Features that matter more than speed when choosing a VPN

In the race to find the fastest VPN, we forget that besides speed, there are some really important VPN features that you need to consider.

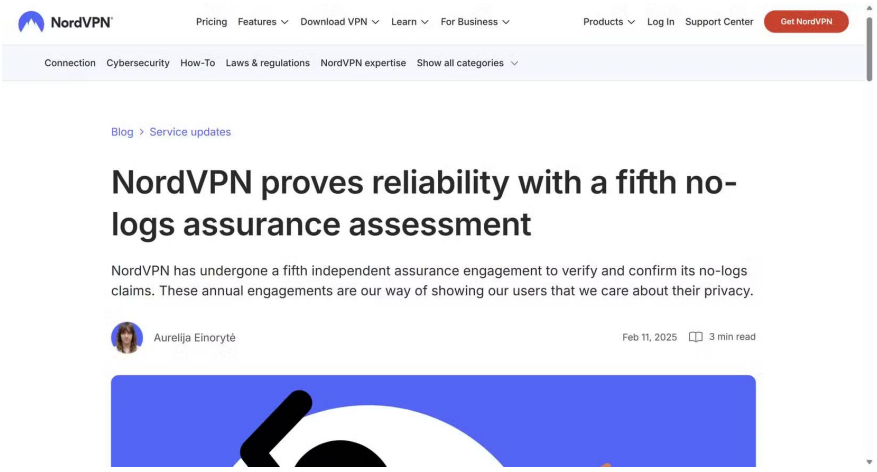
When people talk about VPNs , they often think about speed. The first thing to do when you start a new VPN is almost always a speed test. How fast is the VPN provider, and how does it affect your actual internet speed?

All of that is great, but it doesn't address the real essence of VPNs: privacy. And in the race to find the fastest VPN, we forget that there are some really important VPN features to consider besides speed.

Speed ??is certainly important – but these VPN features are actually even more important.

Independent security audit

No one wants their VPN to be tracked



For years, VPNs relied on the 'Trust me, man' standard. That is, a VPN provider would say they don't log your data, and you basically just accepted that. Companies even plastered 'Strict No Logging Policy' on their homepages, knowing full well that users had no way to actually check.

Then things changed. Multiple cases of VPN providers handing over data to authorities eroded trust in VPNs, and people began to question whether those no-log claims were true.

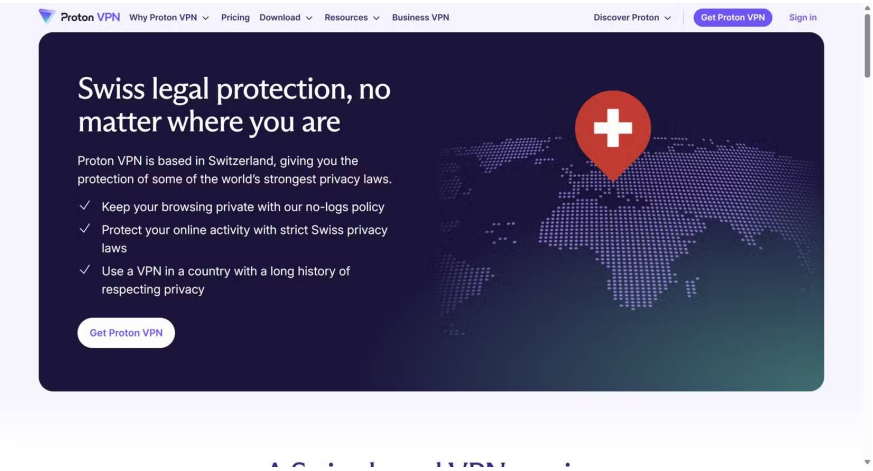
In turn, major VPN services have started hiring third-party auditing firms like PwC, Deloitte, or Cure53 to analyze their infrastructure and confirm whether or not VPNs actually do what they say they do. The flashy 'we're audited and don't log your data' badge has become a selling point for VPNs looking to attract privacy-conscious users.

