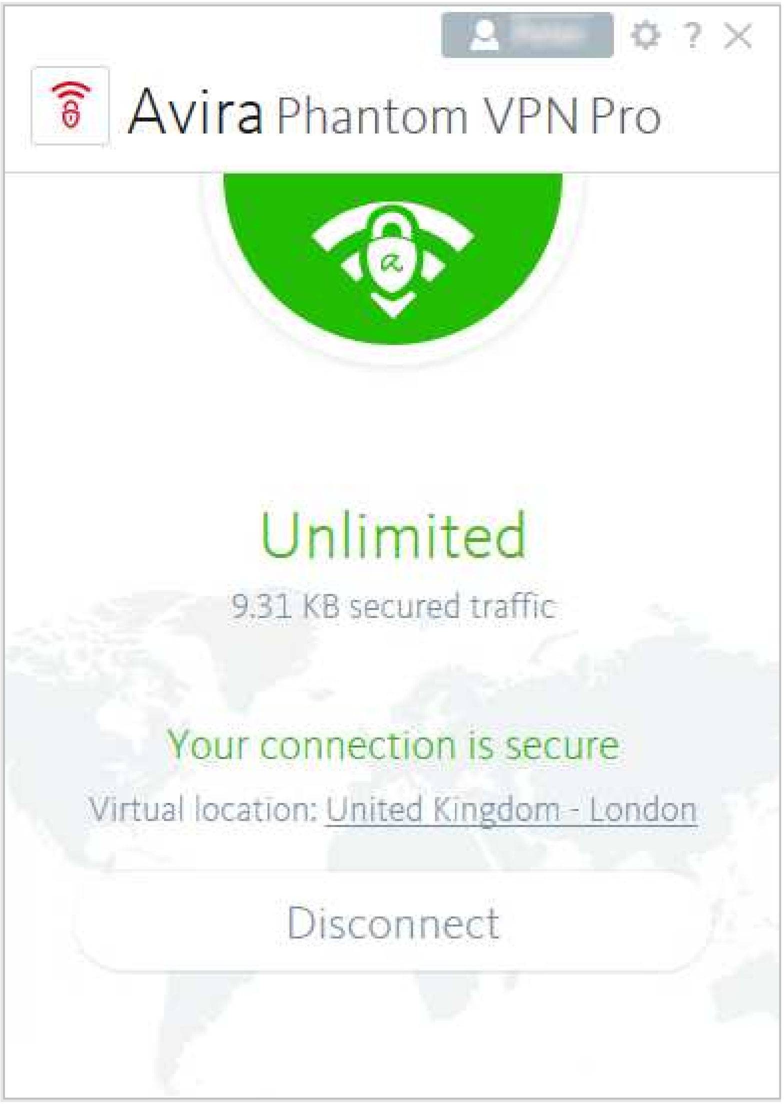
- 7-day free trial
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very low latency
- No traffic logging

Cons

- No choice of protocols
- Mediocre upload speed
- Connection logging

Avira Phantom VPN

Avira Operations GmbH & Co. KG
Germany



Unlimited

9.31 KB secured traffic

Your connection is secure

Virtual location: United Kingdom - London

At a glance

- Avira Phantom VPN is a paid-for VPN product (a restricted free version is also available)
- Website: https://www.avira.com/en/avira-phantom-vpn
- The restricted free version provides no UK location and is limited to 500 MB of data traffic per month
- 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 78
- Pricing DE: 5 devices / 1 year: EUR 60
- Common payment options: credit/debit card, PayPal
- Suitable for non-expert users
- Other features: block malicious sites and content

Summary

It's really easy to install and use Avira Phantom VPN, so it's ideal for non-expert users. You can choose from 37 different countries, including the USA and UK and both a 1-month and a 1-year plan are available. You can try the program out by using the restricted free version, or take advantage of the 30-day money-back guarantee. Both the monthly and the yearly plans let you install the software on unlimited devices.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "mediocre", the upload speed as "slow" and the latency as "low".

According to the company's FAQs, the provider logs only bandwidth usage in terms of amount of data consumed.

Ease of use

Setting up Avira Phantom VPN is extremely simple, as there are no options or decisions to make. The program is also very simple to use. You select a server by clicking on the *Virtual location* link, then click *Secure my connection*. The main configuration options in the settings dialog are: auto-connect VPN for Wi-Fi networks; launch at system start; block malicious sites and content; kill switch. Avira Phantom VPN supports the protocols OpenVPN and PPTP.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Chile, Czech Republic, Denmark, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Israel, Italy, Japan, Mexico, Moldova, Netherlands; Norway, Poland, Romania, Russia, Serbia, Singapore, Slovenia, Spain, Sweden, Switzerland, United Kingdom (2), United States (13).

Pros

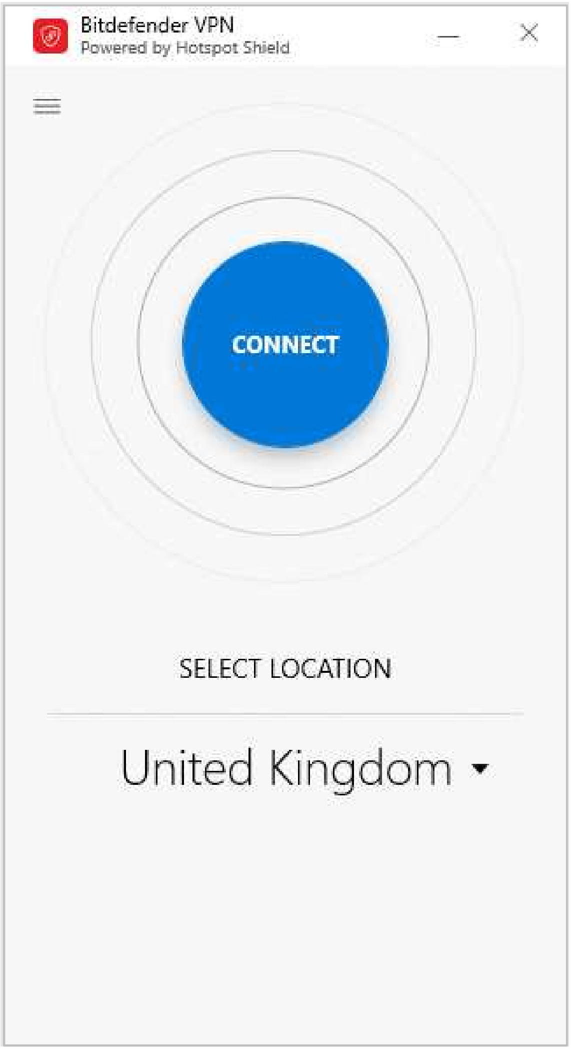
- Restricted free version
- 30-day money-back guarantee for Pro version
- Very simple to install and use
- Can connect automatically when Wi-Fi used
- Leak Test passed
- Kill-Switch Test passed
- Low latency
- No traffic logging

Cons

- Mediocre download speed
- Slow upload speed
- Minimal connection logging

Bitdefender VPN

Bitdefender
Romania



At a glance

- **Important note:** Bitdefender VPN can only be purchased if you already have a Bitdefender antivirus (AV), or purchase one at the same time. In the latter case, the total price depends on the selected AV product.
- Bitdefender VPN is a paid-for VPN product
- Website: https://www.bitdefender.com/solutions/vpn.html
- Free trial: 30 days, 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 85 (with Bitdefender Total Security)
- Pricing DE: 5 devices / 1 year: EUR 65 (with Bitdefender Total Security)
- Common payment options: credit/debit card, PayPal, wire transfer
- Suitable for non-expert users

Summary

Bitdefender VPN is only an option for you if you already have, or wish to buy, a Bitdefender antivirus product. The combined price of the VPN and antivirus product depends on which security solution one purchases, whereby the table above shows the cheapest combination given 5 devices. Bitdefender VPN is simple to use, and provides a choice of 27 different countries, including the UK and USA. Both a 30-day free trial and a 30-day money-back guarantee are provided.

It passed our Leak Test, but failed the Kill-Switch Test, so you won't be disconnected from the Internet if the VPN drops out. We rated the download speed as "slow", the upload speed as "fast" and the latency as "high".

Bitdefender's privacy policy states that the company stores, in hashed form, both user IDs and devices IP addresses, which are then processed by the AnchorFree company. The latter, in turn, claims to store duration of the VPN session, bandwidth usage and all accessed domains on an anonymized basis, in such a way as not to associate a user with a particular connection session. A lack of detail in Bitdefender's policy makes it difficult to understand to what extent this third party is involved with the user's data.

Ease of use

For our functionality test, we purchased Bitdefender VPN along with Bitdefender Internet Security. The installer for Internet Security also installed Premium VPN at the same. We simply had to activate the product by adding the licence key to our Bitdefender account. The product is very simple to use. You just select a location from the drop-down list in the program window, and click *Connect*.
The configuration options in the settings dialog are: display product notifications; automatically launch Bitdefender VPN Windows startup; connect VPN automatically when using unsecured Wi-Fi networks. There is no kill switch. Bitdefender VPN supports the protocols OpenVPN and Hotspot Shield's Catapult Hydra.

Server locations

At the time of testing, the product had servers in these countries: Argentina, Australia, Brazil, Canada, Switzerland, Czech Republic, Germany, Denmark, Spain, France, United Kingdom, Hong Kong, Indonesia, Ireland, India, Italy, Japan, Mexico, Netherlands, Norway, Romania, Russia, Sweden, Singapore, Turkey, Ukraine, United States.

Pros

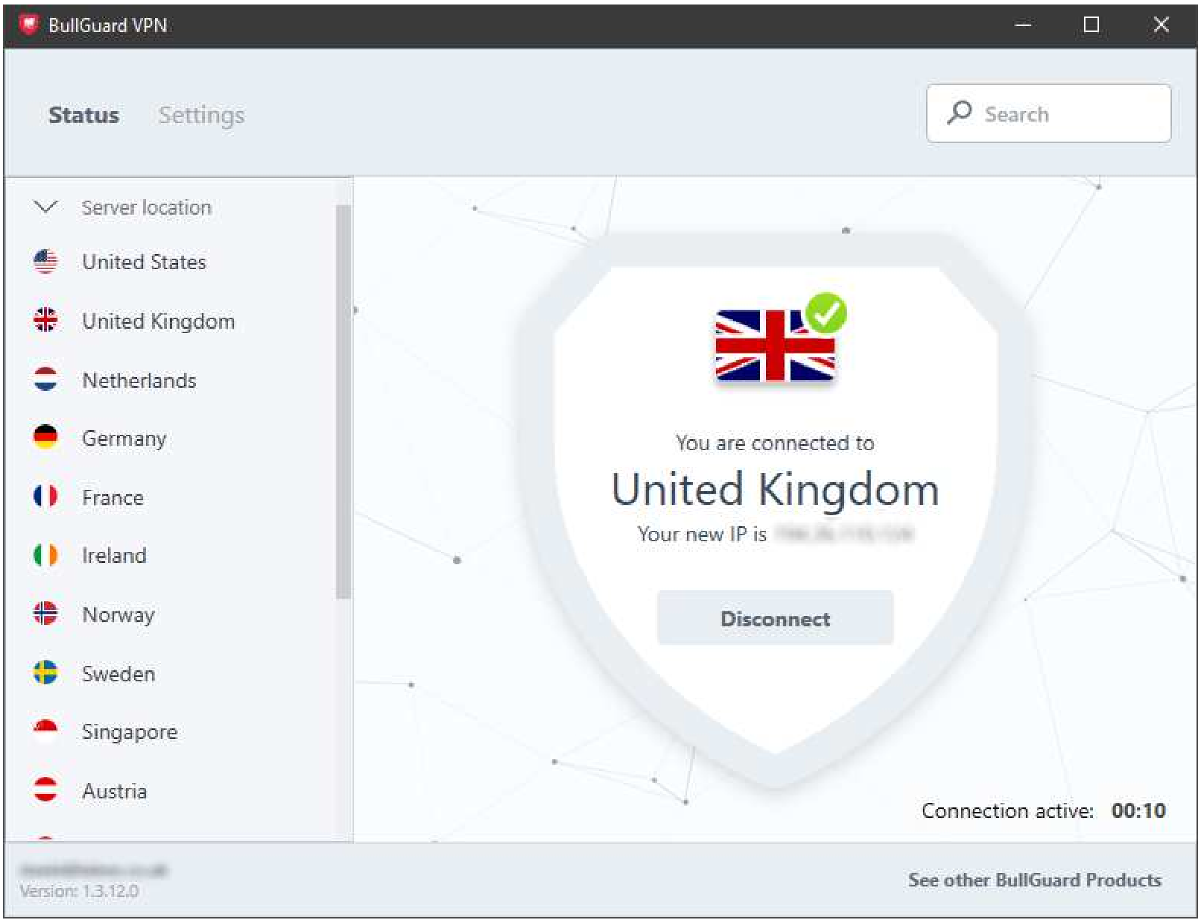
- 30-day free trial
- 30-day money-back guarantee
- Very simple to use
- Can connect automatically on unsecured Wi-Fi
- Leak Test passed
- Fast upload speed

Cons

- Kill-Switch Test failed
- Slow download speed
- High latency
- Unclear privacy policy

BullGuard VPN

BullGuard Ltd.
UK



You are connected to
United Kingdom
Your new IP is [redacted]

Connection active: **00:10**

[redacted]
Version: 1.3.12.0

At a glance

- BullGuard VPN is a paid-for VPN product
- Website: https://www.bullguard.com/products/bullguard-vpn.aspx
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 83
- Pricing DE: 5 devices / 1 year: EUR 73
- Common payment options: credit/debit card, PayPal, wire transfer
- Suitable for non-expert users

Summary

BullGuard VPN is a good choice for non-expert users, as it is very simple to install and use. There is a choice of 16 different countries, the UK and USA included. The pricing plans include 1, 2 and 3-year subscriptions. No free trial is available, although a 30-day money-back guarantee is provided.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "mediocre", the upload speed as "fast" and the latency as "very low".

The company's privacy policy claims that it follows a no-logs policy.

Ease of use

To set up BullGuard VPN, download the installer from the vendor's website and run it; all you need to do then is click *Install*. The program is very simple to use. Just click on a server location from the list on the left-hand side, and you will be automatically connected. The main configuration options in the settings dialog are: auto connect to specified server; start program with Windows; kill switch; custom DNS. BullGuard VPN supports the protocols OpenVPN, IKEV2, and L2TP.

Server locations

At the time of testing, the product had servers in these countries: United States, United Kingdom, Netherlands, Germany, France, Ireland, Norway, Sweden, Singapore, Austria, Spain, Belgium, Australia, Canada, Switzerland, Denmark.

Pros

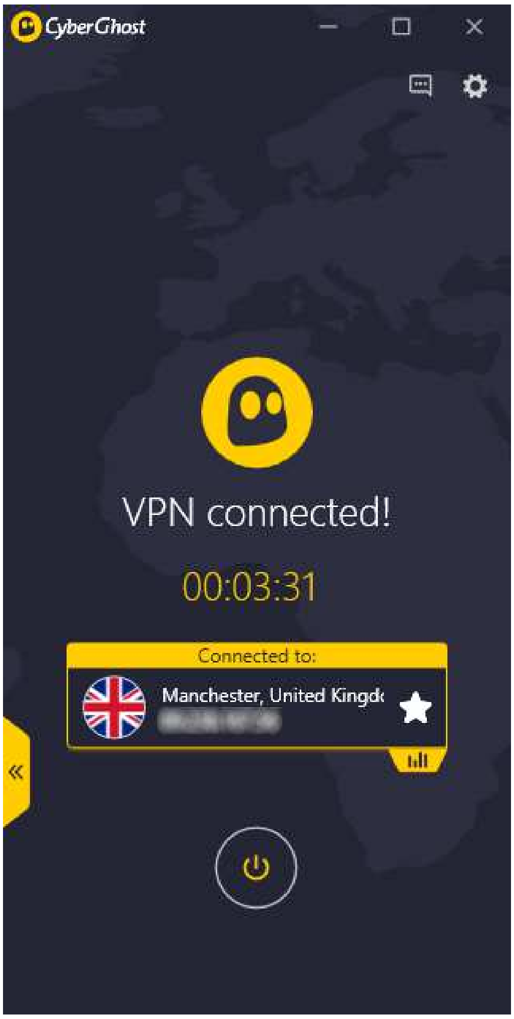
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast upload speed
- Very low latency
- No traffic/connection logging

Cons

- No free trial
- Mediocre download speed

CyberGhost VPN

CyberGhost S.A.
Romania



VPN connected!

00:03:31

Connected to:

Manchester, United Kingd
[redacted]

At a glance

- CyberGhost VPN is a paid-for VPN product
- Website: https://www.cyberghostvpn.com
- Free trial: none, but there is a 45-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 72
- Pricing DE: 5 devices / 1 year: EUR 72
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Suitable for non-expert users

Summary

CyberGhost VPN is well suited to non-expert users, as it is easy to set up and use. 90 country locations are available, including the USA and UK. The pricing plans include 1-month, 1-year, 2-year and 3-year subscriptions. A money-back guarantee is provided (14 days for the monthly plan, 45 days for the 1 and 2-year plans), but no free trial is available.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as “mediocre”, the upload speed as “fast” and the latency as “very low”.

According to the company’s privacy policy, neither connection logs nor traffic logs are gathered, whereby the vendor claims (quoted verbatim) *“The performance of the Service is measured through a series of events sent anonymously to third-party services (MixPanel) which is building aggregate data based on certain trends”*. Said data keeps track of connection attempts and successes, and the countries the requests originated from.

Ease of use

Setting up CyberGhost VPN is very simple – just download and run the installer, and installation completes in a couple of clicks. It’s also very easy to use: just select a server from the “Connect to” list, and slide the On/Off switch to the right. The main configuration options in the settings dialog are: user interface language; kill switch; DNS leak protection; disable IPv6 when using VPN. CyberGhost VPN supports the protocols OpenVPN, IKEV2, L2TP, and PPTP.

Server locations

At the time of testing, the product had servers in these countries: Albania, Algeria, Andorra, Argentina, Armenia, Australia, Austria, Bahamas, Bangladesh, Belarus, Belgium, Bosnia & Herzegovina, Brazil, Bulgaria, Cambodia, Canada, Chile, China, Columbia, Costa Rica, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Georgia, Germany, Greece, Greenland, Hong Kong, Hungary, Iceland, India, Indonesia, Iran, Ireland, Isle of Man, Israel, Italy, Japan, Kazakhstan, Kenya, South Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Macao, North Macedonia, Malaysia, Malta, Mexico, Moldova, Monaco, Mongolia, Montenegro, Morocco, Netherlands, New Zealand, Nigeria, Norway, Pakistan, Panama, Philippines, Poland, Portugal, Qatar, Romania, Russia, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Venezuela, Vietnam.

Pros

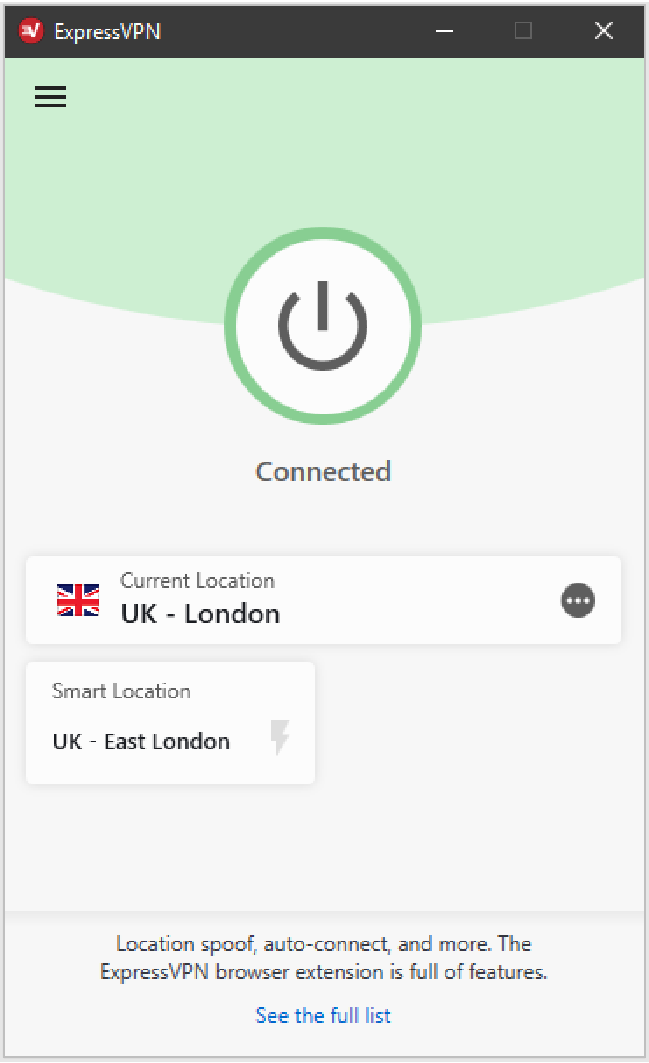
- 45-day money-back guarantee
- Very simple to install and use
- Leak Test passed
- Kill-Switch Test passed
- Fast upload speed
- Very low latency
- No traffic logging
- Fast upload speed
- Very low latency
- No traffic logging

Cons

- No free trial
- Mediocre download speed
- Minimal connection logging

ExpressVPN

Express VPN International Ltd.
British Virigin Islands



Location spoof, auto-connect, and more. The ExpressVPN browser extension is full of features.

At a glance

- ExpressVPN is a paid-for VPN product
- Website: https://www.expressvpn.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 100
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Suitable for non-expert users
- Other features: browser add-on

Summary

ExpressVPN is simple to install and use, so fine for non-expert users. There is a choice of over 100 countries, including the USA and UK. The pricing plans include 1-month, 6-month and 1-year subscriptions. A 30-day money-back guarantee is available, although there is no free trial.

The program passed our Leak Test and Kill-Switch Test. We rated the download speed as “mediocre”, the upload speed as “mediocre” and the latency as “very low”.

