REVIEWS / SOFTWARE

NordVPN: PCMag's Top Pick

PC MAGAZINE EDITORS' CHOICE

As VPN services go, it's hard to beat NordVPN. It has a large and diverse collection of servers, an excellent collection of advanced features, strong privacy and security practices, and approachable clients for every major platform. While NordVPN's monthly fee is higher than the average, it more than justifies that cost with an excellent product. It's a rare 5-star PCMag Editors' Choice winner.

NordVPN

$11.95 per month, other pricing options

●●●●●

WHAT IS A VPN?

When you switch on a VPN, it creates an encrypted tunnel between your computer and a server controlled by the VPN service. All your web traffic is routed through this tunnel, meaning that no one, not even someone on the same network, can sneak a peek at your data. It also prevents malicious network operators from intercepting your information or using DNS poisoning techniques to trick you into visiting phishing pages. A VPN even protects your web traffic from being monitored by your ISP, which is critically important now that ISPs can sell anonymized user data.

NORDVPN PRICING AND FEATURES

NordVPN offers four pricing tiers: $11.95 per month, $83.88 annually, $95.75 every two years, or $107.55 every three years. The company accepts credit cards, of course, but it also takes PayPal, various anonymous cryptocurrencies, and other online payment methods. NordVPN has a 30-day money-back guarantee.

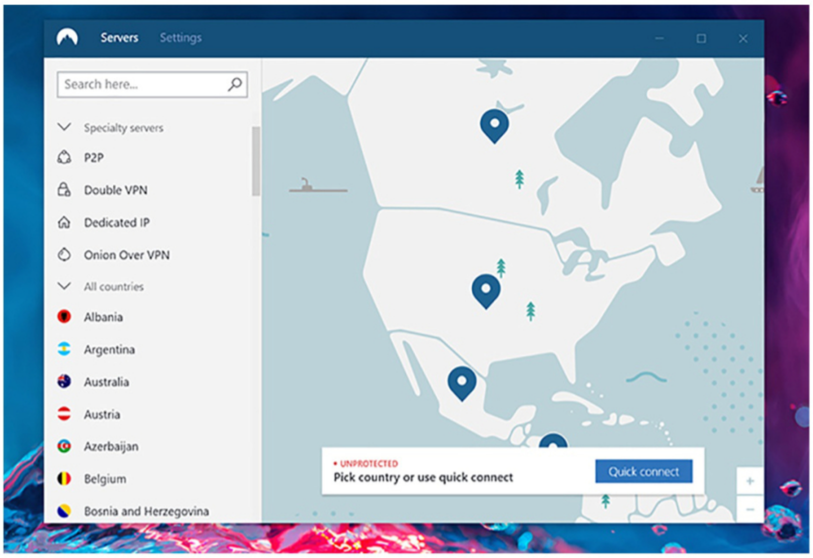
As of this writing, the average monthly price for the top 10 PCMag-rated VPN services is about $10.28. NordVPN's cost is above that average, but its host of extra features, excellent apps, and core service more than justify the price tag. That said, other VPN services have less expensive and more flexible pricing plans. Private Internet Access, for example, costs just $6.95 per month and shares an Editors' Choice award with NordVPN.

NordVPN has discontinued its free trial offering, stating that scammers were taking advantage of it. If you need a no-cost VPN, though, there are some capable and generous free VPN services. Most free VPNs limit users in some way. Notably, ProtonVPN does not limit the amount of data free members can use.

NordVPN

PROS More than 5,200 servers in diverse locations worldwide. Unique, specialized servers. Six simultaneous connections. P2P allowed. Browser apps. Blocks ads, other web threats. Strong customer privacy stance.

CONS Expensive. Cannot purchase additional simultaneous connections.



> A VPN creates an encrypted tunnel between your computer and a server controlled by the VPN service.

