TrustedServer

[video narration]

VPNs are critical tools for protecting you online. But not all VPNs protect you equally. Let's take a look at how the innovations of ExpressVPN's TrustedServer technology raise the bar for online privacy and security.

Two major TrustedServer innovations work together to deliver a more secure internet experience:

First, TrustedServer technology ensures that no data can persist on the hard drive, even by accident. It does that by having servers run strictly on RAM only.

Second, TrustedServer technology ensures that all servers load the exact same, up-to-date code when they start up. All software, even the operating system, is freshly run from the latest read-only image each and every time the server is restarted.

Let's take a closer look at how each of these innovations works.

With TrustedServer, ExpressVPN's VPN servers run only on volatile memory, or RAM. Because RAM isn't capable of storing any data when powered off, all information on a server is *completely wiped* every time it's turned off and on again. This minimizes any risk that sensitive information could be compromised.

In the traditional server setup model used by most companies, the operating system requires read/write permissions to the hard drive in order to run applications. Sensitive data stored on a hard drive can be vulnerable to compromise by hackers. If an attacker succeeds in installing a backdoor, this vulnerability may persist indefinitely.

With the TrustedServer setup, ExpressVPN mitigates these risks by preventing the operating system and apps from writing to the hard drive. Instead, the server is run entirely on RAM.

What remains on the hard drive is a cryptographically signed read-only image containing the software needed for the server to boot—nothing else.

By removing write access to the hard drive, TrustedServer prevents both data and potential intruders from persisting on the machine.

Now, let's look at the second major TrustedServer innovation, which is a groundbreaking approach to administering servers. This new method ensures greater consistency, and therefore better security.

You can think of traditional server administration as a game of Tetris. Each piece gets loaded in one at a time–the operating system, the VPN software, security patches, and so on. But when you're loading pieces across thousands of servers, sometimes something unexpected happens. A piece might be misaligned or go missing altogether, creating a security hole. As more time passes, it becomes increasingly difficult to ensure that all servers are running the *exact* software and configuration they should be.

With TrustedServer, instead of being loaded piece by piece, the entire block is loaded at once. And when we need to add a new piece, like a security patch, we just replace the entire block.

In technical terms, the entire software stack, from operating system on up, is loaded fresh from a read-only image every time the server starts up. This gives us confidence that every one of our thousands of servers around the world has the same, most up-to-date software when powered on.

TrustedServer means that we know exactly what's running on each ExpressVPN server—minimizing the risk of vulnerabilities or misconfiguration. With the operating system effectively reinstalled with every single reboot, TrustedServer *dramatically reduces security risks*.

ExpressVPN is proud to lead the VPN industry in redefining what robust privacy and security looks like. With TrustedServer, you can have greater confidence than ever that you're protected online.