The company's privacy policy states that it follows a “no-logs policy”, but information registered to the user’s account regarding the dates the VPN is used, from which country/ISP, and to which VPN location the user connects to, is still gathered.

Ease of use

To set up ExpressVPN, download and run the installer from the vendor’s website. The program is very simple to use: just select a country and server from the button in the middle of the window, then click the *Connect* button. The main configuration options in the settings dialog are: start the program with Windows; connect to last-used location when the program starts; kill switch to stop all Internet traffic if the VPN connection is lost; IPv6 leak protection. ExpressVPN supports the protocols OpenVPN, IKEV2, L2TP, and PPTP.

Server locations

At the time of testing, the product had servers in these countries: Albania, Algeria, Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahamas, Bangladesh, Belarus, Belgium, Bhutan, Bosnia & Herzegovina, Brazil, Brunei, Bulgaria, Cambodia, Canada, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech, Republic, Denmark, Ecuador, Egypt, Estonia, Finland, France, Georgia, Germany, Greece, Guatemala, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kazakhstan, Kenya, Kyrgyzstan, Laos, Latvia, Liechtenstein, Lithuania, Luxembourg, Macau, Malaysia, Malta, Mexico, Moldova, Monaco, Mongolia, Montenegro, Myanmar, Nepal, Netherlands, New Zealand, North Macedonia, Norway, Pakistan, Panama, Peru, Philippines, Poland, Portugal, Romania, Serbia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sri, Lanka, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Kingdom, United States, Uruguay, Uzbekistan, Venezuela, Vietnam.

Pros

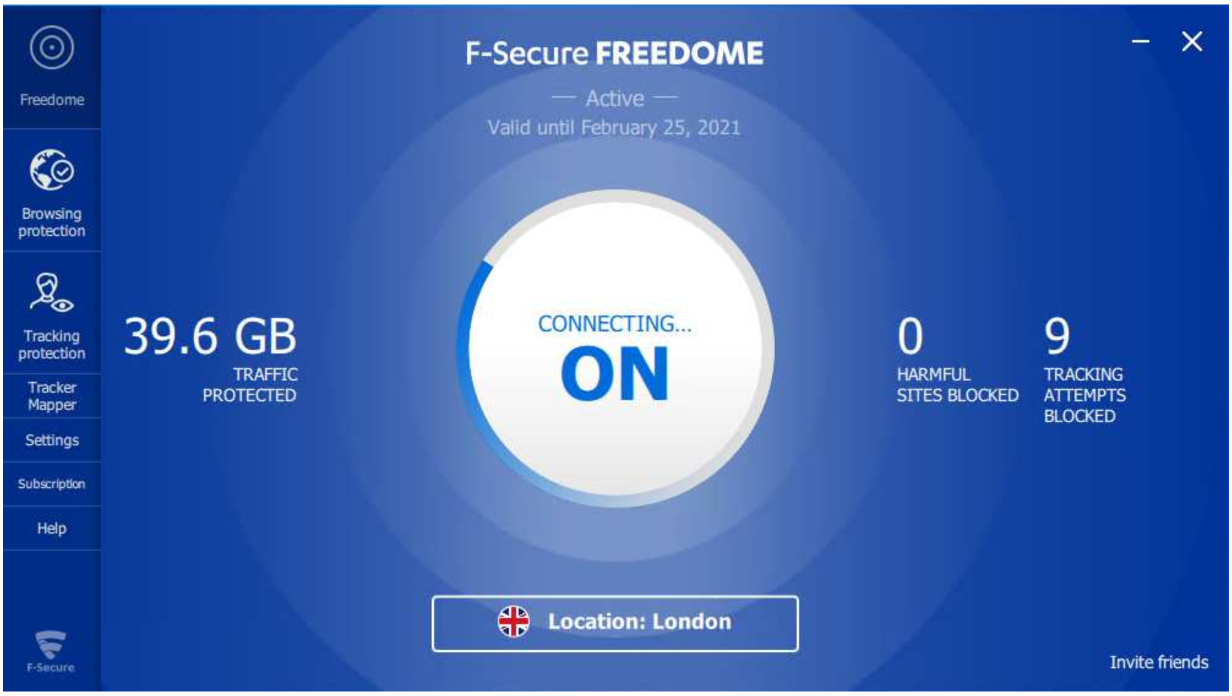
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very low latency
- No traffic logging

Cons

- No free trial
- Mediocre download speed
- Mediocre upload speed
- Minimal connection logging

F-Secure Freedome

F-Secure Corp.
Finland



At a glance

- F-Secure Freedome is a paid-for VPN product
- Website: https://www.f-secure.com/en/web/home_global/freedome
- Free trial: 30 days, plus 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 90
- Pricing DE: 5 devices / 1 year: EUR 80
- Common payment options: credit/debit card, PayPal, wire transfer, digital wallets
- A boxed version may be available, so the licence key will not be linked to your credit card or email
- Suitable for non-expert users
- Other features: Browsing Protection, Tracking Protection, Tracker Mapper

Summary

Installing and using F-Secure Freedome is as simple as it gets, making it a great choice for non-expert users. A range of pricing plans is available, whereby one can choose 3 or 7 devices, each with a 1-year or 2-year subscription. There's a choice of 23 different countries, including the USA and UK. Both a 30-day free trial and a 30-day money-back guarantee are available.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "very fast" and the latency as "low".

According to the company's privacy policy, connection logs (e.g. to monitor bandwidth usage) are created. Furthermore, the company claims to analyse the traffic for suspicious URLs and to (quoted verbatim) "*automatically screen the traffic to inhibit usage that is against our acceptable use policy*".

Ease of use

To set up F-Secure Freedome, you just need to download the installer file from the website, run it, and accept the licence agreement. The program window has a big *On/Off* button in the middle of the window, and below this is the Location button, which lets you choose your virtual location. Other features and options are found in a menu column on the left-hand side. The main options in the settings dialog are: automatically start Freedome with Windows; automatically turn on protection when Freedome starts; use automatic kill switch to cut off the Internet connection if the VPN connection is lost. F-Secure Freedome supports only the OpenVPN protocol.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Belgium, Canada (3), Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Ireland, Italy, Japan, Mexico, Netherlands, Norway, Poland, Singapore, Spain, Sweden, Switzerland, United Kingdom, USA (5).

Pros

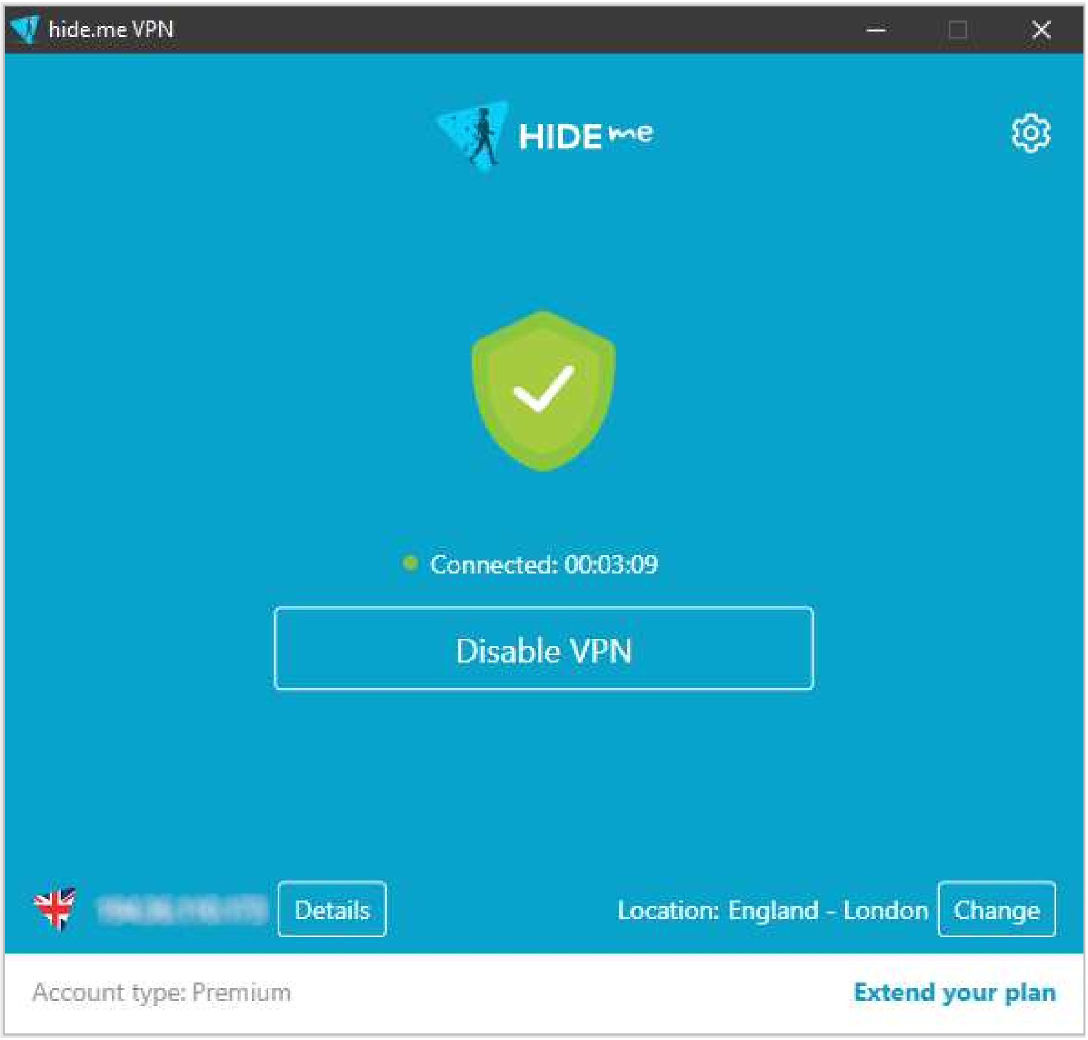
- 30-day free trial
- 30-day money-back guarantee
- Boxed version may be available
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very fast upload speed
- Low latency

Cons

- No choice of protocols
- Minimal traffic logging
- Connection logging

hide.me VPN

eVenture Ltd.
Malaysia



Connected: 00:03:09

[redacted]

Location: England - London

Account type: Premium

At a glance

- hide.me VPN is a paid-for VPN product (a restricted free version is also available)
- Website: https://hide.me
- The restricted free version is limited to fewer locations and 10 GB of data traffic per month
- 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 100
- Pricing DE: 5 devices / 1 year: EUR 100
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency
- Suitable for non-expert users

Summary

hide.me VPN is ideal for non-expert users, due to its ease of installation and operation. There are 38 different countries to choose from, UK and USA included. The pricing plans include 1-month, 1-year and 2-year subscriptions. You can try the program out using the free version, and a 30-day money-back guarantee is offered.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "very fast" and the latency as "low".

According to the company's privacy policy, hide.me VPN follows a no-logs policy. However, for technical reasons, the vendor does generate troubleshooting logs for each user, who are assigned a randomly generated username and internally assigned (non-public) IP address. This log keeps track of data usage and is deleted every few hours.

Ease of use

To set up hide.me VPN, download the installer from the vendor's website. There are no decisions to make, and setup completes very quickly with a couple of clicks. Once installed, the program is very simple to use. You just select a server by clicking the *Change* button, then click *Enable VPN*. The main configuration options in the settings dialog are: launch on system startup; connect on application start; auto-connect on secure Wi-Fi/insecure Wi-Fi/Ethernet connection; kill switch. hide.me VPN supports the protocols OpenVPN, IKEv2, SOCKS, and SSTP.

Server locations

At the time of testing, the product had servers in these countries: Australia (2), Austria, Belgium, Brazil, Bulgaria, Canada (2), Czech Republic, Denmark, France, Germany (4), Greece, Hong Kong (2), Hungary, Iceland, India, Ireland, Italy (2), Japan, Lithuania, Luxembourg, Mexico, Morocco, Netherlands (3), Norway, Poland, Romania, Serbia, Singapore (3), Slovakia, South Korea, Spain (2), Sweden, Switzerland, Turkey, United Arab Emirates, USA (13), Ukraine, United Kingdom (2).

Pros

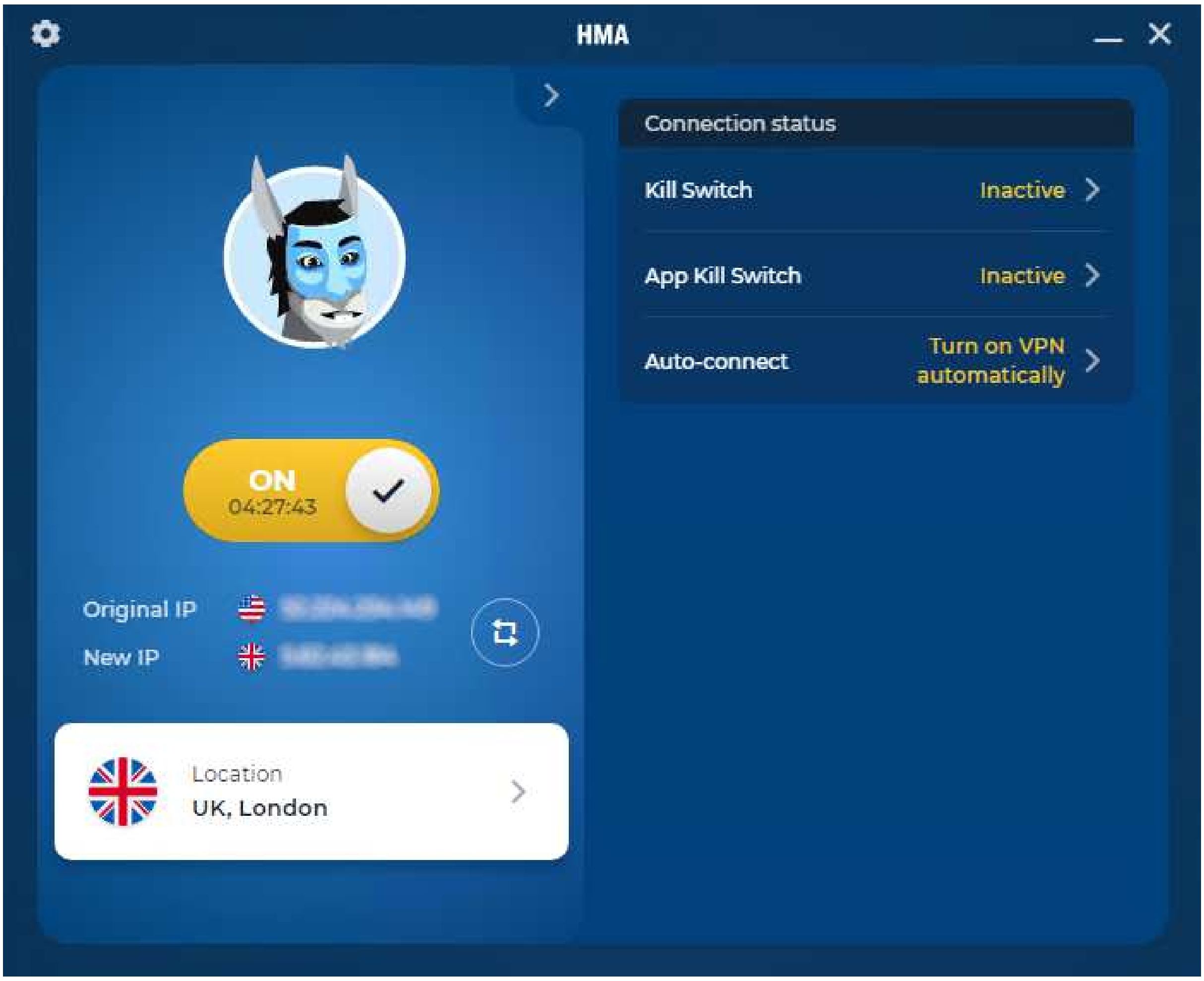
- Restricted free version
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very fast upload speed
- Low latency
- No traffic logging

Cons

- Minimal connection logging but this is deleted after a few hours

HMA VPN

Privax Ltd.
UK



HMA

Connection status

Kill Switch Inactive

App Kill Switch Inactive

Auto-connect Turn on VPN automatically

ON
04:27:43

Original IP [redacted]

New IP [redacted]

Location
UK, London

At a glance

- HMA VPN is a paid-for VPN product
- Website: https://www.hidemyass.com
- Free-trial: 7 days, 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 84
- Pricing DE: 5 devices / 1 year: EUR 72
- Common payment options: credit/debit card, PayPal
- Suitable for non-expert users

Summary

HMA VPN is fine for non-expert users, as it is very easy to install and use. The choice of countries is enormous, and appears to include every sovereign state in the world, plus some dependencies. The pricing plans include 1-month, 1-year and 3-years subscription. A money-back guarantee of 30 days is offered, and a 7-day free trial is available.

The program passed our Leak Test and Kill-Switch Test. We rated the download speed as “mediocre”, the upload speed as “very fast” and the latency as “very low”.

The company claims to follow a no-logs policy. It only collects some anonymised connection data.

Ease of use

To set up HMA VPN, just download the installer from the vendor’s website and run it. Installation is very quick and simple. The program is simple to use. You just need to click on the location button and click on the location you want; you will then be connected automatically. The creators evidently have a sense of humour. Status is shown not only by the slider button, but in a cartoon above. This shows a donkey (taking advantage of both meanings of “ass”) with a mask when the VPN is on, or with a worried expression when the VPN is off. Whether or not you like the humour, it’s quite an effective indicator of the VPN status. The main configuration options in the settings dialog are: start the program with Windows; system kill switch; app kill switch (prevents specific apps accessing the Internet when the VPN is not connected); IP shuffle (makes location tracking more difficult); exclude trusted LANs; use TCP only. HMA VPN supports the protocols OpenVPN, L2TP, and PPTP.

Server locations

HMA VPN claims to have over 290 virtual locations. At the time of testing, the list in the app appeared to cover not only every sovereign state in the world, including the Vatican, but also a number of other territories and dependencies such as Gibraltar and St Kitts & Nevis.

Pros

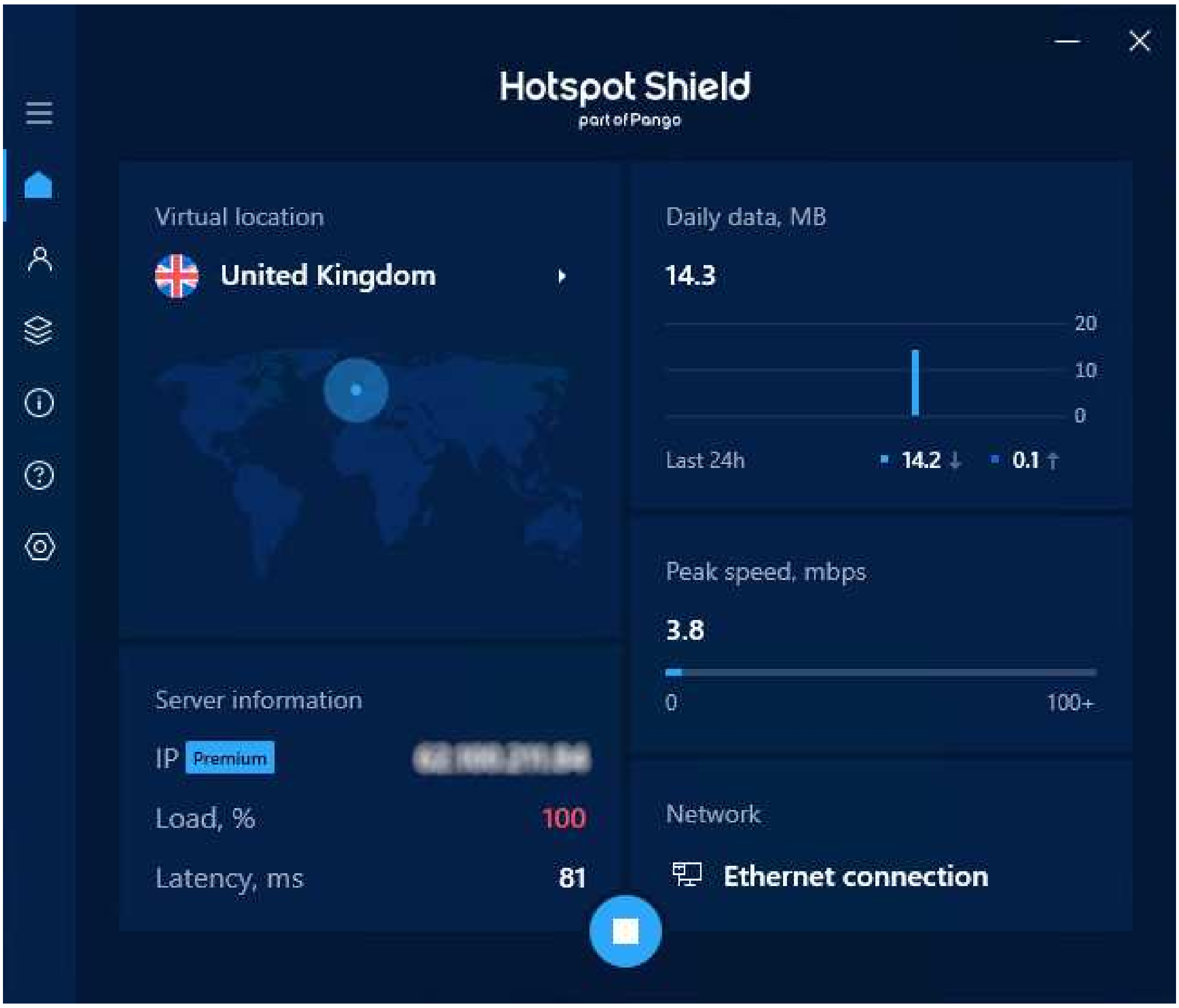
- 7-day free trial
- 30-day money-back guarantee
- Very simple to install and use
- Can start automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very fast upload speed
- Very low latency
- No traffic logging

Cons

- Mediocre download speed
- Minimal connection logging

Hotspot Shield

AnchorFree Inc.
USA



Virtual location
United Kingdom

Daily data, MB
14.3
Last 24h 14.2 ↓ 0.1 ↑

Peak speed, mbps
3.8

Server information
IP Premium [redacted]
Load, % 100
Latency, ms 81

Network
Ethernet connection

At a glance

- Hotspot Shield is a paid-for VPN product (a restricted free version is also available)
- Website: https://www.hotspotshield.com
- The restricted free version is limited to 1 US location, 500 MB data traffic per month, and has no streaming optimization or technical support
- 45-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 96
- Pricing DE: 5 devices / 1 year: EUR 96
- Common payment options: credit/debit card, PayPal
- Other features: malware and phishing protection

Summary

Hotspot Shield is easy to install and fairly straightforward to use. There is a choice of 80 different countries, including the United Kingdom and United States and both a 1-month and a 1-year plan are available. You can try the program out using the restricted free version and a 45-day money-back guarantee is offered.