You can use up to six devices simultaneously on NordVPN, but there are some limitations concerning connecting multiple devices to the same server at the same time. That's still excellent, as most VPN services limit you to five simultaneous connections. CyberGhost notably provides seven device slots, and IPVanish offers 10. Neither Avira Phantom VPN nor Windscribe VPN place a limit on the number of devices you can use. Most services let you add more device slots to your subscription for a fee, but NordVPN does not give you that option.

VPN PROTOCOLS

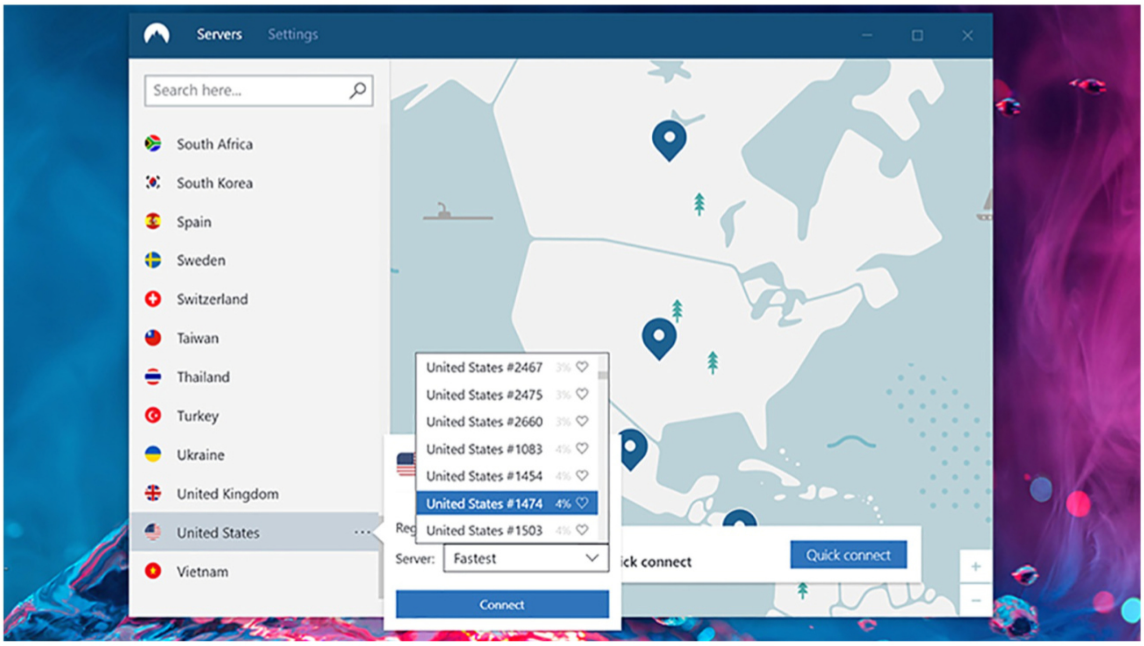
There are several ways to establish a VPN connection, and our preference is for services that use OpenVPN, which is open-source and has been thoroughly examined for potential problems. It also has a reputation for excellent speed and quickly reestablishing a dropped connection. NordVPN supports OpenVPN and my second choice, IKEv2/IPSec, on all platforms. Note that NordVPN also uses OpenVPN in its iPhone app. That's unusual, as Apple has more stringent requirements for apps that include this technology.

The new hotness in the world of VPN protocols is WireGuard. This technology is still under development, but NordVPN is already tinkering with the technology. It's not yet public and may not pan out in the long run. If you're interested in it, other VPN services, such as Mullvad, already offer WireGuard servers as a limited feature.

VPN SERVERS AND SERVER LOCATIONS

Part of what you're paying for when you buy a VPN subscription is access to the company's network of VPN servers. The best services offer lots of server locations, giving you many options for spoofing your location and improving the odds that there will be a server near your actual, physical location. That's important, because the closer you are to the VPN server you're using, the better performance you're likely to experience.