After all, that's what a VPN is for. Why hand over your privacy to a third party when you don't know if they'll actually do what they say they'll do?

Even then, however, you should be wary of VPNs that claim to be audited. Read the terms carefully to find out what the audit analyzed. Did it perform a full no-logs audit of the company's servers and code? Or was it actually a less in-depth audit? The devil is in the details, and any trustworthy VPN should be happy to show you what it does.

Jurisdiction and ownership

Where is that VPN located?



Along with a comprehensive, audited no-logs policy, you should also check where the VPN is based. Where does the company legally and physically exist, and who actually owns it?

Most users treat a VPN server list like a travel brochure. They see that they can connect to Japan, France, or the UK, and assume that's where the company operates. In reality, VPN providers are bound by the laws of the country where they're headquartered, not where they rent servers. This distinction is the difference between privacy and prison.

You should avoid using VPNs in countries that share intelligence with the 'Five Eyes.' These include the United States, the United Kingdom, Canada, Australia, and New Zealand. Companies in these jurisdictions may be forced to share any data their VPN provider holds about you. However, if you're using a properly audited, no-

logs VPN, there won't be any information to share.

But why take the risk when there are so many VPN providers outside of these locations?

Typically, you want a VPN based somewhere with strong data laws, like Panama or Switzerland. These countries don't have mandatory data retention laws and are generally out of reach of US subpoenas.

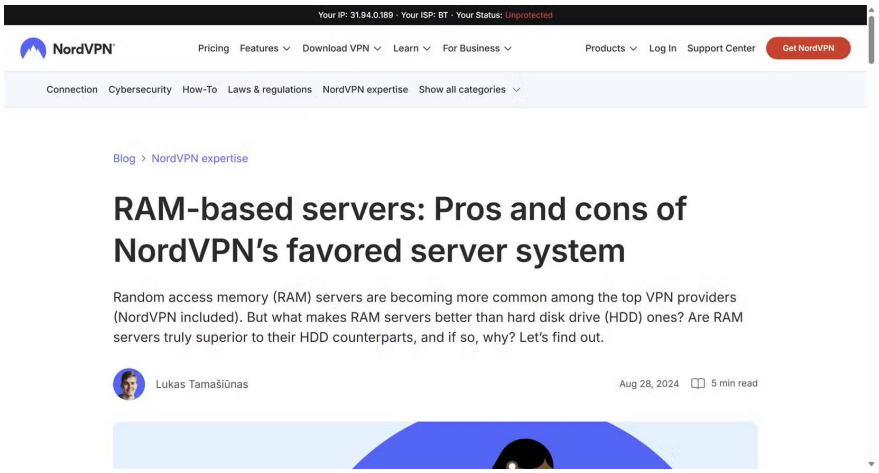
Overlapping ownership

Like most tech companies, over time VPN providers have been bought out by larger corporations, concentrating power and privacy in the hands of a few. It may seem like you're choosing between several different providers, but they may actually be owned by a single company.

For example, Kape Technologies owns ExpressVPN, CyberGhost, Private Internet Access, ZenMate, and Goose VPN, which controls a large portion of the VPN market. The article isn't suggesting that Kape is up to something shady by owning so many VPNs, but it's best to choose an independent provider.

RAM-only server

According to the principles of physics, your data cannot exist



Completing this security trifecta are RAM-only servers. These are VPN servers that don't use traditional disk architecture.

Instead, these servers run entirely on volatile memory (RAM). RAM requires a constant power source to store data. As soon as the power goes out—whether from a system reboot or a panicked administrator pulling the plug during a police raid—every byte of data on that server is instantly erased and cannot be recovered.

This feature is the ultimate failsafe. It ensures that even if a government seizes a physical server rack (which has happened to VPN providers in Türkiye, Iceland, and Ukraine), there will be nothing on the machine to search. It's not just the software that promises to erase your data; it's the physics that ensures your data can't survive without a power source.