It passed our Leak Test and Kill-Switch Test. We rated the download speed as “fast”, the upload speed as “fast” and the latency as “very low”.

The company claims it stores the duration of the VPN session, bandwidth usage and all accessed domains on an anonymised basis, in such a way as not to associate a user with a particular connection session.

Ease of use

To set up Hotspot Shield, download and run the installer from the vendor’s website. There are no decisions to make, and installation completes very quickly with a couple of clicks. The program is fairly straightforward to use. Initially, the interface only displays a “connect button”; clicking this connects to the default location. Once this connection has been established, a drop-down list of locations is shown, from which you can choose a different server. The main configuration options in the settings dialog are: run on Windows launch; prevent IP leak; kill switch; auto-connect when connecting to unsecured/secured Wi-Fi; user interface language. Hotspot Shield supports only its proprietary protocol Catapult Hydra.

Server locations

At the time of testing, the product had servers in these countries: United States (20), United Kingdom (2), Algeria, Argentina, Armenia, Australia (6), Austria, Azerbaijan, Bahamas, Belarus, Belgium, Belize, Bulgaria, Cambodia, Canada (4), Chile, China, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Ecuador, Egypt, Estonia, Finland, France (2), Georgia, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Isle of Man, Israel, Italy (3), Japan, Kazakhstan, Kyrgyzstan, Laos, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Moldova, Monaco, Montenegro, Nepal, Netherlands, New Zealand, Norway, Pakistan, Panama, Peru, Philippines, Poland, Portugal, Romania, Russia, Singapore, Slovakia, South Africa, South Korea, Spain (2), Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, Uruguay, Venezuela, Vietnam.

Pros

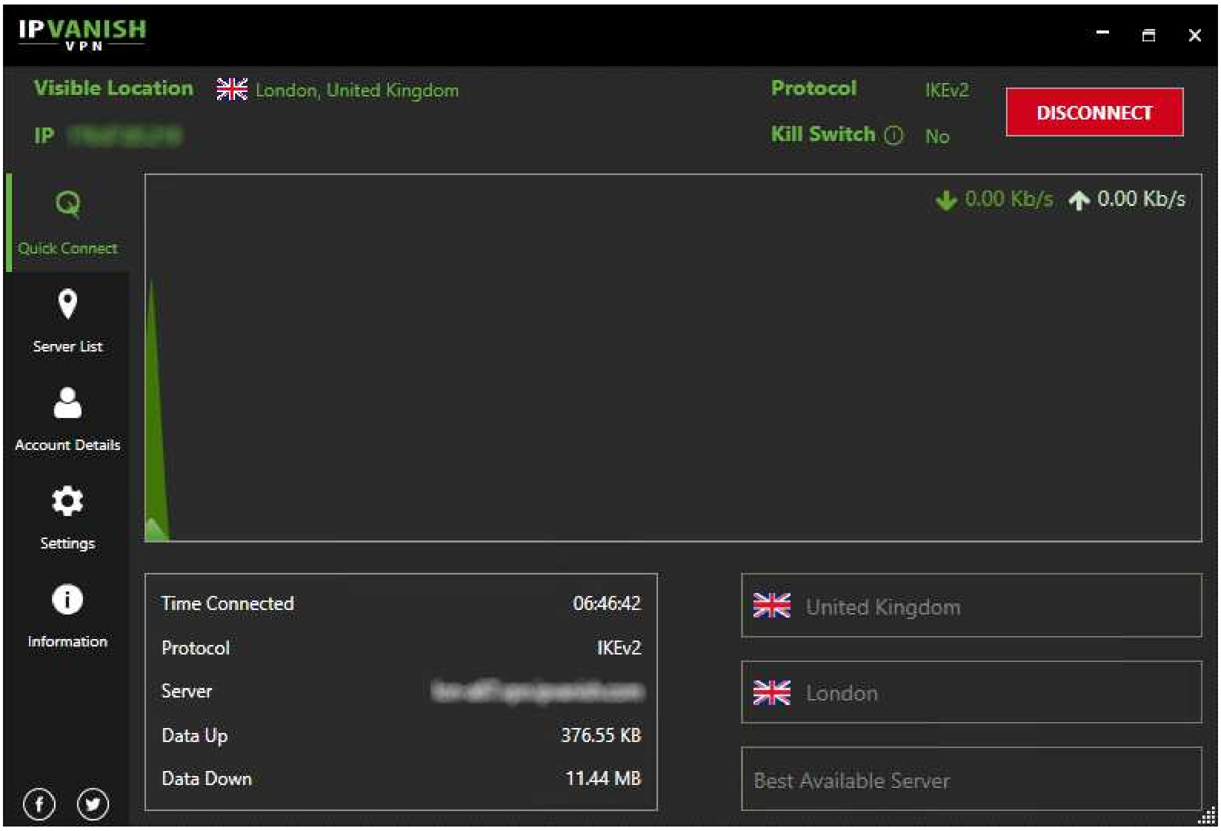
- Restricted free version
- 45-day money-back guarantee
- Very simple to install
- Can run automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download
- Fast upload speed
- Very low latency

Cons

- No choice of protocols
- Minimal traffic/connection logging

IPVanish

Mudhook Media Inc.
USA



Visible Location: London, United Kingdom
IP [redacted]
Protocol: IKEv2
Kill Switch: No

Time Connected	06:46:42
Protocol	IKEv2
Server	[redacted]
Data Up	376.55 KB
Data Down	11.44 MB

United Kingdom
London
Best Available Server

At a glance

- IPVanish is a paid-for VPN product
- Website: https://www.ipvanish.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 78
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal

Summary

IPVanish is simple to install, and fairly straightforward to use. There is a choice of 55 countries, most of which have a number of different servers – 100 for the UK, and 657 for the USA. The range of servers may be good for tech enthusiasts, but possibly bewildering for non-expert users. The pricing plans include 1-month, 3-month and 1-year subscriptions. A free trial is not available, but a 7-day money-back guarantee is provided.

The program passed our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "mediocre" and the latency as "low".

According to the company's privacy policy (quoted verbatim)"*IPVanish is a zero-logs VPN service provider, which means that we do not keep a record of any connection, traffic, or activity data in regards to our Services.*", although a more detailed description of what is logged would be welcome. Furthermore, this statement led to controversy in 2016, as an IPVanish user was accused of being in possession of child pornography. The company provided Homeland Security with data logs, including the originating IP address and connection timestamps of the user.

Ease of use

To set up IPVanish, download the installer from the vendor's website and run it. There are no options or decisions to make, and setup completes very quickly and easily. The program is straightforward to use. You need to choose a country, city and server from the respective drop-down lists, and click *Connect*. For each of the lists, the option "Best available" is provided. The main configuration options in the settings dialog are: auto reconnect if VPN disconnects; kill switch to cut Internet connection if VPN disconnects; start program with Windows; auto-connect on startup (various different options). IPVanish supports the protocols OpenVPN, IKEv2, L2TP, PPTP, SOCKS, and SSTP.

Server locations

At the time of testing, the product had servers in these countries: Albania (4), Argentina, Australia (67), Austria (6), Belgium (3), Brazil (19), Bulgaria (4), Canada (30), Chile, Columbia (4), Costa Rica, Croatia (4), Cyprus (2), Czech Republic (14), Denmark (12), Estonia (6), Finland (13), France (26), Germany (57), Greece (5), Hong Kong (19), Hungary (2), Iceland (2), India (6), Ireland (2), Israel (2), Italy (21), Japan (6), South Korea (2), Latvia (7), Luxembourg (2), Malaysia (2), Mexico (4), Moldova (2), Netherlands (98), New Zealand (3), Nigeria, Norway (2), Philippines (6), Poland (13), Portugal (11), Romania (2), Serbia (5), Singapore (18), Slovakia (3), Slovenia (2), South Africa (7), Spain (10), Sweden (14), Switzerland (9), Taiwan, Ukraine (7), United Arab Emirates, United Kingdom (100), United States (657).

Pros

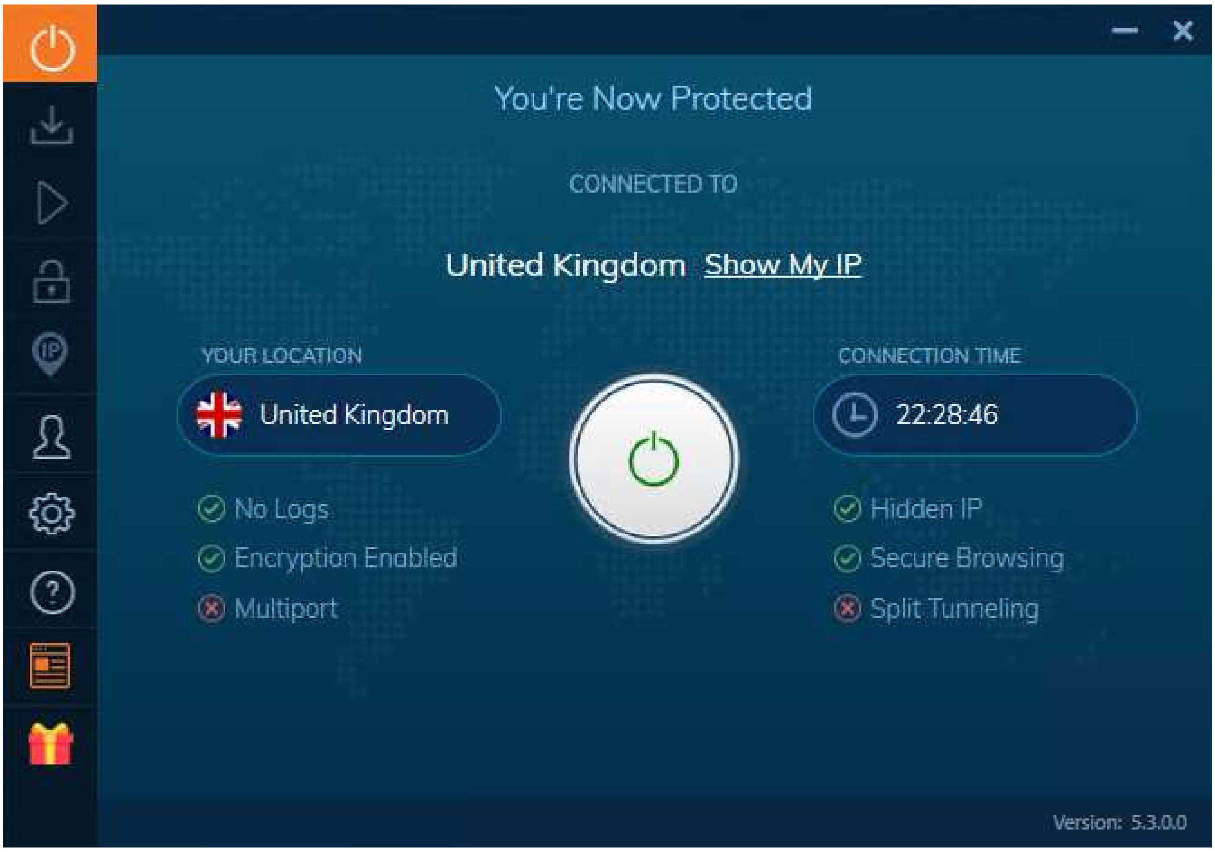
- 30-day money-back guarantee
- Very simple to install
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Low latency
- No traffic/connection logging

Cons

- No free trial
- Mediocre upload speed

Ivacy

PMG Pte. Ltd.
Singapore



You're Now Protected

CONNECTED TO

United Kingdom Show My IP

YOUR LOCATION: United Kingdom

CONNECTION TIME: 22:28:46

✓ No Logs
✓ Encryption Enabled
☒ Multiport

✓ Hidden IP
✓ Secure Browsing
☒ Split Tunneling

Version: 5.3.0.0

At a glance

- Ivacy is a paid-for VPN product
- Website: https://www.ivacy.com
- Free trial: 7 days, 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 42
- Pricing DE: 5 devices / 1 year: EUR 55
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Suitable for non-expert users

Summary

Ivacy is simple to install and use, and thus well suited to non-expert users. You can choose from 53 countries, including the UK and USA. The pricing plans include 1-month, 1-year and 2-year subscriptions. A 30-day money-back guarantee is provided and a 7-day free trial is available.

It passed both our Leak Test and Kill-Switch Test. We rated the download speed as "mediocre", the upload speed as "fast" and the latency as "low".

The company state in their privacy policy that they do not collect connection or traffic logs.

Ease of use

To set up Ivacy, download the installer from the vendor's website and run it. Installation is very quick and easy, and the program itself is very simple to use. You just select a location from the drop-down list, and click the "connect" button. The drop-down list can be set to show just the countries, or also the cities for countries that have multiple locations. The main configuration options in the settings dialog are: launch on system startup; auto connect after launch; DNS leak protection; kill switch. Ivacy supports the protocols OpenVPN, IKEv2, L2TP, PPTP, and SSTP.

Server locations

At the time of testing, the product had servers in these countries: Australia (4), Austria, Belgium, Brazil, Brunei, Bulgaria, Canada (3), China, Costa Rica, Czech Republic, Denmark, Egypt, Finland, France, Germany, Ghana, Hong Kong (2), India, Indonesia, Italy, Japan, Jordan, Kenya, South Korea, Kuwait, Latvia, Luxembourg, Malaysia (2), Mexico, Netherlands, New Zealand, Nigeria, Norway, Pakistan, Panama, Peru, Philippines, Poland, Romania, Russia, Saudi Arabia, Seychelles, Singapore, Spain, Sweden, Switzerland, Taiwan, Turkey, Ukraine, United Arab Emirates, United Kingdom (2), United States (12), Venezuela.

Pros

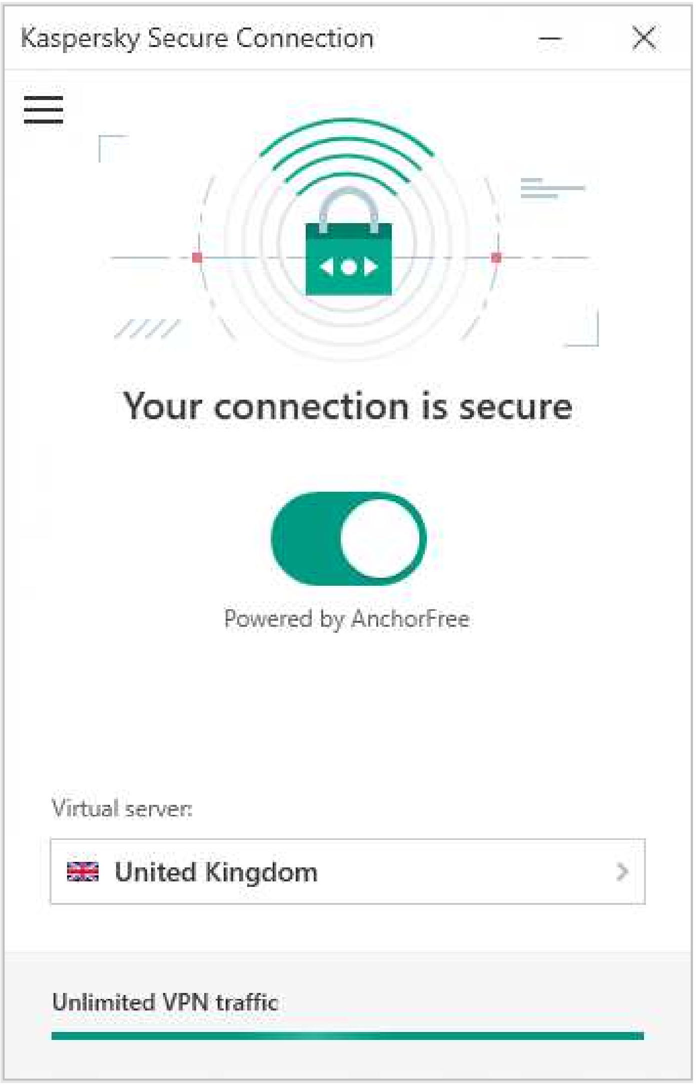
- 7-day free trial
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast upload speed
- Low latency
- No traffic/connection logging

Cons

- Mediocre download speed

Kaspersky Secure Connection

AO Kaspersky Lab
Russia



Kaspersky Secure Connection

Your connection is secure

Powered by AnchorFree

Virtual server:

United Kingdom

Unlimited VPN traffic

At a glance

- Kaspersky Secure Connection is a paid-for VPN product (a restricted free version is also available)
- Website: https://www.kaspersky.com/vpn-connection
- The restricted free version sets the location to automatic only, and is limited to 200 MB of data traffic per day
- 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 30
- Pricing DE: 5 devices / 1 year: EUR 30
- Common payment options: credit/debit card, PayPal, wire transfer
- Suitable for non-expert users

Summary

Kaspersky Secure Connection is very easy to set up and use, so ideal for non-expert users. There are 18 different countries to choose from, including the UK and USA, and only a 1-year plan is available. You can try the program out using the restricted free version, and a 30-day money-back guarantee is offered.

The program passed our Leak Test, but failed the Kill-Switch Test. We rated the download speed as “fast”, the upload speed as “mediocre” and the latency as “high”.

The vendor claims to follow a no-logs policy, however on the Kaspersky website, the vendor states (quoted verbatim) *“Kaspersky Lab is not a provider of VPN (Virtual Private Network) services. If access to specific websites or services is limited in the VPN service provider's region, you will not be able to access these websites and services through Kaspersky Secure Connection*.” On another website, the company claims (quoted verbatim) “*Servers encrypting and redirecting user traffic are located in different countries around the world, including the USA, Germany, Singapore and many others. They are provided by our partner, the software company AnchorFree, using their Hotspot Shield technology*.” Due to the nature of the two statements, we are not quite sure whether the logging policy of Anchorfree also applies in this scenario, which would imply that traffic logs are gathered on an anonymized basis.

Ease of use

To set up Kaspersky Secure Connection, download the installer from the vendor’s website and run it. Setup is quick and easy. The user interface is very simple and easy to use. There is a drop-down list of servers to connect to, and an on-off slider switch. The main configuration options in the settings dialog are: start program with Windows; automatically connect on program start; activate VPN automatically when connecting to unsecure Wi-Fi, or prompt to do this; specify Wi-Fi networks to be treated as insecure. There is no kill switch. Kaspersky Secure Connection supports the protocols OpenVPN, IKEv2, L2TP, PPTP, and Hotspot Shield's Catapult Hydra.

Server locations

At the time of testing, the product had servers in these countries: Canada, Czech Republic, Denmark, France, Germany, Hong Kong, Japan, Mexico, Netherlands, Ireland, Russia, Singapore, Spain, Sweden, Turkey, Ukraine, United Kingdom, United States

Pros

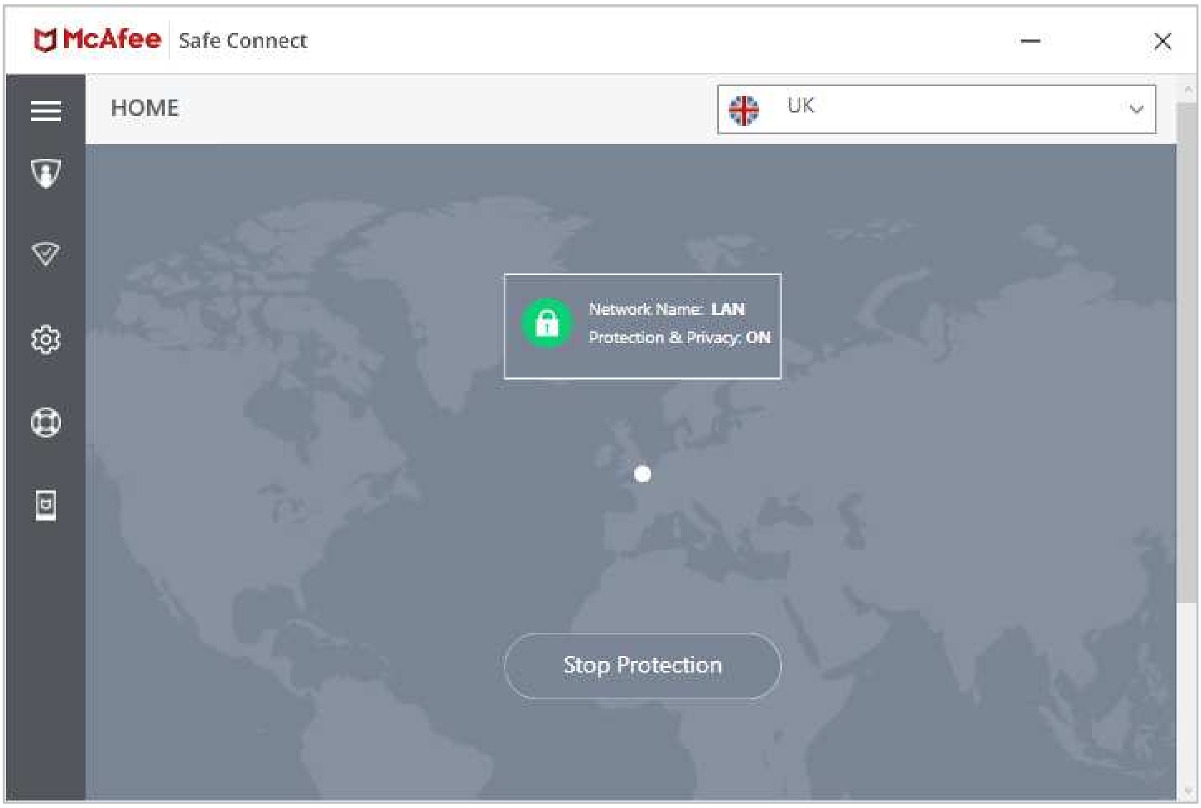
- Restricted free version
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Fast download speed

Cons

- Kill-Switch Test failed
- Mediocre upload speed
- High Latency
- Unclear privacy policy

McAfee Safe Connect

McAfee LLC
USA



At a glance

- McAfee Safe Connect is a paid-for VPN product (a restricted free version is also available)
- Website: https://www.mcafee.com/en-us/vpn/mcafee-safe-connect.html
- The restricted free version is limited to 250 MB of data traffic per month
- 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 48
- Pricing DE: 5 devices / 1 year: EUR 48
- Common payment options: credit/debit card, PayPal, wire transfer, digital wallets
- A boxed version may be available, so the licence key will not be linked to your credit card or email
- Suitable for non-expert users

Summary

McAfee Safe Connect is simple to install and use, so well suited to non-expert users. There is a choice of 22 countries, including the UK and USA and both a 1-month and a 1-year plan are available. You can try the program out using the restricted free version, and a 30-day money-back guarantee is offered for the paid version.