NordVPN lets you select one from a list of 62 countries. The bulk of NordVPN's servers are in the US and the UK, which is not unusual for VPN companies. But NordVPN also has a good mix of servers the world over, covering locations across Asia, Central and South America, Central and Eastern Europe, and a handful in India and the Middle East. The company currently offers two locations in Africa (Egypt and South Africa), a region ignored by most other VPN services.



While I like NordVPN's geographic diversity, other VPN companies outshine it. ExpressVPN, for example, covers 94 countries. But NordVPN has 5,293 servers available, which is by far the largest network of any service I've yet reviewed. Private Internet Access, by comparison, has 3,522 servers, and ProtonVPN has only 300. VPN services spin up new servers on an as-needed basis, so the total number of servers is partly a reflection of how popular a service is. Ideally, a large pool of servers ensures that no one server becomes overcrowded. I can't correlate performance directly to server count, but the sheer size of NordVPN's network suggests that you're unlikely to encounter an overburdened server.

> **NordVPN has 5,293 servers available, which is by far the largest network of any service I've yet reviewed.**

While most of us think of a server as a physical box with computer guts inside, it's also possible to create multiple virtual servers hosted on a single physical machine. Many VPNs use virtual servers to keep up with demand, but some VPNs configure their virtual servers to appear in a different country than the physical machine that hosts them. Virtual servers aren't necessarily a bad thing, but they can be worrisome if you're specifically concerned about your web traffic being routed through a country other than the one you chose. It's also possible that virtual servers may offer slower speeds than physical servers, but we have not verified this in testing.

A NordVPN representative told me that all of its servers are dedicated, and none are virtual servers. That means that the servers are physically located where they claim to be. Other services approach virtual servers differently. ExpressVPN has 3 percent of its servers in locations other than where they are listed and offers a list of those servers' true locations. Hide My Ass, on the other hand, claims 286 server locations but has physical hardware in only 61 sites.

VPNs are sometimes used to bypass government censorship by connecting to a VPN server in another country. I don't make a specific recommendation for a VPN to bypass government censorship, because the stakes of getting it wrong are simply too high. NordVPN does provide obfuscated servers designed to be accessible from within China.

Notably, NordVPN offers servers in Hong Kong, Russia, Turkey, and Vietnam, all of which have restrictive internet policies. Connecting to one of these servers will not bypass censorship, but it could provide a modicum of privacy when browsing the web within those countries.

NordVPN's best feature, however, is the variety of specialized servers it offers. These include servers for BitTorrent traffic over VPN, double encryption, connection to the Tor anonymization network, and defending against DDoS attacks. It also provides obfuscated servers that are intended to slip past governments or services that block VPN traffic.

YOUR PRIVACY WITH NORDVPN

When you use a VPN, it has as much insight into your online activities as your ISP does. If it desired, it could examine every bit of information passing through its system. It also can potentially identify you to another party (read: law enforcement), making it possible to track you online. That's why it's important that before you buy a VPN subscription, you understand and are comfortable with the steps the company takes to safeguard your privacy.

A NordVPN representative tells me the company does not, "store connection timestamps, used bandwidth, traffic logs, or IP addresses." That's excellent. Instead, NordVPN retains the username and time of the last session, but for only 15 minutes after you disconnect from the VPN. All this information is available in the company's privacy policy.

A representative from NordVPN assured me that the company does not profit from the sale of user data. The company does not generate revenue from sources other than customer subscriptions.

In November of 2018, NordVPN announced that it had passed a third-party audit of its no-log policy by one of the "big four audit firms." It joins several VPN companies, including TunnelBear VPN, that are undertaking similar audits. Each of these audits is different, but the effort shows that the companies are serious about consumer privacy and security. Much of the information in this audit was initially withheld, along with the name of the audit firm. NordVPN has since made the full report available to all subscribers, and it's been leaked elsewhere, revealing that PricewaterhouseCoopers was the firm that conducted the audit. I hope that NordVPN will work to make future audits more transparent from the start.

NordVPN has not participated in the Center for Democracy and Technology's VPN questionnaire project, but it has shared much of the same information with PCMag, which also sends out extensive questionnaires as part of our testing. NordVPN also does not make it easy to find the name of its parent company or information on corporate leadership on its website—a point the CDT would likely consider a negative. A company representative told me, however, that it is owned by Tefincom S.A. NordVPN does not

> **“NordVPN retains the username and time of the last session, but for only 15 minutes after you disconnect from the VPN.”**

issue transparency reports about requests for information by law enforcement, but it does maintain a warrant canary that indicates it has not received any National Security letters, gag orders, or government-issued warrants. A company representative told me it has not received any government or law enforcement requests for information.

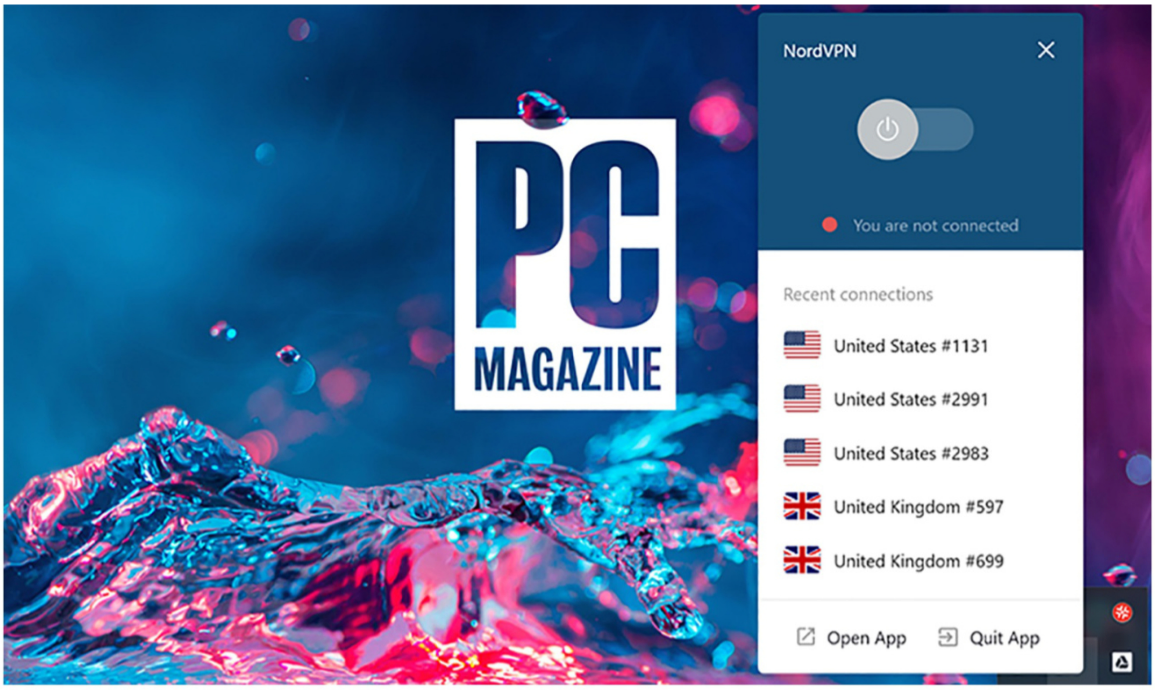
NordVPN is based in and operates under the legal jurisdiction of Panama, where there are no laws requiring the company to retain data for a mandatory period. The company says it doesn't collect log data, so it has no information it could actually hand over in response to a subpoena. It also would respond only to a court order or subpoena issued by a Panamanian court.

> “The company says it doesn't collect log data, so it has no information it could actually hand over in response to a subpoena.”

In general, I'm satisfied with NordVPN's stance on privacy and the efforts it makes to protect customers. It is difficult, however, to fully endorse the privacy practices of any given VPN company. To do so would require deep access to the company's code and hardware as well as the technical expertise to interpret it all. As always, however, you as the consumer should ask yourself whether you are comfortable with trusting any given company with your personal information.