The program passed our Leak Test, but failed the Kill-Switch Test. We rated the download speed as "fast", the upload speed as "very fast" and the latency as "low".

We could not find any VPN-specific privacy policy, but McAfee's general privacy policy.

Ease of use

To set up McAfee Safe Connect, download the installer from the vendor's website and run it. Installation is very simple, and completes in a couple of clicks. A Windows UAC prompt appears when you start the program. The product is very simple to use; just select a location from the drop-down list on the home page, and click *Start Protection*. The only configuration options in the settings dialog are: connect manually/automatically on Wi-Fi and LAN/automatically on Wi-Fi only; add trusted network. There is no kill switch. McAfee Safe Connect supports only the OpenVPN protocol.

Server locations

At the time of testing, the product had servers in these countries: Australia, Brazil, Canada, Switzerland, Germany, Denmark, Spain, France, UK, Hong Kong, Ireland, India, Italy, Japan, Mexico, Netherlands, Norway, New Zealand, Romania, Sweden, Singapore, USA.

Pros

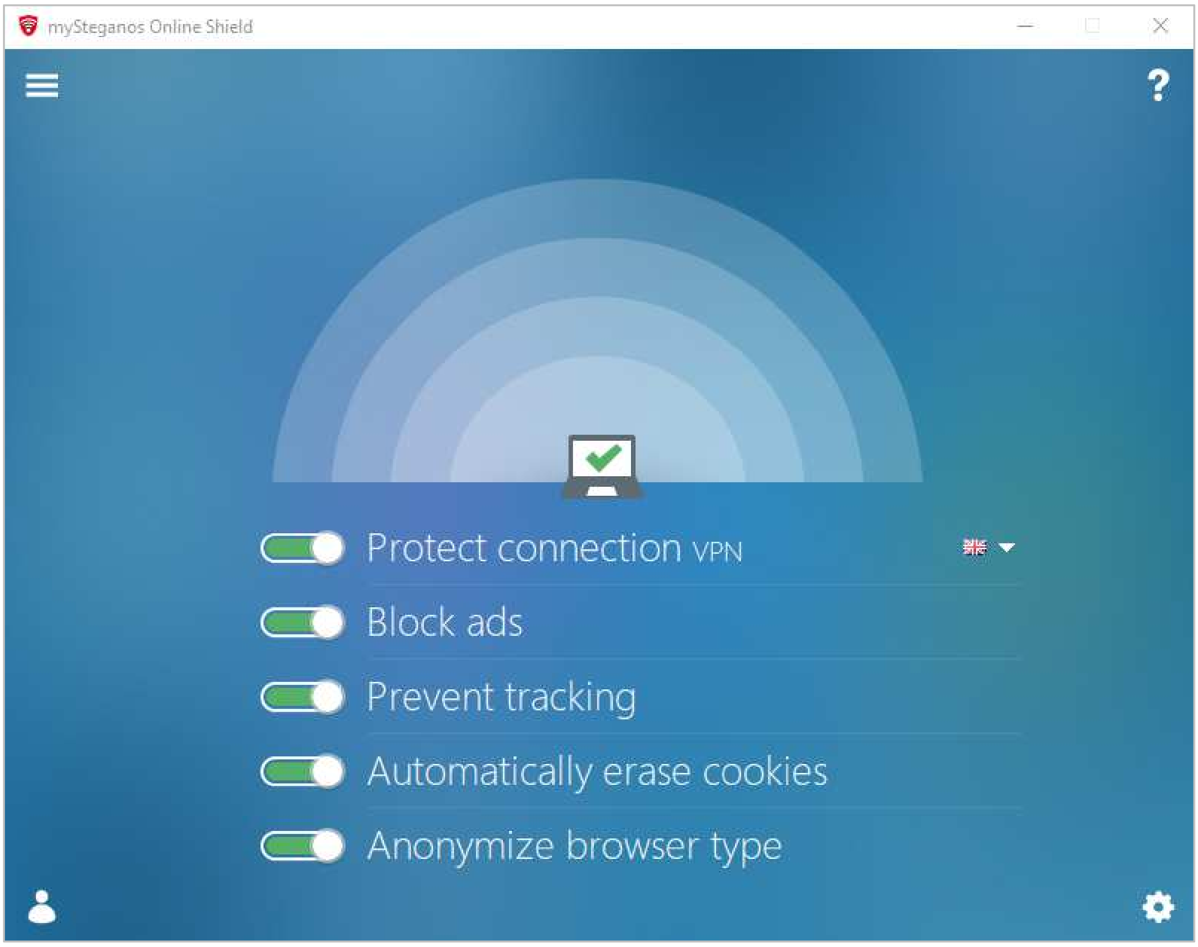
- Restricted free version
- 30-day money-back guarantee
- Boxed version may be available
- Very simple to install and use
- Can connect automatically
- Leak Test passed
- Fast download speed
- Very fast upload speed
- Low latency

Cons

- No choice of protocols
- Kill-Switch Test failed
- Unclear privacy policy

mySteganos Online Shield VPN

Steganos Software GmbH
Germany



mySteganos Online Shield

Protect connection VPN

Block ads

Prevent tracking

Automatically erase cookies

Anonymize browser type

At a glance

- mySteganos Online Shield VPN is a paid-for VPN product
- Website: https://www.steganos.com/en/products/mysteganos-online-shield-vpn
- Free trial: 7 days, 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 50
- Pricing DE: 5 devices / 1 year: EUR 50
- Common payment options: credit/debit card, PayPal, wire transfer
- Suitable for non-expert users
- Other features: ad blocker, tracking prevention, automatic cookie erase, anonymize browser type

Summary

mySteganos Online Shield VPN is suitable for non-expert users, as it is simple to install and use. There is a choice of 23 country locations, including the USA and UK. The pricing plans include 1-month, 6-month and 1-year subscriptions. There is a 7-day free trial ,along with a 30-day money-back guarantee.

The program passed our Leak Test and Kill-Switch Test, but provided only a slow download speed. We rated the download speed as “slow”, the upload speed as “fast” and the latency as “mediocre”.

The company claims in its privacy policy not to store any traffic logs or the user’s originating or VPN-assigned IP addresses. They also mention that they monitor the bandwidth usage of each user, using a pseudonym rather than the real username. However, they do not mention any other connection-log features such as connection timestamps, or whether relevant location information is collected.

Ease of use

To install mySteganos Online Shield VPN, just download the installer from the vendor’s website and run it. In our functionality test, a Windows SmartScreen prompt appeared, meaning that we had to click the *More info/Run anyway* options. Once the setup wizard starts, there is no further action required, and after a few seconds the program starts. The VPN component is very simple to use. You just select your chosen location by clicking on the flag icon on the right of the *Protect connection* button, and then set the slider switch to the “On” position. The main configuration options in the settings dialog are: interface language, start program automatically at logon, and automatically connect the VPN when the program starts. There is a kill switch for unsecured connections. mySteganos Online Shield VPN supports the protocols OpenVPN and IKEv2.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Brazil, Canada, Denmark, Finland, France, Germany, Great Britain*, India, Italy, Japan, Netherlands, Norway, Poland, Romania, Russia, Singapore, Spain, Sweden, Switzerland, Turkey, USA.
*This should read “United Kingdom”. After connecting to the “Great Britain” server, our test system was assigned an IP address in Belfast, Northern Ireland (in the UK but not in Great Britain).

Pros

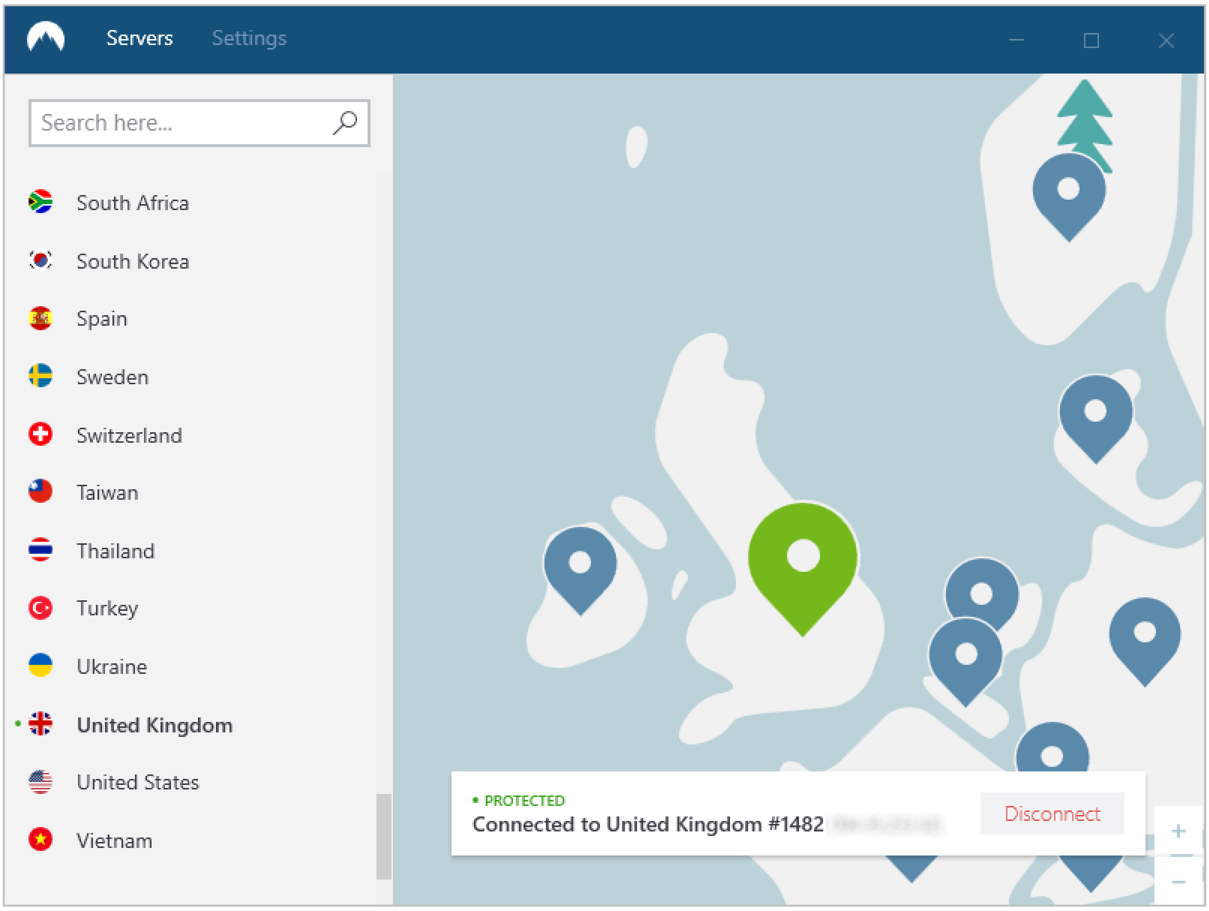
- 7-day free trial
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast upload speed
- No traffic logging

Cons

- Slow download speed
- Mediocre latency
- Minimal connection logging

Nord VPN

Tefincom & Co. S.A.
Panama



• PROTECTED
Connected to United Kingdom #1482 [redacted]

At a glance

- Nord VPN is a paid-for VPN product
- Website: https://nordvpn.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 84
- Pricing DE: 5 devices / 1 year: EUR 89
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Suitable for non-expert users
- Other features: “protection against intrusive advertisements, malware, phishing attempts and other threats”

Summary

Nord VPN is suited to non-expert users, as it is easy to install and use. 58 different country locations are provided, including the USA and UK. The pricing plans include 1-month, 1-year, 2-year and 3-year subscriptions, and a 30-day money-back guarantee is provided, although no free trial is available.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "very fast" and the latency as "very low".

According to the company's privacy policy, they follow a no-logs policy.

Ease of use

To set up Nord VPN, log into your account, download the installer and run it. Setup completes very easily with a couple of clicks. The program is very easy to use. You just need to click on a country from the list on the left-hand side of the window, and you will be connected to that location. You can choose a specific server by clicking on the "…" menu at the end of the country's name, and selecting a server from the drop-down list shown. The main configuration options in the settings dialog are: start program with Windows, connect automatically on program start, kill switch, make computer invisible in its LAN. Nord VPN supports the protocols OpenVPN, IKEv2, and SOCKS.

Server locations

At the time of testing, the product had servers in these countries: Albania, Argentina, Australia, Austria, Belgium, Bosnia & Herzegovina, Brazil, Bulgaria, Canada, Chile, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Latvia, Luxembourg, Malaysia, Mexico, Moldova, Netherlands, New Zealand, North Macedonia, Norway, Poland, Portugal, Romania, Serbia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Kingdom, United States, Vietnam.

Pros

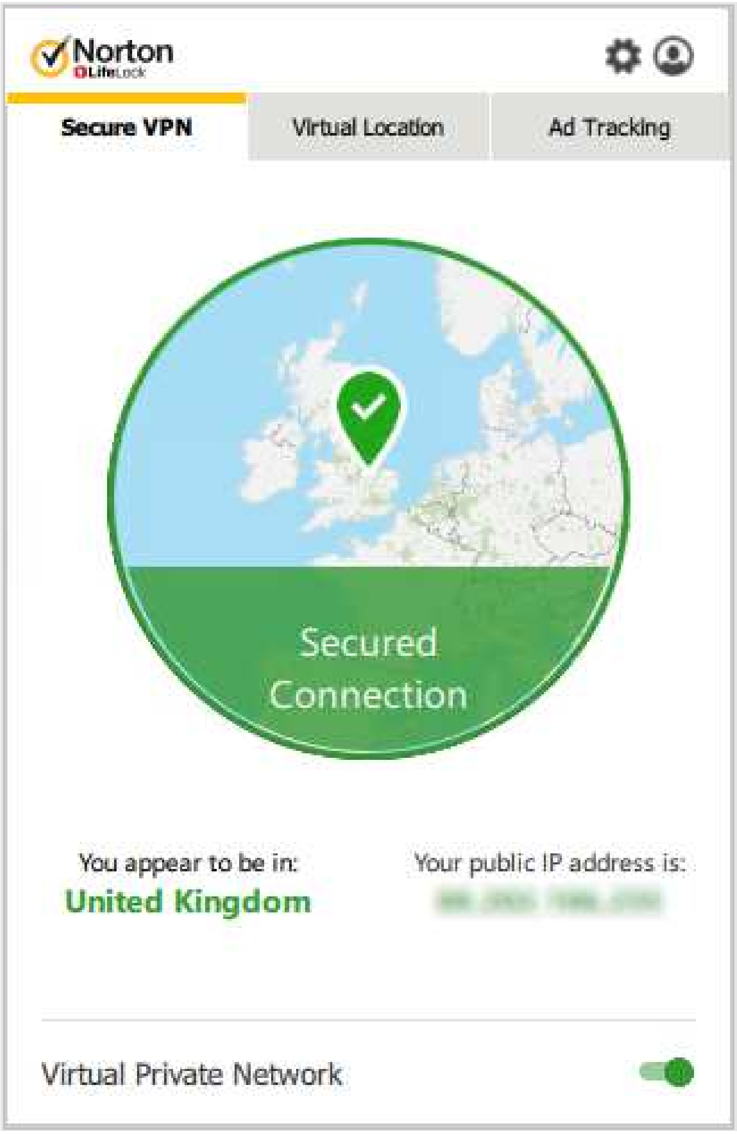
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very fast upload speed
- Very low latency
- No traffic/connection logging

Cons

- No free trial

Norton Secure VPN

NortonLifeLock Inc.
USA



You appear to be in: United Kingdom

Your public IP address is:

Virtual Private Network

At a glance

- Norton Secure VPN is a paid-for VPN product
- Website: https://norton.com/wifi-privacy
- Free trial: none, but there is a 60-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 100
- Pricing DE: 5 devices / 1 year: EUR 70
- Common payment options: credit/debit card, PayPal, wire transfer
- Suitable for non-expert users
- Other features: Tracker blocking

Summary

Norton Secure VPN is easy to set up and use, so ideal for non-expert users. You can choose from 31 country locations, including the UK and USA. A range of pricing plans is available, whereby one can choose 1, 5 or 10 devices for a monthly or yearly subscription. Although no free trial is available, a 60-day money-back guarantee is provided.

The program passed our Leak Test but failed the Kill-Switch Test. We rated the download speed as “fast”, the upload speed as “very fast” and the latency as “low”.

On the main website, when looking for the privacy policy, one is redirected to the Broadcom privacy policy, which leaves a potential buyer rather confused, as it is not explained to what degree the two companies are related. Another privacy policy hosted on the Norton website claims that the product does not generate any traffic logs. However, they state that they collect for each user bandwidth usage, IP Address and device ID serial number using a pseudonym rather than the real username.

Ease of use

To set up Norton Secure VPN, download and run the installer from the vendor’s website. There are no decisions to make, and setup completes very quickly and easily. The product is very simple to use. On the *Virtual Location* tab, select a country from the list; then on the *Secure VPN* tab, set the *Virtual Private Network* switch to “On”. The main configuration options in the settings dialog are: launch at startup; auto-connect. There is no kill switch. Norton Secure VPN supports only the OpenVPN protocol.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Belgium, Brazil, Canada, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, India, Ireland, Israel, Italy, Japan, Mexico, Netherlands, New Zealand, Norway, Poland, Romania, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, United States.

Pros

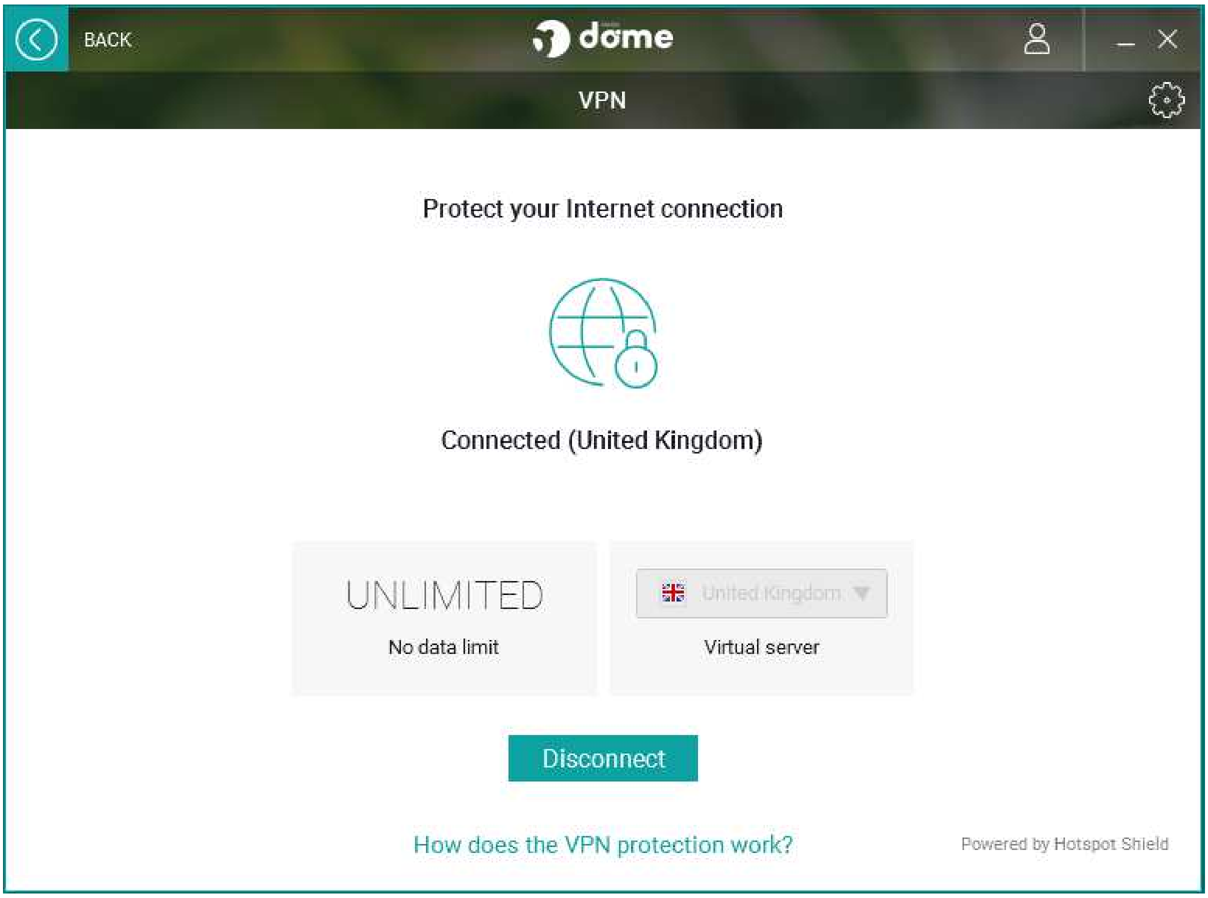
- 60-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- No traffic logging
- Leak Test passed
- Fast download speed
- Very fast upload speed
- Low latency
- Can connect automatically when PC starts
- Leak Test passed
- No traffic logging

Cons

- No free trial
- Kill-Switch Test failed
- Minimal connection logging

Panda Dome VPN

Panda Security S.L.
Spain



BACK
dome
VPN
Protect your Internet connection
Connected (United Kingdom)
UNLIMITED
No data limit
United Kingdom
Virtual server
Disconnect
How does the VPN protection work?
Powered by Hotspot Shield

At a glance

- Panda Dome VPN is a paid-for VPN product (a restricted free version is also available)
- Website: https://www.pandasecurity.com/en/homeusers/solutions/vpn/
- The restricted free version sets the location to automatic only, and is limited to 150 MB of data traffic per day
- 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 77
- Pricing DE: 5 devices / 1 year: EUR 62
- Common payment options: credit/debit card, PayPal
- May prove confusing for non-expert users, as it turns out to be part of a full security suite
- Other features: full antivirus program

Summary

Panda Dome VPN is in itself simple to set up and use, but may surprise and confuse many users by installing an unadvertised antivirus program along with the VPN. There is a choice of 23 country locations, including the USA and UK. The pricing plans include 1-month, 1-year and 3-year subscriptions. You can try the product out by using the restricted free version, and there is a 30-day money-back guarantee.