HANDS ON WITH NORDVPN

Nearly every VPN service I have reviewed offers handy apps instead of requiring that you manually set up your VPN. NordVPN has always offered an excellent user experience with its apps, regardless of the platform you use. The Windows client shares a lot of design features with NordVPN mobile apps, with a monochrome blue map as its focus. It's a bit whimsical, with submarines and ships on the cartoon seas, but it's an easy way to select the server you want. I used a Lenovo ThinkPad T460s laptop running the latest version of Windows 10.



Clicking the Quick Connect option at the top of the screen or the System Tray connects you to the VPN server that NordVPN thinks is best (generally, the closest and therefore fastest). That's a great option for people unfamiliar with VPN services. You can change servers by clicking a location on the map or, if your geography skills are lacking, using the search bar at the top of the screen. NordVPN's specialized servers are at the top of the list, putting them within easy reach. The client also includes a Kill Switch that shuts off access to the internet for specific applications, should your computer become disconnected from the VPN.

> **"NordVPN gives you the option to drill down to specific cities and servers and shows the current load on those servers."**

I really like that NordVPN gives you the option to drill down to specific cities and servers and shows the current load on those servers. It's handy for finding a server that will work well for you.

NordVPN does not support split tunneling, which lets you designate which apps send their traffic through the VPN tunnel and which do not. It's useful for apps that require a more robust connection but don't need additional security, such as video games. TunnelBear and ExpressVPN both include this feature.

One concern is that your VPN may be leaking your true IP address or DNS information. In my testing, I found that NordVPN successfully changed my IP address and hid my ISP information. My DNS leak test indicated that NordVPN was not leaking information.

> **In my testing, I found that NordVPN successfully changed my IP address and hid my ISP information.**

NORDVPN AND NETFLIX

I am pleasantly surprised that Netflix did not block me from streaming content while I was connected to a US-based NordVPN server when I tested it. That's great, because Netflix blocks VPNs aggressively. I also found that I was able to stream content from Netflix while connected to NordVPN servers in Australia, Canada, Japan, and the UK. Of the VPNs I have tested so far, it's the most compatible with Netflix, but that could change at any point—Netflix often manages to block services that previously worked well.

Note that while Netflix does not explicitly prohibit the use of VPNs, section 4.3 of its terms of use mentions the use of technology to confirm your location. This document also doesn't guarantee access to content outside of the country where you created your account. Using a VPN might not breach this agreement, but it's clear that Netflix takes a dim view of the technology.

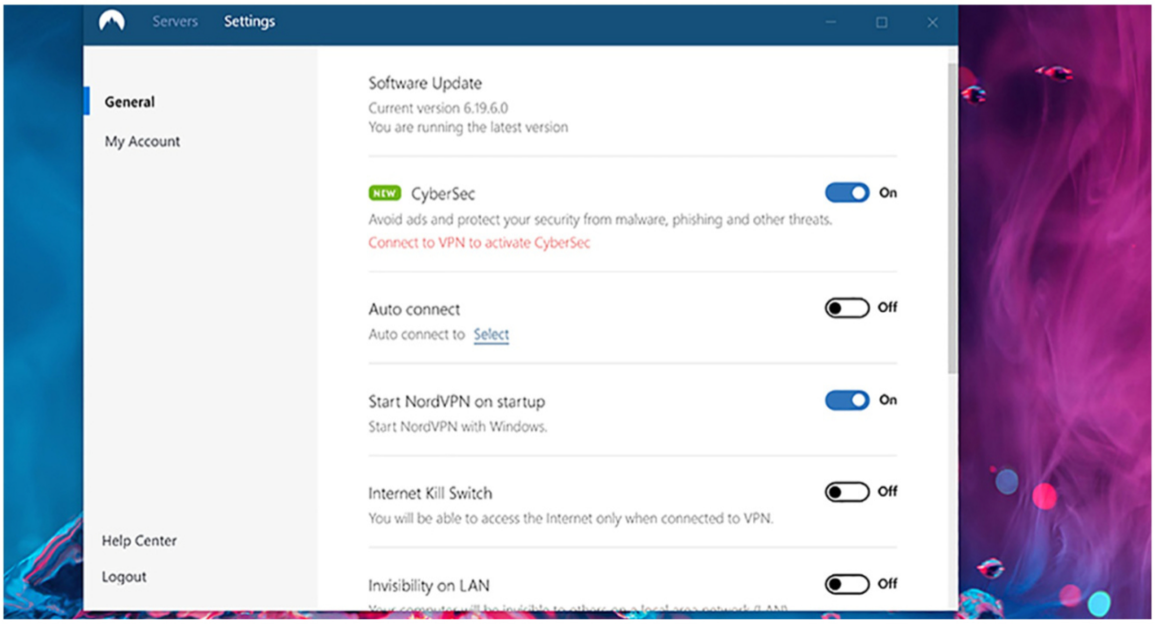
BEYOND VPN

Many VPNs include additional features to help secure customers and lure in new ones. NordVPN has a small collection it calls CyberSec. With it, NordVPN can block ads and malware and prevent DDoS activity at the network level.

I don't test the efficacy of ad-blocking with VPNs, but I do appreciate that VPNs are adding this particular feature, since many online ads contain trackers that can correlate your movement between websites. That said, TunnelBear provides ad and tracker blocking in a handy browser plug-in with far more flexibility in what ads get blocked and on what sites. My preferred ad blocker for browsers is still the Electronic Frontier Foundation's Privacy Badger. Note that Google has begun requiring VPNs to disable ad-blocking in mobile apps.

To block malware payloads, NordVPN uses blacklists of known malicious sites as well as phishing sites that are designed to trick you into handing over your personal information. It's a good start, but these sites are short-lived, and new ones pop up in seconds. And blacklists can only do so much. Stand-alone antivirus software generally includes advanced heuristic models that can catch never-before-seen malware before it damages your computer. I do not currently evaluate the effectiveness of the anti-phishing capabilities of VPNs.

None of this is to sell NordVPN short; having more features is always good, but don't expect it to replace your antivirus.



Software Update
Current version 6.19.6.0
You are running the latest version

NEW CyberSec — On
Avoid ads and protect your security from malware, phishing and other threats.
Connect to VPN to activate CyberSec

Auto connect — Off
Auto connect to Select

Start NordVPN on startup — On
Start NordVPN with Windows.

Internet Kill Switch — Off
You will be able to access the Internet only when connected to VPN.

Invisibility on LAN — Off

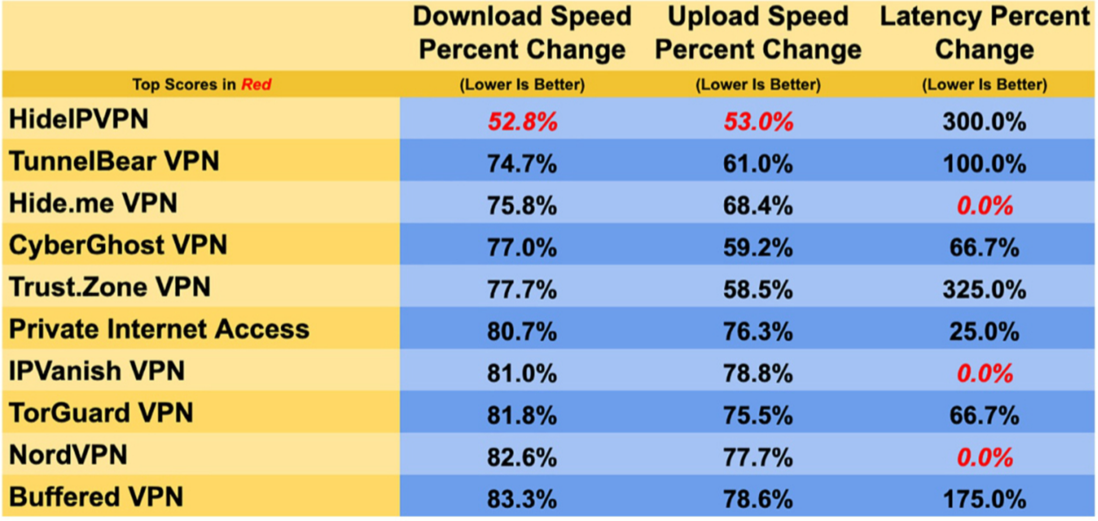
The last tool, DDoS protection, is a unique and interesting offering. During a DDoS attack, infected computers simultaneously access the same website over and over again. If there are enough machines involved, it can bring even the most robust website to a screeching halt. NordVPN says that even if your computer has been infected with malware for these kinds of nefarious purposes, the anti-DDoS feature prevents your computer from joining in the attack.