The program failed both our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "fast" and the latency as "very low".

We were not able to find a specific VPN privacy policy for the product, hence we refer to the product's general privacy policy. However we were not able to extract any relevant information, although on the support website the vendor claims not to store any identifiable personal information. The fact that Panda Dome VPN is powered by Hotspot Shield leaves a potential user wondering whether the Anchorfree logging policy applies in this scenario.

Ease of use

Setting up Panda Dome VPN is very simple. However, after installing the program, we were surprised to discover that the product we had purchased was in fact a security suite (Panda Dome), with a full antivirus program included. There is no indication of this on the Panda website, or even in the setup wizard (which offers no choice of components to install). This could be confusing for non-expert users who already had a third-party antivirus solution installed. It is possible to disable the antivirus component and use Windows Defender or a third-party antivirus program, but every time you open the Panda program to use the VPN, you will see a warning stating that the computer is not protected. The VPN component of the program is very easy to use, once you realise that it is part of a security suite. On the program's home page, click on the VPN icon; then on the VPN page, select the virtual location you want from the drop-down list, and click *Connect*. The only configuration options in the VPN settings dialog are whether to connect the VPN at Windows logon, and if so, which location to use. There is no kill switch. Panda Dome VPN supports only Hotspot Shield's Catapult Hydra protocol.

Server locations

At the time of testing, the product had servers in these countries: Norway, Germany, Hong Kong, Russia, India, Japan, Denmark, Mexico, Italy, France, Ukraine, Spain, Brazil, Sweden, Singapore, Australia, Czech Republic, United Kingdom, Ireland, Turkey, Canada, USA, Netherlands.

Pros

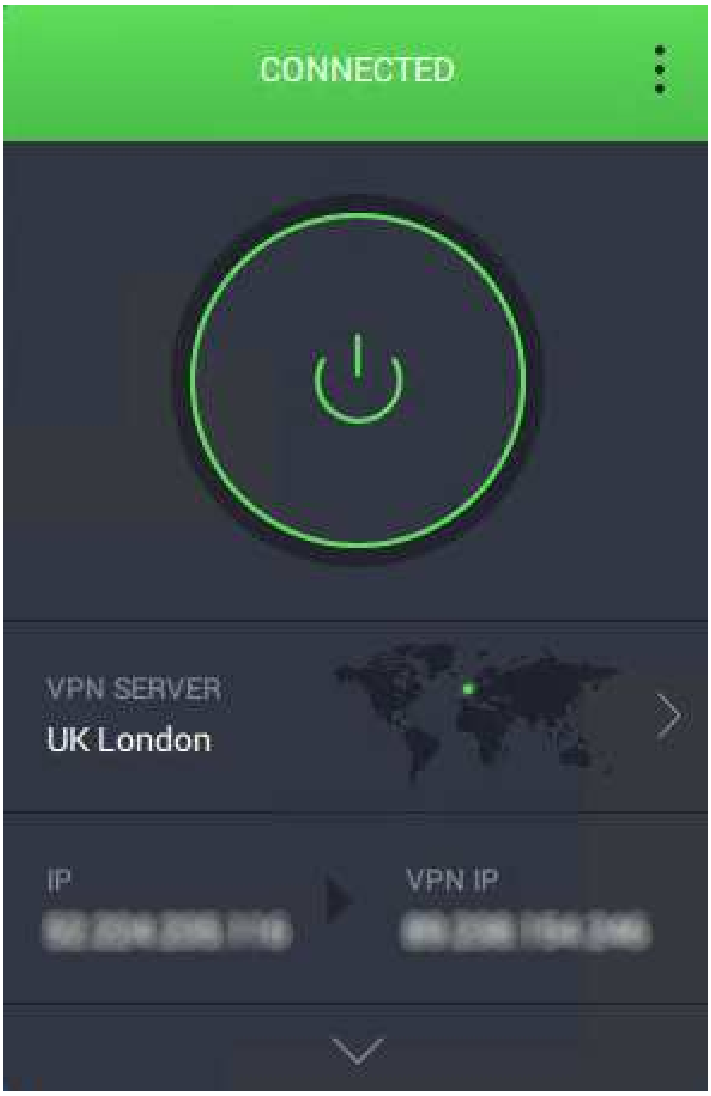
- Restricted free version
- 30-day money-back guarantee
- Simple to install
- Easy to use once you locate the VPN function
- Can connect automatically when PC starts
- Fast download speed
- Fast upload speed
- Very low latency

Cons

- Confusing if you already have AV installed
- No choice of protocols
- Leak Test failed
- Kill-Switch Test failed
- Unclear privacy policy

Private Internet Access

Private Internet Access Inc.
USA



CONNECTED

VPN SERVER
UK London

IP
[redacted]

VPN IP
[redacted]

At a glance

- Private Internet Access is a paid-for VPN product
- Website: https://www.privateinternetaccess.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 40
- Pricing DE: 5 devices / 1 year: EUR 37
- Common payment options: credit/debit card, PayPal, cryptocurrency, digital wallets
- Suitable for non-expert users
- Other features: Block domains used for trackers, advertisements, and malware

Summary

Private Internet Access is easy to set up and use, making it a good choice for non-expert users. 33 country locations are provided, including the USA and UK. The pricing plans include 1-month, 6-months and 1-year subscriptions. Although no free trial is provided, there is a 30-day money-back guarantee.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "mediocre", the upload speed as "very fast" and the latency as "very low".

The company's privacy policy states (quoted verbatim) "*The data controller does not collect or log any traffic or use of its Virtual Private Network ("VPN") or Proxy*". When required to provide information to the FBI as part of a court case, the company stated that it does not log user activity and so was unable to provide any such evidence.

Ease of use

To set up Private Internet Access, download and run the installer from the vendor's website. Once you have double-clicked it, there is nothing else to do – the installer runs, without any further interaction being required. The wizard does not put a shortcut on the Windows Desktop; you have to find it yourself in the Start Menu. The program is simple to use. Just click on the *VPN Server* button to choose a location, then click the "connect" button. The main configuration options in the settings dialog are: autostart program with Windows; connect on program startup; kill switch; UDP/TCP; encryption type (AES-128 GCM, AES-128 CBC, AES-256 GCM, AES-256 CBC); static IP address. Private Internet Access supports the protocols OpenVPN, L2TP, PPTP, SOCKS, and WireGuard.

Server locations

At the time of testing, the product had servers in these countries: Albania, Ireland, Luxembourg, France, United Kingdom (3), Netherlands, Switzerland, Czech Republic, Denmark, Spain, Germany (2), Finland, Belgium, Poland, Italy, Norway, United States (14), Romania, Austria, Sweden, Hungary, Israel, United Arab Emirates, Canada (3), Mexico, India, Singapore, Brazil, South Africa, Hong Kong, Japan, Australia (3), New Zealand.

Pros

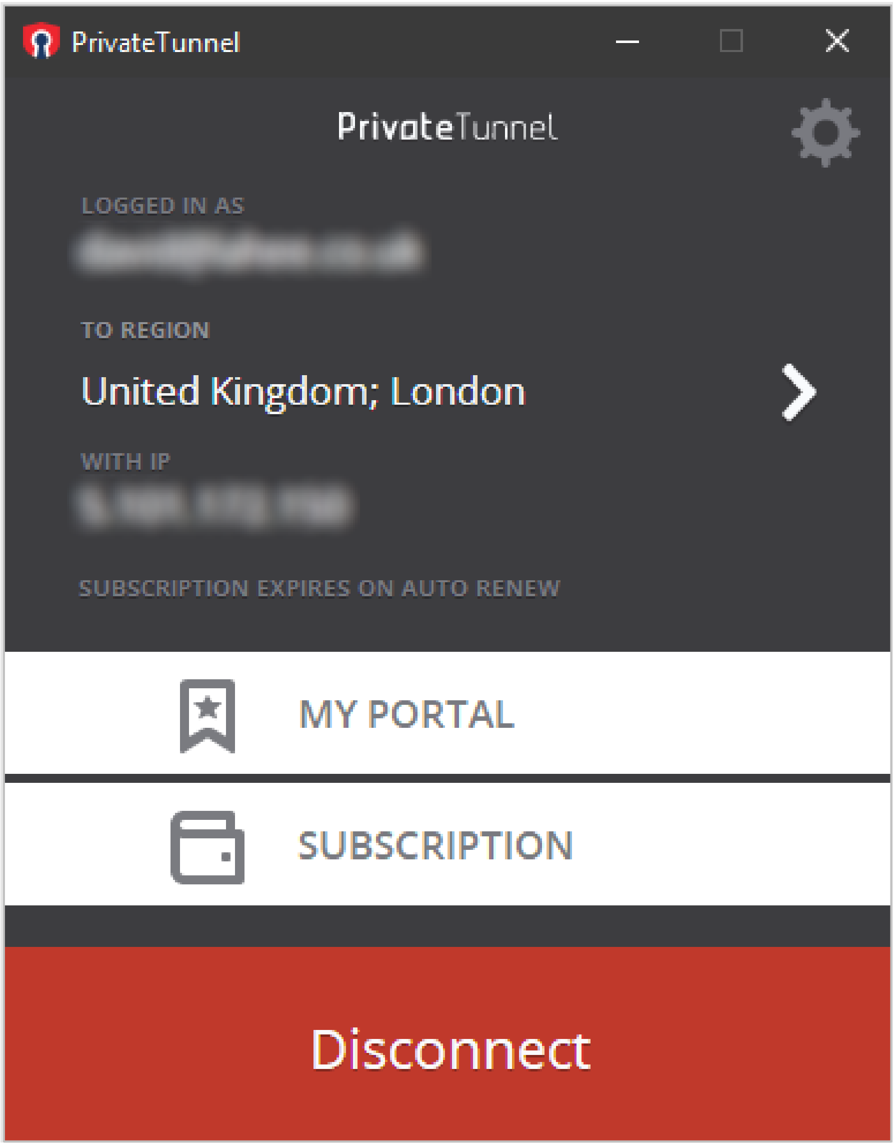
- 30-day money-back guarantee
- Simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very fast upload speed
- Very low latency
- No traffic/connection logging

Cons

- No free trial
- Mediocre download speed

Private Tunnel

OpenVPN Technologies Inc.
USA



LOGGED IN AS
[redacted]

TO REGION
United Kingdom; London

WITH IP
[redacted]

SUBSCRIPTION EXPIRES ON AUTO RENEW

At a glance

- Private Tunnel is a paid-for VPN product
- Website: https://www.privatetunnel.com
- Free trial: 7 days, 60-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 48
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal, digital wallets
- Suitable for non-expert users

Summary

Private Tunnel is simple to set up and use, so well suited to non-expert users. There is a choice of 12 country locations, including the UK and USA. A wide range of pricing plans is available, including one for hundreds of devices. A 7-day free trial and a 60-day money-back guarantee are provided.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "mediocre", the upload speed as "very fast" and the latency as "low".

The company's privacy policy states that it does not gather any traffic logs, whereby connection logs such as connection timestamps, bandwidth usage, both VPN-assigned IP address and user's originating IP address are stored.

Ease of use

To set up Private Tunnel, download the installer from the vendor's website and run it. Setup completes very quickly and easily. You have to sign in with your user account when the program first starts. The program is very simple to use. You just need to click on the server list and select your desired virtual location, and then click *Connect*. The main configuration options in the settings dialog are: Auto Start; protocol (Adaptive; UDP; TCP; HTTP Proxy; OBFS Proxy; OBFS-Hybrid Proxy); Connection Timeout. The kill-switch functionality is built into the product but not visible to the user. Private Tunnel supports only the OpenVPN protocol.

Server locations

At the time of testing, the product had servers in these countries: United Kingdom; Canada; Switzerland; Germany; Spain; France; Hong Kong; Italy; Japan; Netherlands; Sweden; United States (12).

Pros

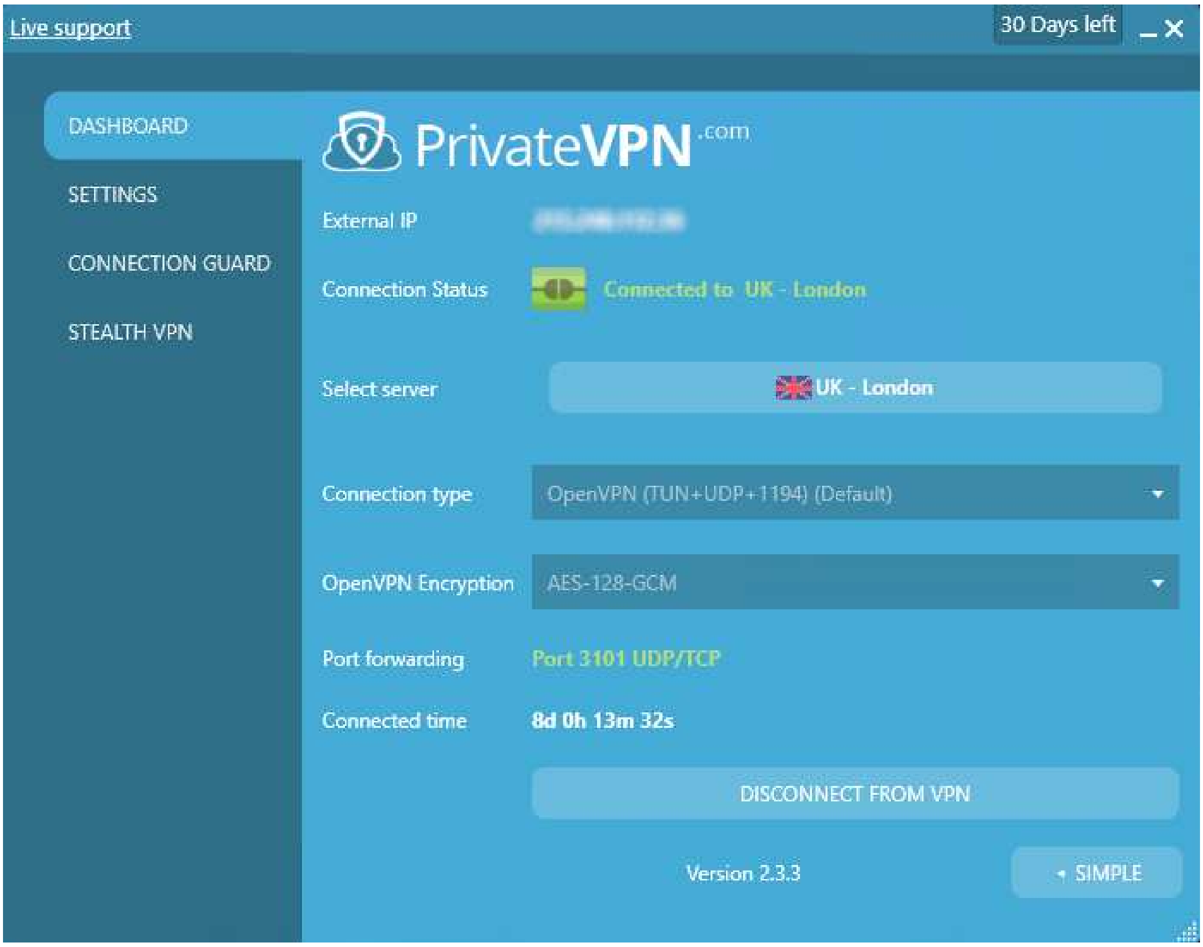
- 7-day free trial
- 60-day money-back guarantee
- Very simple to install and use
- Can start automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very fast upload speed
- Low latency
- No traffic logging

Cons

- No choice of protocols
- Mediocre download speed
- Connection logging

PrivateVPN

Privat Kommunikation Sverige AB
Sweden



External IP [redacted]

Connection Status Connected to UK - London

Select server UK - London

Connection type OpenVPN (TUN+UDP+1194) (Default)

OpenVPN Encryption AES-128-GCM

Port forwarding Port 3101 UDP/TCP

Connected time 8d 0h 13m 32s

Version 2.3.3

At a glance

- PrivateVPN is a paid-for VPN product
- Website: https://privatevpn.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 50
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal, cryptocurrency
- Suitable for non-expert users

Summary

PrivateVPN is simple to install and use, thus making it ideal for non-expert users. 62 country locations are provided, including the UK and USA. The pricing plans include 1-month, 3-month, and 1-year subscriptions. Although there is no free trial, a 30-day money-back guarantee is provided.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "very fast" and the latency as "very low".

According to the vendor's privacy policy, the company claims (quoted verbatim) "*PrivateVPN does not collect or log any traffic or use of its service*", although a more detailed description would be welcome.

Ease of use

To set up PrivateVPN, download the installer from the vendor's website and run it. Installation is very simple and completes with a couple of clicks. You need to restart the computer afterwards, and sign in with your account credentials before using the program. PrivateVPN is very simple to use. You just choose a server using the *Choose Location* button, and then click *Connect*. Clicking the *Advanced* button displays additional functions, such as encryption options, on the home page. The main configuration options in the settings dialog are: start program with Windows; connect automatically on program startup; reconnect automatically on connection failure; DNS leak protection; kill switch. PrivateVPN supports the protocols OpenVPN, IKEv2, L2TP, PPTP, and SOCKS.

Server locations

At the time of testing, the product had servers in these countries: Argentina, Australia (2), Austria, Belgium, Brazil, Bulgaria, Canada (3), Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Finland, France, Germany (2), Greece, Hong Kong, Hungary, Iceland, India (3), Indonesia, Ireland, Isle of Man, Israel, Italy (2), Japan, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Moldova, Netherlands, New Zealand, Norway, Panama, Peru, Philippines, Poland, Portugal, Romania, Russia (3), Serbia, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden (3), Switzerland, Taiwan, Thailand, Turkey, United Kingdom (2), Ukraine, United Arab Emirates, United States (11), Vietnam. There is an additional list of servers that are optimised for streaming services, such as Netflix and BBC iPlayer.

Pros

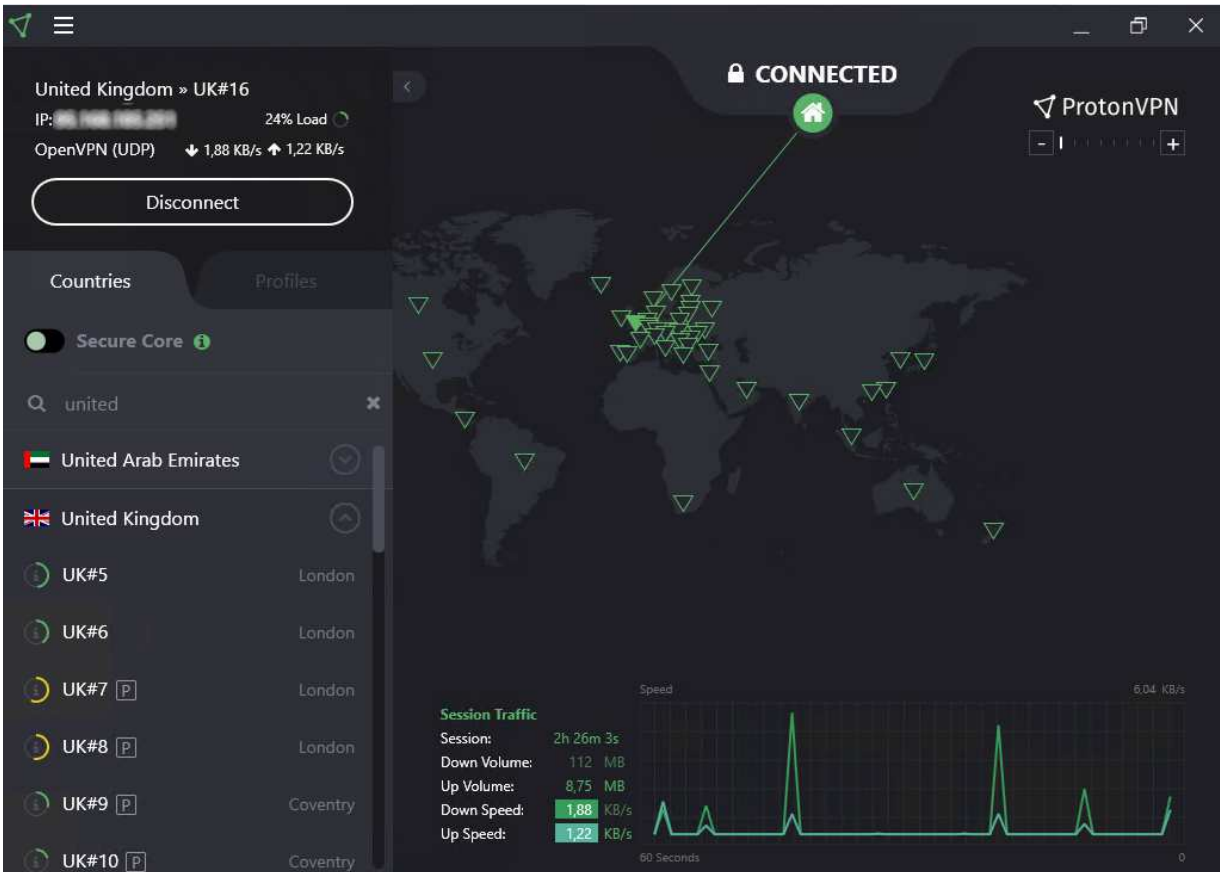
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very fast upload speed
- Very low latency
- No traffic/connection logging

Cons

- No free trial

ProtonVPN

Proton Technologies AG
Switzerland



United Kingdom » UK#16
IP: [redacted] 24% Load
OpenVPN (UDP) ↓ 1,88 KB/s ↑ 1,22 KB/s

Session Traffic
Session: 2h 26m 3s
Down Volume: 112 MB
Up Volume: 8,75 MB
Down Speed: 1,88 KB/s
Up Speed: 1,22 KB/s

At a glance

- ProtonVPN is a paid-for VPN product (a restricted free version is also available)
- Website: https://protonvpn.com
- The restricted free version is limited to 3 locations, 1 device, and has speed limitations
- 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 96
- Pricing DE: 5 devices / 1 year: EUR 96
- Common payment options: credit/debit card, PayPal, cryptocurrency
- Suitable for non-expert users

Summary

ProtonVPN is simple to set up and use, so a good choice for non-experts. 45 country locations are provided, including the UK and USA. A wide range of pricing plans is available, where one can choose the number of devices (from 1 up to 10) and countries hosting VPN servers available. There is no free trial, although you can get a feel for the program using the restricted free version and a 30-day money-back guarantee is provided.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as “mediocre”, the upload speed as “very fast” and the latency as “low”.