SPEED AND PERFORMANCE

When you use a VPN, it will have an effect on your web browsing performance. To get a sense how great an impact a VPN has, we conduct a series of speed tests using the Ookla speedtest tool. (Ookla is owned by Ziff Davis, which also owns PCMag.)

In these tests, I found that NordVPN had no effect on latency, likely a result of its abundant servers. But download speeds were reduced by 82.6 percent and upload speeds reduced by 77.7 percent.

You can see how NordVPN compares in the chart below with the top 10 performers of the 30-plus services we tested.



	Download Speed Percent Change	Upload Speed Percent Change	Latency Percent Change
Top Scores in *Red*	(Lower Is Better)	(Lower Is Better)	(Lower Is Better)
HideIPVPN	*52.8%*	*53.0%*	300.0%
TunnelBear VPN	74.7%	61.0%	100.0%
Hide.me VPN	75.8%	68.4%	*0.0%*
CyberGhost VPN	77.0%	59.2%	66.7%
Trust.Zone VPN	77.7%	58.5%	325.0%
Private Internet Access	80.7%	76.3%	25.0%
IPVanish VPN	81.0%	78.8%	*0.0%*
TorGuard VPN	81.8%	75.5%	66.7%
NordVPN	82.6%	77.7%	*0.0%*
Buffered VPN	83.3%	78.6%	175.0%

My tests showed that HideIPVPN is the fastest VPN, having the smallest impact on both upload and download speeds. It did, however, have a significant impact on latency. That said, speed shouldn't be the only criteria for choosing a VPN. Value, ease of use, and a commitment to privacy are far more important factors.

OTHER PLATFORMS

NordVPN supports Android, Chrome, Firefox, iOS, Linux, macOS, and Windows. NordVPN's mobile clients allow you to purchase full subscriptions through their respective app stores. Alternatively, some routers can be configured to connect via NordVPN. Doing so supplies coverage for all the devices on your network, including smart home devices that can't run VPNs on their own.

In our testing, NordVPN has performed well on all those platforms. It's an Editors' Choice winner for Android, iOS, Linux, and macOS, in addition to Windows. Note that like all proxy browser plugins, the NordVPN Firefox and Chrome plugins secure only the traffic of those respective browsers.

> It's an Editors' Choice winner for Android, iOS, Linux, and macOS, in addition to Windows.

5-STAR VPN

In my experience, the average person would rather risk having no protection than deal with frustrating security software. That's why NordVPN succeeds: It makes using a security tool simple and doesn't skimp on features. The company offers the largest server collection we've yet seen and also has an excellent stance on user privacy, collecting very little data and operating out of the legal jurisdiction of Panama.

Taken together, these factors are more than enough to justify its comparatively high monthly cost. NordVPN is a smart choice, and it remains a PCMag Editors' Choice, along with Private Internet Access, ProtonVPN, and TunnelBear. Each of these excels in its own way: TunnelBear is friendly and approachable, while ProtonVPN is flexible and technically savvy, and Private Internet Access is robust and affordable. But NordVPN continues to lead the pack.

MAX EDDY