According to the company’s privacy policy, a no-logs policy is followed, with the only information monitored being the timestamp of the last successful login attempt. This information is overwritten each time one logs in.

Ease of use

To set up ProtonVPN, download the installer from the vendor’s website and run it. Installation completes very quickly with a couple of clicks. The program is very simple to use. Click on a country in the list, then on an individual, then click *Connect*. The main configuration options in the settings dialog are: start program with Windows; auto-connect on program start; protocol (TCP; UDP; “Smart”); kill switch; DNS leak protection. ProtonVPN supports the protocols OpenVPN and IKEv2.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Moldova, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Serbia, Singapore, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Ukraine, United Arab Emirates, United Kingdom, United States. There are multiple servers for each country.

Pros

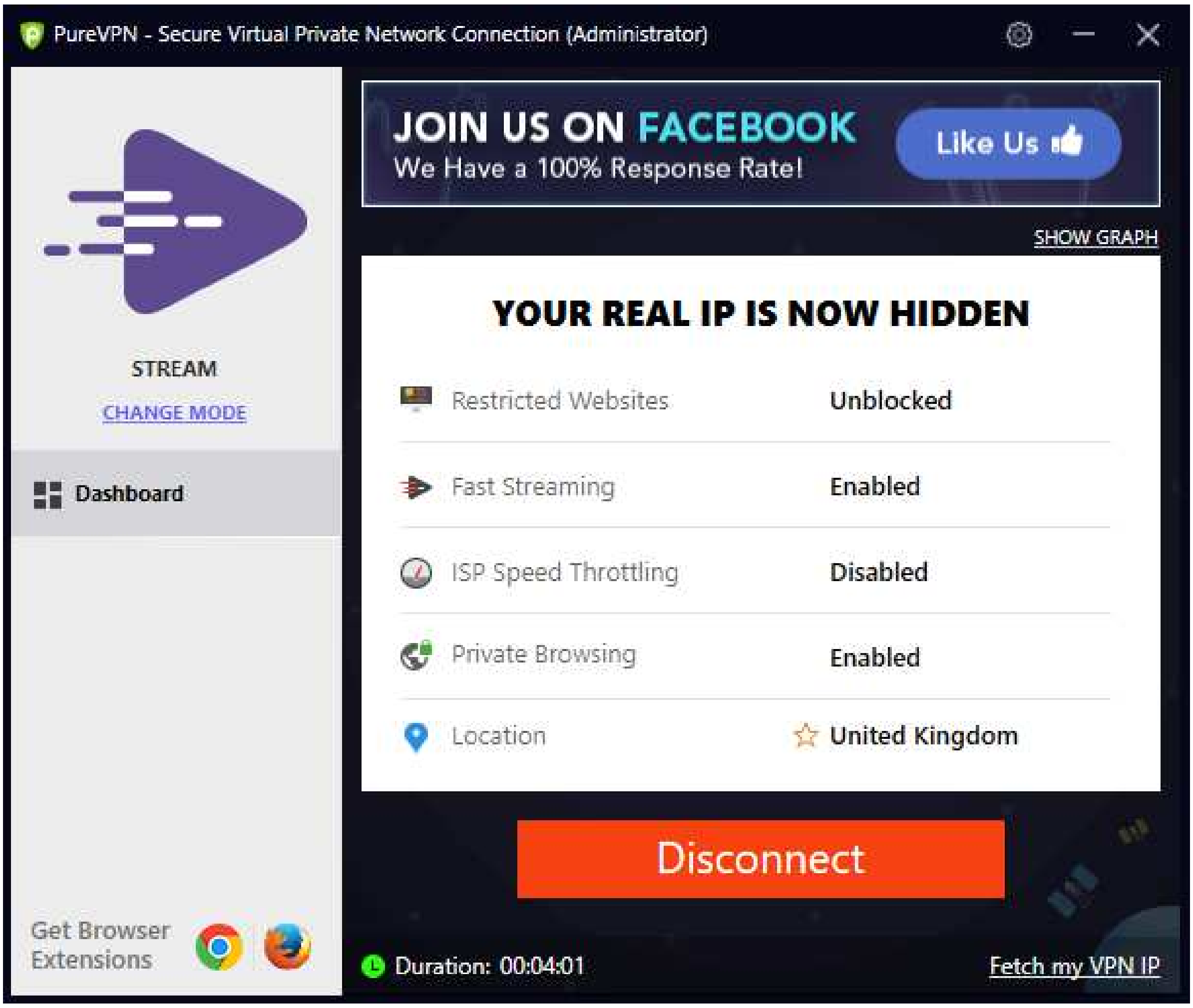
- Restricted free version
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very fast upload speed
- Low latency
- No traffic logging

Cons

- Mediocre download speed
- Minimal connection logging

PureVPN

GZ Systems Ltd.
Hong Kong



PureVPN - Secure Virtual Private Network Connection (Administrator)

JOIN US ON FACEBOOK
We Have a 100% Response Rate!

YOUR REAL IP IS NOW HIDDEN

Restricted Websites	Unblocked
Fast Streaming	Enabled
ISP Speed Throttling	Disabled
Private Browsing	Enabled
Location	United Kingdom

Duration: 00:04:01

At a glance

- PureVPN is a paid-for VPN product
- Website: https://www.purevpn.com
- Free trial: none, but there is a 31-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 70
- Pricing DE: 5 devices / 1 year: EUR 70
- Common payment options: credit/debit card, PayPal
- The program itself is suitable for non-expert users, although the initial setup may confuse some

Summary

PureVPN is rather complicated to set up, but easy enough to use once it is installed. There is a choice of over 140 country locations, including the UK and USA. The pricing plans include 1-month, 6-month and 1-year subscriptions. Although no free trial is provided, one can test the product for 7 days for USD 1, and upon purchase there is a 31-day money-back guarantee.

The program passed our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "mediocre" and the latency as "low".

According to the company's privacy policy, they monitor bandwidth usage for technical reasons, in addition to keeping track of dates the VPN was used, to which location, and from which ISP.

Ease of use

The process involved in getting to the download page for the installer file is certainly the longest and most complicated we have encountered. Once you have purchased the product, you have to complete a sort of web-page wizard, with various pages shown, before you get to the account login page. We found this confusing and did not understand its purpose. Our best advice to users who encounter this would be to keep clicking the *Next* button at the bottom of the page, and simply ignore the content on the page. Two sets of credentials – one for the online account, the other for the VPN app itself – are provided. Once you finally get into your new account, you click on *Downloads/Apps*, and from there you can download the Windows app. You then just need to click *Install*. When the program starts, you have to enter the VPN credentials provided by email; a choice of modes is then shown (*Stream, Be Secure, Download*) with a link to the vendor's website that explains how to use them. We chose *Stream* for our functionality test. When the program first opens, the list of available locations is shown. To make a connection, you just need to click on one of these, and the program will then connect to this location. The main configuration options in the settings dialog are: launch on system startup; auto-connect after launch; user-interface language; encryption options; kill switch; port forwarding. PureVPN supports the protocols OpenVPN, IKEv2, L2TP, PPTP, and SSTP.

Server locations

With regard to virtual locations, an extremely comprehensive list of countries and territories – over 140 in total – is provided, including the USA and UK.

Pros

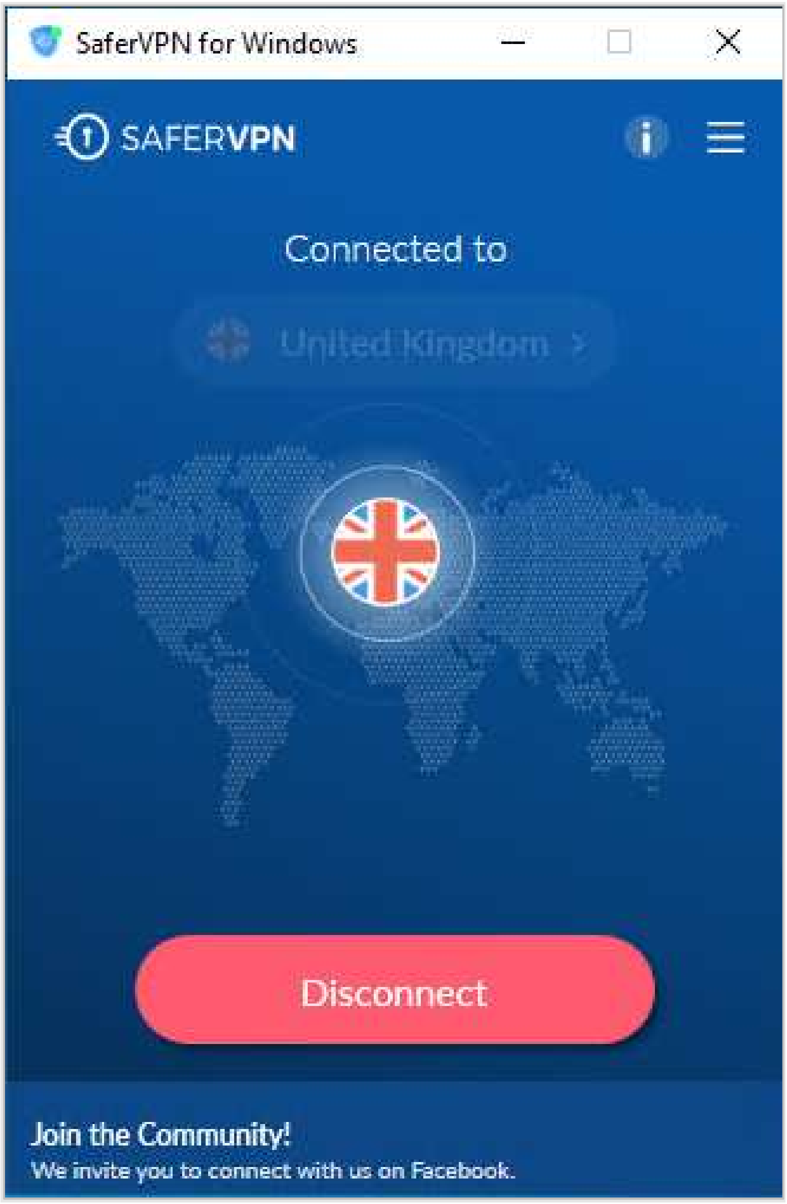
- 31-day money-back guarantee
- Very simple to use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Low latency
- No traffic logging

Cons

- No free trial
- Confusing to set up after purchase
- Mediocre upload speed
- Minimal connection logging

SaferVPN

Safer Social Ltd.
Israel



SaferVPN for Windows

Connected to

United Kingdom

Disconnect

Join the Community!

We invite you to connect with us on Facebook.

At a glance

- SaferVPN is a paid-for VPN product
- Website: https://www.safervpn.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 66
- Pricing DE: 5 devices / 1 year: EUR 54
- Common payment options: credit/debit card, PayPal, cryptocurrency
- Suitable for non-expert users

Summary

SaferVPN is easy to set up and use, so well suited to non-expert users. You can choose from 32 country locations, including the UK and USA. The pricing plans include 1-month, 1-year, 2-year and 3-year subscriptions. Although no free trial is provided, there is a 30-day money-back guarantee.

The program passed our Kill-Switch Test, but failed the Leak Test. We rated the download speed as "very fast", the upload speed as "very fast" and the latency as "very low". SaferVPN was in fact the fastest program in our test, but also the leakiest.

According to the company's privacy policy, they do not collect any traffic logs. However, they do collect connection-related information, such as connection timestamps and data consumed, plus to and from which locations the user connects, without storing IP addresses.

Ease of use

To set up SaferVPN, download the installer from the vendor's website and run it. Setup completes very quickly with a couple of clicks. When the program first starts, you have to log in with your account credentials. The program is very simple to use. Click on the flag in the centre of the window to select a location, then click the *Connect* button. The main configuration options in the settings dialog are: Start with Windows; kill switch; connect automatically when using unsecured Wi-Fi. SaferVPN supports the protocols OpenVPN, IKEv2, L2TP, and PPTP.

Server locations

At the time of testing, the product had servers in these countries: Argentina, Australia, Austria, Belgium, Brazil, Canada, Cyprus, Denmark, Finland, Hong Kong, Hungary, India, Ireland, Israel, Italy, Japan, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, United Kingdom, United States.

Pros

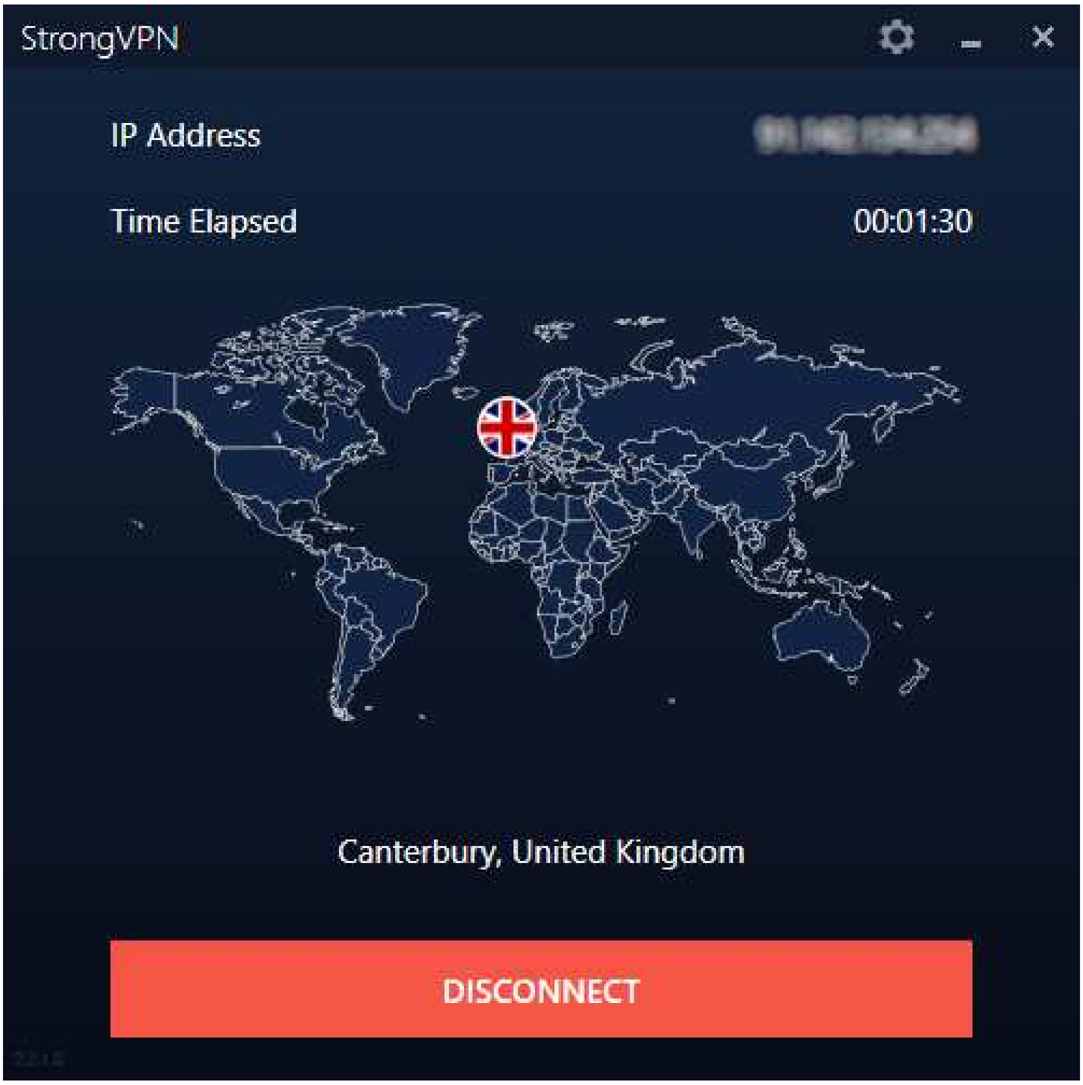
- 30-day money-back guarantee
- Very simple to install and use
- Can start automatically when PC starts
- Kill-Switch Test passed
- Very fast download speed
- Very fast upload speed
- Very low latency
- No traffic logging

Cons

- No free trial
- Leak Test failed
- Minimal connection logging

StrongVPN

Strong Technology LLC
USA



IP Address [redacted]

Time Elapsed 00:01:30

Canterbury, United Kingdom

At a glance

- StrongVPN is a paid-for VPN product
- Website: https://strongvpn.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 70
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal, digital wallets
- Suitable for non-experts

Summary

StrongVPN is a good choice for non-expert users, as it is easy to set up and use and 37 country locations are available. Both a 1-month and a 1-year plan are available, and although no free trial is provided, there is a 30-day money-back guarantee.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "mediocre", the upload speed as "very fast" and the latency as "low".

The company claims in its privacy policy (quoted verbatim) "*We are a zero-logging VPN service, meaning we do not track or store your data while connected to our VPN service*", although a more detailed description would be welcome.

Ease of use

To set up StrongVPN, download the installer from the vendor's website. Installation is very simple and completes in a couple of clicks. When the program first starts, you have to sign in with your account credentials. StrongVPN is simple to use. Just click on the location button, choose a server from the list, and click *Connect*. The main configuration options in the settings dialog are: start with Windows; connect on launch; kill switch. StrongVPN supports the protocols OpenVPN, IKEv2, L2TP, SSTP, and WireGuard.

Server locations

At the time of testing, the product had servers in these countries: Australia United States (15), United Kingdom 6, Turkey, Taiwan, Switzerland, Sweden, Spain, Singapore, Romania, Portugal, Poland, Philippines, Norway, Netherlands, Mexico, Malaysia, Luxembourg, Latvia, South Korea, Japan, Italy, Israel, India, Hong Kong, Germany (2), France, Estonia, Czech Republic, Colombia, Canada (3), Chile, Costa Rica, Brazil (2), Argentina, Australia (4), Ireland, South Africa.

Pros

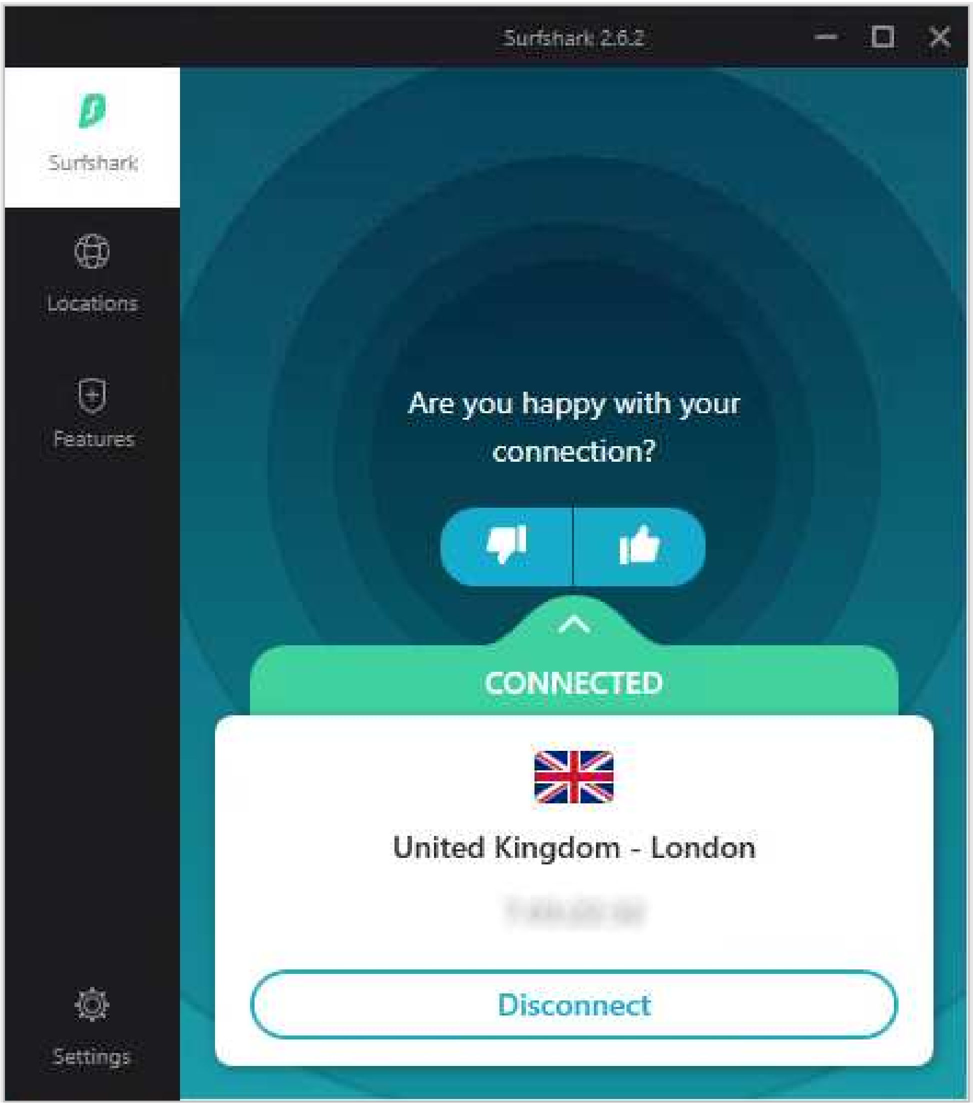
- 30-day money-back guarantee
- Can connect automatically when PC starts
- Very simple to install and use
- Leak Test passed
- Kill-Switch Test
- Very fast upload speed
- Low latency
- No traffic/connection logging

Cons

- No free trial
- Mediocre download speed

Surfshark

Surfshark Ltd.
British Virgin Islands



Are you happy with your connection?

United Kingdom - London

At a glance

- Surfshark is a paid-for VPN product
- Website: https://surfshark.com
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 72
- Pricing DE: 5 devices / 1 year: EUR 60
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Suitable for non-experts
- Other features: "CleanWeb", which claims to block advertisements, trackers, and malware

Summary

Surfshark is well suited to non-expert users, as it is easy to set up and use. 62 country locations are provided, including the UK and USA. Surfshark offers 1-month, 1-year and 2-year pricing plans for an unlimited number of connections. Although there is no free trial, a 30-day money-back guarantee is provided.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "very fast", the upload speed as "fast" and the latency as "very low".

According to the vendor's privacy policy, the company follows a no-logs policy.

Ease of use

To set up Surfshark, download the installer from the vendor's website and run it. Installation is very quick and easy. When the program first starts, you have to log in with your account credentials. The program is very straightforward to use. You just need to select a location from the *Locations* button, and click on it. The main configuration options in the settings dialog are: start program with Windows; auto-connect on program start; kill switch; UI language; bypass Internet restrictions. Surfshark supports the protocols OpenVPN, IKEv2, and SOCKS.

Server locations

At the time of testing, the product had servers in these countries: Albania, Australia (5), Austria, Belgium, Bosnia & Herzegovina, Brazil, Bulgaria, Canada (3), Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France (3), Germany (4), Greece, Hong Kong, Hungary, Iceland, India (3), Indonesia, Ireland, Israel, Italy (2), Japan, Kazakhstan, Latvia, Libya, Luxembourg, Malaysia, Moldova, Netherlands, New Zealand, Nigeria, North Macedonia, Norway, Paraguay, Poland (2), Portugal (3), Romania, Russia (2), Serbia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain (3), Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom (3), United States (26), Vietnam.

Pros

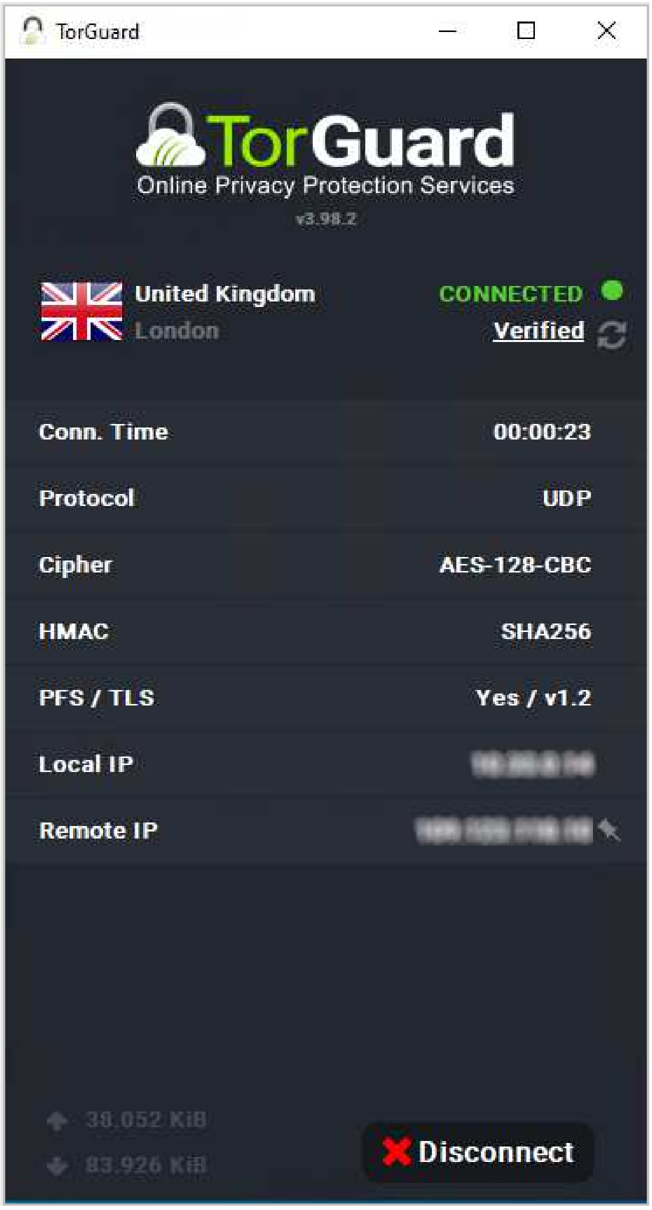
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very fast download speed
- Fast upload speed
- Very low latency
- No traffic/connection logging

Cons

- No free trial

TorGuard

VP Networks LLC
USA



United Kingdom
London

CONNECTED
Verified

Conn. Time	00:00:23
Protocol	UDP
Cipher	AES-128-CBC
HMAC	SHA256
PFS / TLS	Yes / v1.2
Local IP	[redacted]
Remote IP	[redacted]

At a glance

- TorGuard is a paid-for VPN product
- Website: https://torguard.net
- Free trial: 7 days, 7-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 60
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, wire transfer, cryptocurrency, digital wallets

Summary

TorGuard is simple to use, even if the setup wizard might confuse some people. 46 country locations are provided, including the USA and UK. Pricing plans include 1-month, 3-month, 6-month, 1-year and 2-year subscriptions. Both a 7-day free trial and a 7-day money-back guarantee are available.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "mediocre", the upload speed as "very fast" and the latency as "very low".

The company claims in their privacy policy (quoted verbatim) "*TorGuard does not collect or log any data from its Virtual Private Network (VPN) or Proxy services*.", although a more detailed description would be welcome.

Ease of use

To set up TorGuard, download the installer from the vendor's website and run it. The setup wizard offers a choice of components, which may confuse non-expert users; we recommend leaving the default settings. The product is easy to use. You just need to select a location from the *Select Server…* dropdown list, and then click the *Connect* button. Other drop-down lists on the home page let you change protocols and encryption methods. The main configuration options in the settings dialog are: start with Windows; auto-connect when the program is launched; DNS leak features; kill switch. TorGuard supports the protocols OpenVPN, IKEv2, L2TP, PPTP, SOCKS, SSTP, SSH, and WireGuard.

Server locations

At the time of testing, the product had servers in these countries: Australia, Austria, Belarus, Belgium, Brazil, Bulgaria, Canada (2), Chile, Cyprus, Czech Republic, Denmark, Egypt, Finland, France, Germany (2), Greece, Hong Kong, Hungary, Iceland, India, Ireland, Israel (2), Italy, Japan, South Korea, Latvia, Luxembourg, Mexico, Moldova, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Singapore, Slovakia, Spain, Sweden, Switzerland, Taiwan, Thailand, Ukraine, United Arab Emirates, United Kingdom, United States (11).

Pros

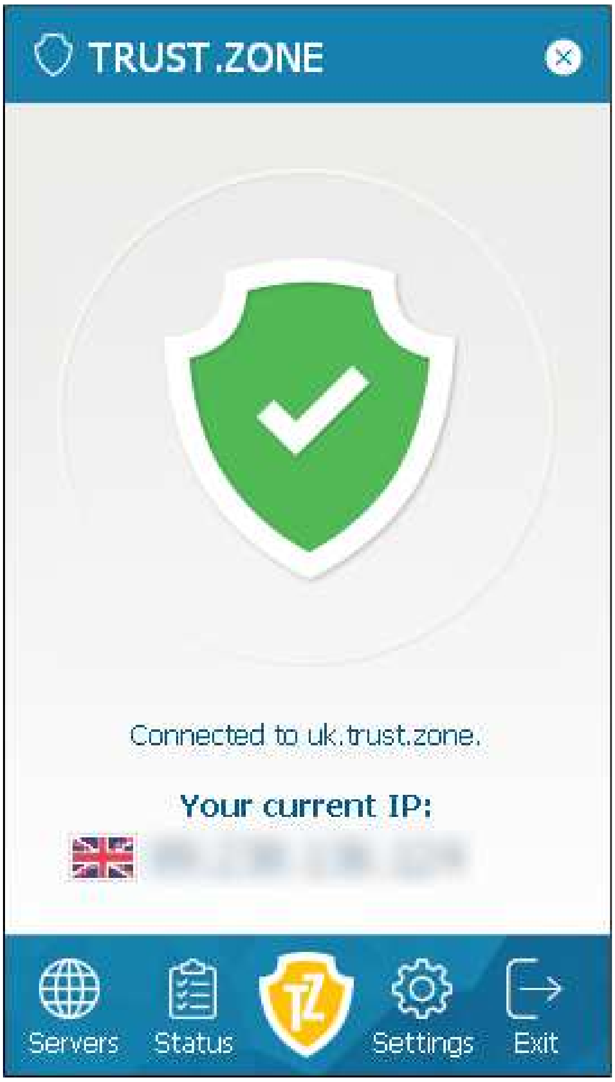
- 7-day free trial
- 7-day money-back guarantee
- Simple to use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very fast upload speed
- Very low latency
- No traffic/connection logging

Cons

- Setup may confuse non-experts
- Mediocre download speed

Trust.Zone VPN

Trusted Solutions Ltd.
Seychelles



Connected to uk.trust.zone.

Your current IP:
[redacted]

At a glance

- Trust.Zone VPN is a paid-for VPN product
- Website: https://trust.zone
- Free trial: none, but there is a 10-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 94 (2x subscription for 3 devices)
- Pricing DE: 5 devices / 1 year: EUR 88 (2x subscription for 3 devices)
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Suitable for non-expert users
- Other features: none

Summary

Trust.Zone VPN is well suited to non-expert users, as it is simple to set up and use. 37 country locations are provided, including the USA and UK. Pricing plans include 1-month, 3-month, 1-year and 2-year subscriptions for 3 devices. Both a 30-day free trial and a 10-day money-back guarantee are provided.

It is unclear to us why the DNS leak protection is disabled by default. It only passed our DNS Leak Test if we enabled the option in the settings. However, the program passed the Kill-Switch Test. We rated the download speed as "very fast", the upload speed as "very fast" and the latency as "low".

The company claims in its privacy policy (quoted verbatim), "*All our VPN servers around the world ARE NOT storing any log files to keep your privacy safe. All the usage data is anonymous and not connected to your real, public IP address.*" This statement implies that no traffic logs are stored, whereas only minimal anonymised connection logs are kept. This assumption is further confirmed in the next section (also quoted verbatim): "*While informing the user that the company does not condone any illegal activities, it also claims to not able to identify a customer even if legally compelled to do so*".

Ease of use

To set up Trust.Zone VPN, download the installer from the vendor's website. The download page tells you that you need to run this as administrator, and provides illustrated instructions for doing this. The last stage of the setup wizard lets you configure the following options: autostart with Windows; auto-connect on program start; kill switch. The settings dialog additionally lets you choose the VPN port. The program is simple to use. You can select a location by clicking on *Servers* in the bottom left-hand corner of the window; click on the server of your choice, and the program will connect to it. Trust.Zone VPN supports the protocols OpenVPN and L2TP.

Server locations

At the time of testing, the product had servers in these countries: South Africa, Hong Kong (2), India (2), Singapore, Japan, Turkey, Albania, Austria, Belgium, Bulgaria, Brazil, Czech Republic, Denmark, Estonia, Finland (2), France (4), Germany, Hungary, Ireland, Italy (2), Latvia (3), Lithuania, Netherlands (4), Norway, Poland, Romania, Russian Federation (2), Serbia, Spain, Sweden, Switzerland, Ukraine, United Kingdom (4), United States (23), Canada (7), Australia (13), New Zealand.

Pros

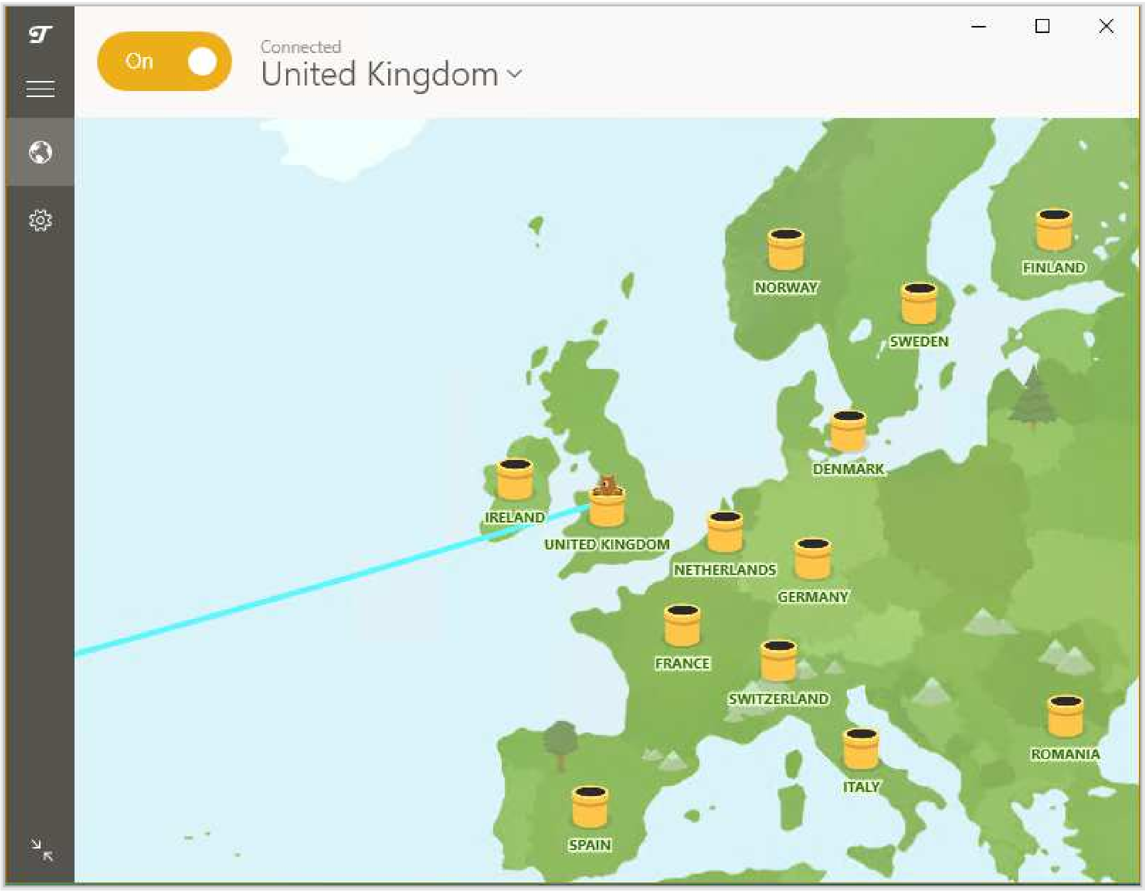
- 10-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very fast download speed
- Very fast upload speed
- Low latency
- No traffic logging

Cons

- No free trial
- DNS leak protection disabled by default
- Minimal connection logging

TunnelBear

TunnelBear Inc.
Canada



At a glance

- TunnelBear is a paid-for VPN product (a restricted free version is also available)
- Website: https://www.tunnelbear.com
- The restricted free version is limited to 500 MB of data traffic per month
- No money-back guarantee
- Pricing US: 5 devices / 1 year: USD 60
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, cryptocurrency
- Suitable for non-expert users

Summary

TunnelBear is ideal for non-expert users, due to its ease of installation and use. 23 country locations are provided, including the USA and UK, and 1-month, 1-year and 3-year plans are available. Even though there is no money-back guarantee, you can try the product out by using the restricted free version.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as "fast", the upload speed as "mediocre" and the latency as "very low".

According to the company's privacy policy, the vendor does not create any traffic-logs, or store originating or VPN-assigned IP Address. They do however keep track of bandwidth usage per month, and whether a user was active during a specific month. TunnelBear was acquired by McAfee in March 2018.

Ease of use

To set up TunnelBear, download and run the installer from the vendor's website. You have to log in after installation, and there is a short wizard explaining how to use the program. The product is very easy to use. You just need to select a country from the list at the top of the window, and slide the connection switch to "On". The program has the most entertaining connection progress display we have seen: a map shows a little animated bear digging a tunnel in the physical location, and popping up in the virtual location. The main configuration options in the settings dialog are: automatically connect VPN on any Wi-Fi network except specified trusted WLANs; start program with Windows; TCP override; block all traffic while VPN is connecting/reconnecting. We assume that the latter amounts to a kill switch. Tunnel Bear supports the protocols OpenVPN, IKEv2, and SOCKS.

Server locations

At the time of testing, the product had VPN servers in these countries: United States, United Kingdom, Canada, Germany, Japan, Australia, Finland, France, Italy, Netherlands, Sweden, Switzerland, Ireland, Spain, Singapore, Norway, Denmark, Hong Kong, Brazil, Mexico, India, New Zealand, Romania.

Pros

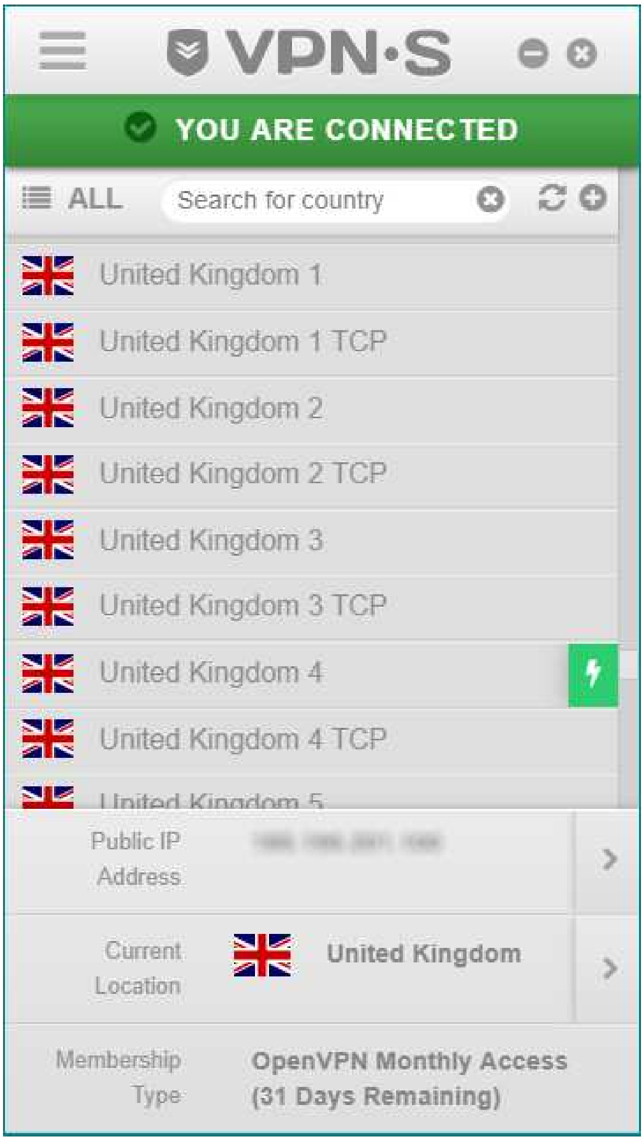
- Restricted free version
- Very simple to install and use
- Can launch automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very low latency
- No traffic log

Cons

- No money-back guarantee
- Mediocre upload speed
- Minimal connection logging

VPNSecure

VPNSecure Pty Ltd.
Australia



YOU ARE CONNECTED

Public IP Address [redacted]

Current Location United Kingdom

Membership Type OpenVPN Monthly Access (31 Days Remaining)

At a glance

- VPNSecure is a paid-for VPN product
- Website: https://www.vpnsecure.me
- Free trial: 30 days, 7-day money-back guarantee, limited to 1 US location and 2 GB of data traffic
- Pricing US: 5 devices / 1 year: USD 80
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Suitable for non-expert users

Summary

VPNSecure is easy to set up and use, and thus ideal for non-expert users. 49 country locations are available, including the UK and USA, and a 7-day money-back guarantee is offered. However, the product's terms and conditions page states that this guarantee only applies if the product does not work at all; inability to access a particular site or service is not a justification for a refund. A 30-day trial is available, and a wide range of pricing plans including 1-month, 6-month, 1-year and 3-year subscriptions are offered.

The program passed our Leak Test and Kill-Switch. We rated the download speed as "mediocre", the upload speed as "slow" and the latency as "high".

The company's privacy policy claims that it does not collect any traffic/connection logs.

Ease of use

To set up VPNSecure, download the installer from the vendor's website and run it. Setup completes quickly with a few clicks. The program is very convenient to use. The main pane of the window shows a scrollable list of servers; you just need to click on the server you want and then click *Connect*. There is a convenient search box that lets you find a location by typing in its first few letters. The main configuration options in the settings dialog are: leak fix; stealth VPN; kill switch; encryption (AES-128-CBC; AES-256-CBC; DES-CBC). VPNSecure supports the protocols OpenVPN, PPTP, SOCKS, and SSH.

Server locations

At the time of testing, the product had servers in these countries: Australia (4), Austria (4), Belgium (4), Bulgaria (4), Brazil (2), Canada (6), Chile (2), Costa Rica (4), Czech Republic (2), Denmark (4), Egypt, Finland (2), France (4), Germany (6), Hong Kong (2), Hungary (4), Iceland (2), India (4), Indonesia (2), Ireland (2), Isle of Man (2), Israel (2), Italy (8), Japan (6), Latvia (2), Lithuania (2), Luxembourg (2), Mexico (2), Moldova (2), Netherlands (6), New Zealand (5), Norway (2), Panama (2), Poland (2), Portugal (2), Romania (4), Russia (2), Singapore (4), South Africa (2), South Korea (2), Spain (4), Sweden (2), Switzerland (4), Taiwan (2), Turkey (2), Ukraine (2), United Kingdom (14), United States (32), Vietnam (2).

Pros

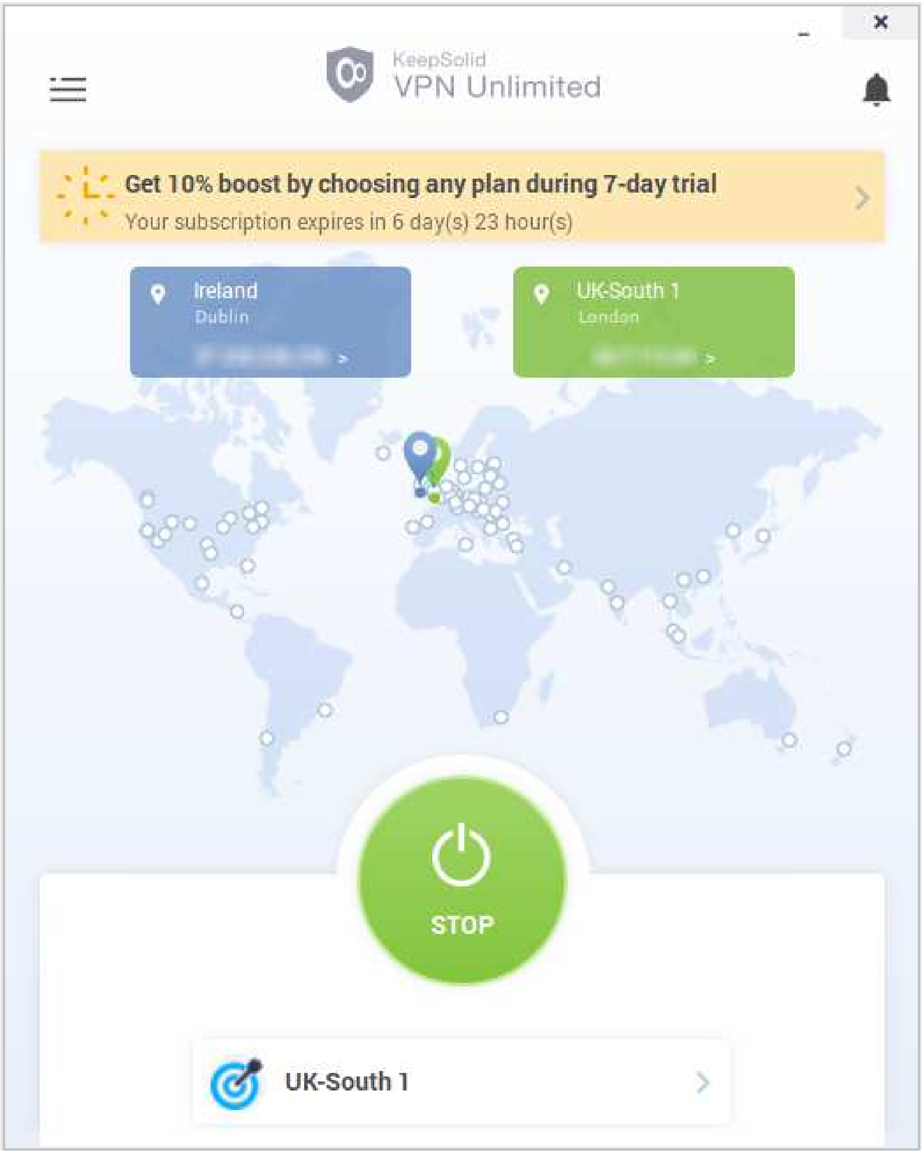
- 30-day free trial
- 7-day money-back guarantee
- Very simple to install and use
- Leak Test passed
- Kill-Switch Test passed
- No traffic/connection logging

Cons

- Mediocre download speed
- Slow upload speed
- High latency

VPN Unlimited

KeepSolid Inc.
USA



Get 10% boost by choosing any plan during 7-day trial
Your subscription expires in 6 day(s) 23 hour(s)

At a glance

- VPN Unlimited is a paid-for VPN product
- Website: https://www.vpnunlimitedapp.com
- Free trial: 7 days, 7-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 60
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Simple to use

Summary

VPN Unlimited is straightforward to set up (though please see the note below regarding disabling antivirus during setup). Once installed, it's very easy to use. Both 55 country locations, including the USA and UK, a 7-day money-back guarantee and a 7-day free trial are provided. A wide range of pricing plans is offered, including 1-month, 1-year and 3-year subscriptions.

The program passed both our Leak Test and Kill-Switch. We rated the download speed as "mediocre", the upload speed as "mediocre" and the latency as "very low".

The company's privacy policy claims it does not store any connection or traffic logs. They claim (quoted verbatim) "*Certain personal data collected by us automatically (i.e. IP address, connection type, browser type and operating system) is stored only for the duration of your session in the VPN Services. This means that KeepSolid never stores or logs these categories of personal data after the end of your session in our VPN Services – we delete such personal data after your session ends*."

Ease of use

To set up VPN Unlimited, download the installer from the vendor's website and run it. The setup wizard warns you to disable your AV to prevent it blocking the product installation (if you do this, you obviously need to reactivate it immediately afterwards). Installation completes very easily in a few clicks. When the program first starts, you have to log in with your account credentials. VPN Unlimited is very easy to use. You just select a server from the list at the bottom of the window, and click the *Start* button. The main configuration options in the settings dialog are: stop DNS leak, kill switch, run on startup. VPN Unlimited supports the protocols OpenVPN, IKEv2, SOCKS, and WireGuard.

Server locations

At the time of testing, the product had servers in these countries: Austria, Australia, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada (3), Chile, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France (2), Germany (2), Greece, Hong Kong, Hungary, Iceland, India (2), Ireland, Isle of Man, Israel, Italy, Japan, Latvia, Libya, Lithuania, Luxembourg, Malaysia, Mexico, Moldova, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, United Kingdom (3), United Arab Emirates, United States (13), Vietnam.

Pros

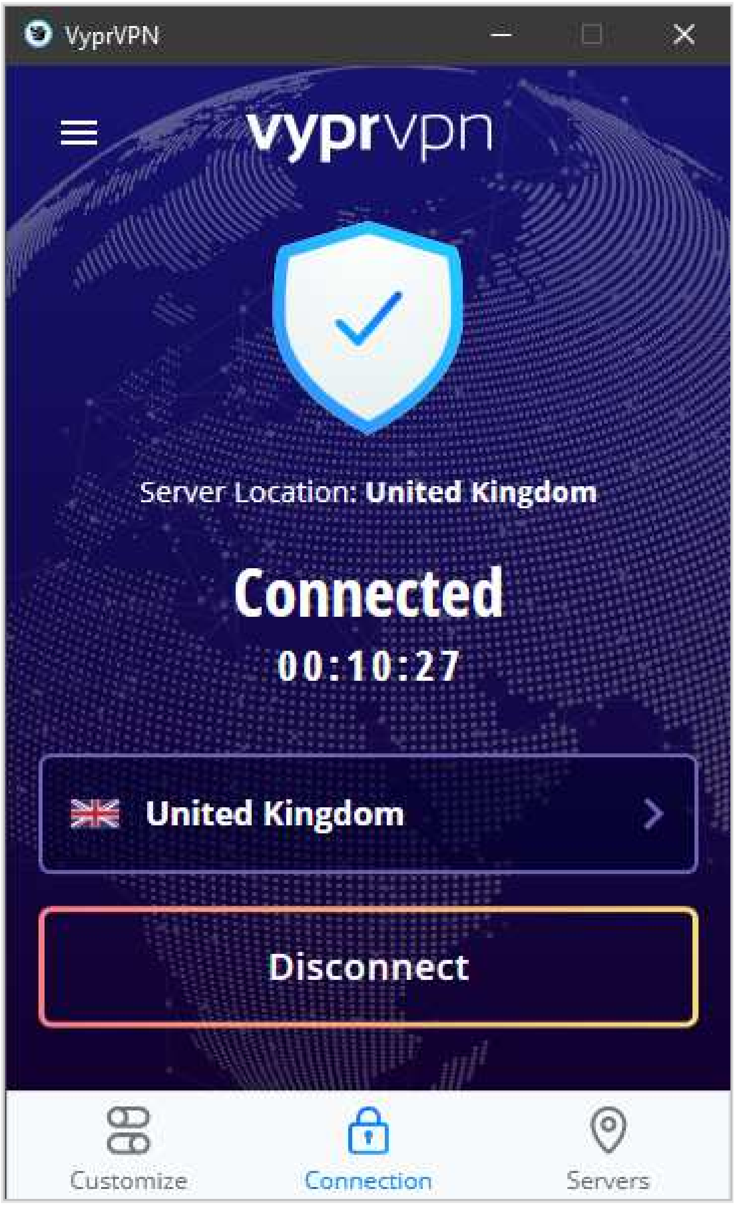
- 7-day free trial
- 7-day money-back guarantee
- Simple to use
- Can start automatically when PC starts
- Leak Test passed
- Kill-Switch Test
- Very low latency
- No traffic/connection logging

Cons

- Mediocre download speed
- Mediocre upload speed

VyprVPN

Golden Frog GmbH
Switzerland



Server Location: United Kingdom

Connected

00:10:27

At a glance

- VyprVPN is a paid-for VPN product
- Website: https://www.goldenfrog.com/vyprvpn
- Free trial: none, but there is a 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 45
- Pricing DE: 5 devices / 1 year: EUR 45
- Common payment options: credit/debit card, PayPal
- Suitable for non-expert users

Summary

VyprVPN is simple to install and use, so suitable for non-expert users. 64 country locations are provided, including the UK and USA and, although there is no free trial, a 30-day money-back guarantee is offered. Available pricing plans include 1-month, 1-year and 2-year subscriptions.

The program passed our Leak Test and Kill-Switch. We rated the download speed as “mediocre”, the upload speed as “mediocre” and the latency as “very low”.

The company’s privacy policy claims that it follows a zero-logs policy, whereby neither traffic nor connection logs are collected.

Ease of use

To set up VyprVPN, download the installer from the vendor’s website and run it. Setup is very straightforward and completes in a few clicks. The program is very simple to use. Just click on the locations list, then on the server you want to connect to. The main configuration options in the settings dialog are: public Wi-Fi protection; kill switch; VyprDNS; connect on system boot/login; launch app on login. VyprVPN supports the protocols OpenVPN, IKEv2, L2TP, and PPTP.

Server locations

At the time of testing, the product had servers in these countries: Algeria, Argentina, Australia 3, Austria, Bahrain, Belgium, Brazil, Bulgaria, Canada, Colombia, Costa Rica, Czech Republic, Denmark, Egypt, El Salvador, Finland, France, Germany, Greece, Hong Kong, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Macao, Malaysia, Maldives, Marshall Islands, Mexico, Netherlands, New Zealand, Norway, Pakistan, Panama, Philippines, Poland, Portugal, Qatar, Romania, Russia, Saudi Arabia, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, Uruguay, USA 8, Vietnam.

Pros

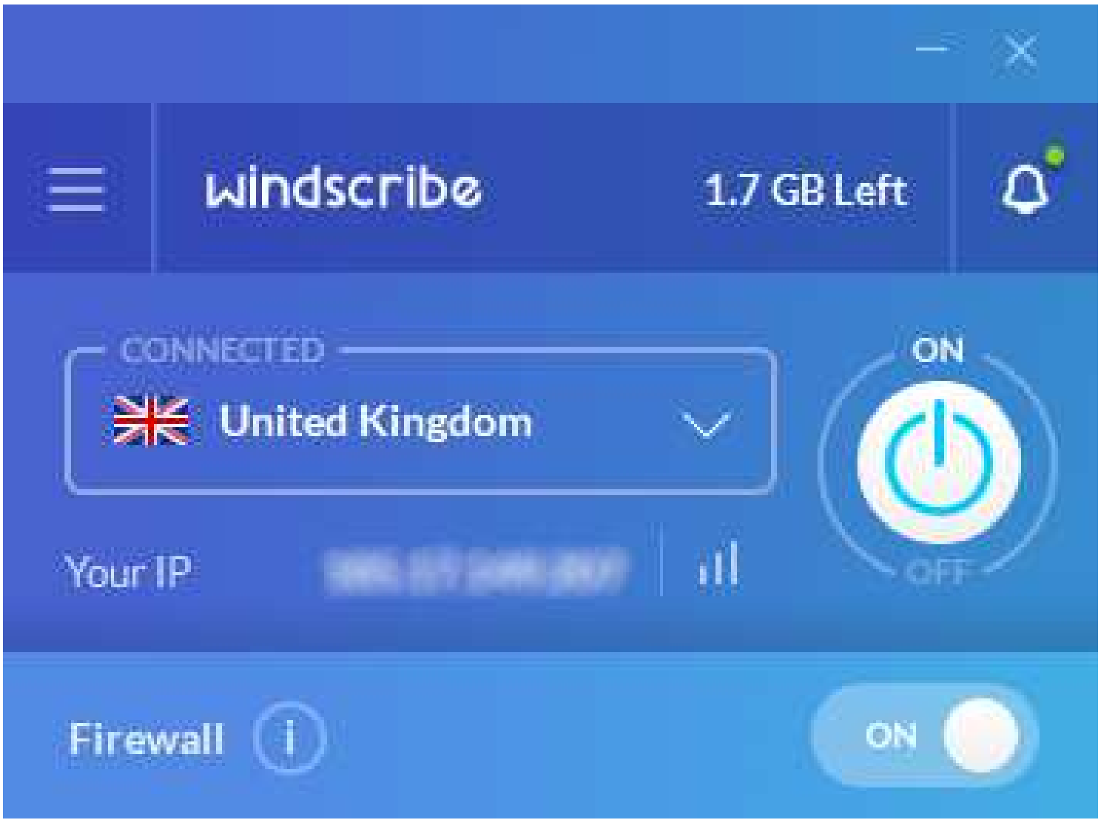
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Very low latency
- No traffic/connection logging

Cons

- No free trial
- Mediocre download speed
- Mediocre upload speed

Windscribe

Windscribe Ltd.
Canada



At a glance

- Windscribe is a paid-for VPN product (a restricted free version is also available)
- Website: https://windscribe.com
- The restricted free version is limited to 10 locations, 2 GB of data traffic per month, and fewer configuration options
- 3-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 49
- Pricing DE: 5 devices / 1 year: EUR n/a
- Common payment options: credit/debit card, PayPal, wire transfer, cryptocurrency, digital wallets
- Easy to use
- Other features: advertisement/tracker/malware blocking (paid version only)

Summary

Windscribe is very easy to use. 59 country locations are provided, including the UK and USA. The subscription covers unlimited devices. Although there is only a 3-day money-back guarantee, one can try out the program using the restricted free version.

The program passed both our Leak Test and Kill-Switch. We rated the download speed as “mediocre”, the upload speed as “fast” and the latency as “low”.

The company state in their privacy policy that they do not collect any traffic-logs. They do however keep track of both bandwidth usage per month, and connection timestamps.

Ease of use

To set up Windscribe, download the installer from the vendor’s website and run it. Installation completes in a matter of seconds. A Windows Firewall prompt appears, asking you to grant firewall exceptions for public networks. Windscribe is very simple to use. You just select a location/server from the drop-down list on the home page, and click the “Connect” button. The main configuration options in the settings dialog are: start with Windows; auto-connect on program start; A kill switch is accessible from the program’s home page, under the name “Firewall”. Windscribe supports the protocols OpenVPN, IKEv2, and SOCKS.

Server locations

At the time of testing, the product had servers in these countries: United States, Canada, United Kingdom, Hong Kong, France, Germany, Netherlands, Switzerland, Norway, Romania, Italy, Mexico, Spain, Sweden, Ireland, Denmark, Poland, Austria, Czech Republic, Hungary, Finland, Bulgaria, Belgium, Latvia, Lithuania, Portugal, Slovakia, Moldova, Croatia, Greece, Estonia, Tunisia, Albania, Slovenia, Serbia, Bosnia and Herzegovina, Iceland, Ukraine, India, Russia, Turkey, Azerbaijan, Israel, South Africa, Brazil, Colombia, Australia, New Zealand, Japan, Singapore, South Korea, Taiwan, Malaysia, Vietnam, Thailand, Indonesia, Philippines, Argentina.

Pros

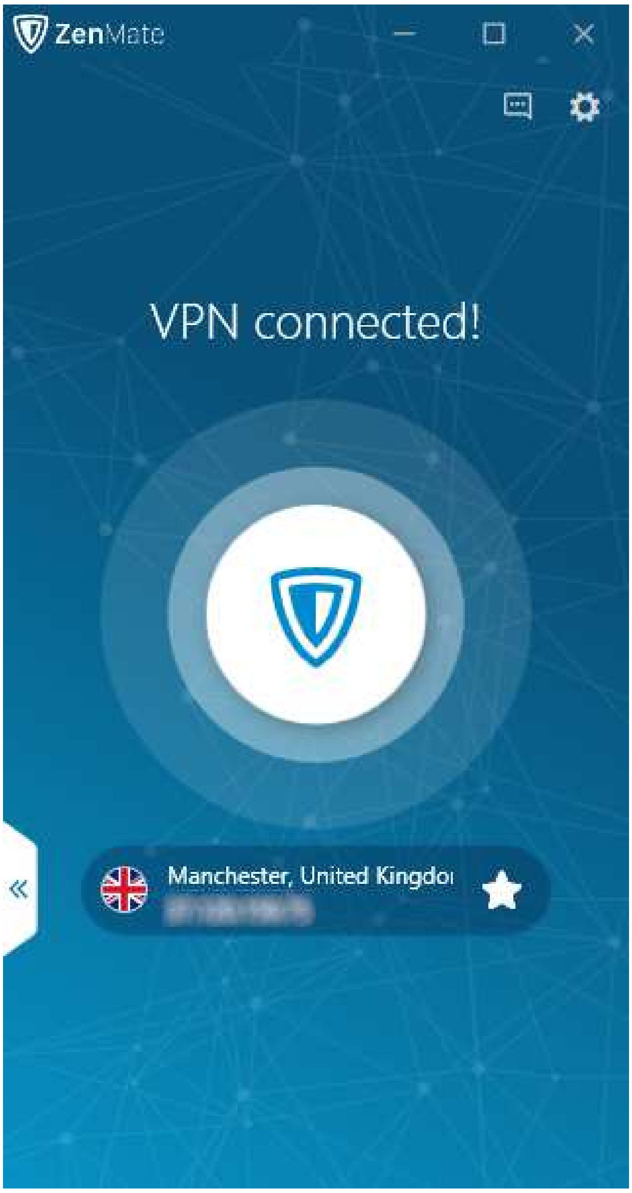
- Restricted free version
- Simple to use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast upload speed
- Low latency
- No traffic logging

Cons

- 3-day money-back guarantee
- Mediocre download speed
- Minimal connection logging

ZenMate VPN

ZenGuard GmbH
Germany



VPN connected!

Manchester, United Kingdoı
[redacted]

At a glance

- ZenMate VPN is a paid-for VPN product (a restricted free version is also available)
- Website https://zenmate.com
- The restricted free version is limited to 4 locations, 2 MB/s of bandwidth, and only available as browser extension for Chrome and Firefox
- 30-day money-back guarantee
- Pricing US: 5 devices / 1 year: USD 40
- Pricing DE: 5 devices / 1 year: EUR 40
- Common payment options: credit/debit card, PayPal, wire transfer

Summary

ZenMate VPN is simple to set up and use, so well suited to non-experts. 37 country locations are provided, including the USA and UK. A 30-day money back guarantee is offered, but one can try out the restricted free version. A wide range of pricing plans are offered, including 1-month, 6-month and 1-year subscriptions for unlimited devices.

The program passed both our Leak Test and Kill-Switch Test. We rated the download speed as “fast”, the upload speed as “mediocre” and the latency as “very low”.

According to the company’s privacy policy the vendor does not collect any logs, although a more detailed description would be welcome. On the support website the company states (quoted verbatim): “*We do not store or log your personal data which can be used to identify you or what you're doing online. We do not monitor your online sessions. In fact - we can’t! Strict German privacy laws regulate our company’s use of your information. As we don’t store the data in the first place, this also means that we can’t be forced into giving away personal data to any government or sell it to any 3rd parties*.”

Ease of use

To set up ZenMate VPN, download the installer from the vendor’s website and run it. There are no decisions to make, and installation completes very quickly. The program is very simple to use. You just select a virtual location from the drop-down list, then click the circular “connect” button. The main configuration options in the settings dialog are: start program automatically with Windows; connect automatically when program starts; specify the server to use if connecting automatically; user interface language; kill switch. ZenMate VPN supports the protocols OpenVPN, IKEv2, and L2TP.

Server locations

At the time of testing, the product had servers in these countries: Albania, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Hungary, Israel, Italy, Japan, South Korea, Latvia, Lithuania, Luxembourg, Moldova, Netherlands, Norway, Poland, Romania, Russia, Serbia, Singapore, Slovakia, South Africa, Spain, Sweden, Switzerland, Ukraine, United Kingdom, United States.

Pros

- Restricted free version
- 30-day money-back guarantee
- Very simple to install and use
- Can connect automatically when PC starts
- Leak Test passed
- Kill-Switch Test passed
- Fast download speed
- Very low latency
- No traffic/connection logging

Cons

- Mediocre upload speed

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
(May 2020)