6 Reasons Linux Doesn't Need Antivirus or Firewall

While you can still decide to install an antivirus or firewall on Linux (there's nothing wrong with that), here are a few reasons why it might not be as helpful as you think.

Linux is not invulnerable. In fact, it's one of the most common cybersecurity myths that gets Linux users in trouble. This belief makes it easy to let your guard down, and when you're caught off guard, you're more likely to be targeted.

But just because Linux has a security hole doesn't mean you need anti-virus software or a firewall. While you can still decide to install an antivirus or firewall on Linux (there's nothing wrong with that), here are a few reasons why it might not be as helpful as you think.

Why does Linux not need anti-virus software?

Let's see the reasons why you might not need antivirus on Linux.

1. Malware targeting Linux desktops is rare

Since Linux is the least popular desktop operating system, and Linux users tend to be a tech-savvy bunch, plus other operating systems have easier-to-exploit vulnerabilities. , so attacking Linux is simply not as beneficial.

Of course, Linux malware does exist. This is undeniable. However, it's not as big of an issue as it is on other operating systems, and it's unlikely you'll experience it (unless you're watching inappropriate content or torrenting from sites that aren't worth it). trust).

2. Install more secure software on Linux

Think about how you install software on your computer. On Windows and Mac, users typically download EXE, MSI, and DMG installer files that require system-level access to make necessary installation changes. It's the main avenue for malware attacks. Walk a mile wrong Li

But Linux is different. Installer files exist but most users rely solely on package managers like APT and YUM. As long as you maintain the trustworthiness of these repositories, the risk of being attacked by malware is virtually zero. That risk increases when you start reaching out to shady PPAs and the like.

3. Linux can protect itself against malware

The underlying structure of Linux makes it difficult for malware to gain root access, and even if you get infected with a virus or Trojan, it will have a hard time causing any real damage to the system. This is due to the way permissions work in Linux.

Every file in Linux has three permission settings:

1. What can the file owner do with this file?
2. What can the file's owner group do with this file?
3. And what can others do with this file?

If it is assumed that a virus infects your system, that virus will probably be executed in your local account and therefore will be limited to user actions. Local user accounts can't perform any action on the system-level "root" file, so malware is limited (assuming you don't accidentally execute malware with " sudo").

4. Virus removal effectiveness is still a question mark

Suppose one day there is a new piece of malware targeting the Linux desktop. It uses a never-before-seen security exploit and gets into your system. Before you know it, malware wreaks havoc on your data and leaves you wondering what you can do to stop it.

Will anti-virus software help you here? Sure is not.

In general, anti-virus software is always one step behind viruses. It can't protect you from threats it doesn't even recognize exist. Chances are, you'll be hit by malware before the antivirus finds a way to deal with it.

And did you know that anti-virus applications for Linux mainly scan for malware on Windows? Some tools detect infections on Linux, but they mainly clean infected files on Windows so that you don't pass the malware on to your other computers or to friends and family through hacking. file transfer.

5. Smart security habits are usually enough on Linux

Some of the most famous attack vectors on Linux are applications from unknown sources, torrents, phishing sites, etc. best security method.

But those are not the only things. Other potential vectors for malware include outdated PDF files, extensions and plugins, cross-platform apps that aren't regularly updated, etc. USB drives can also carry potential malware.

All this proves that if you eliminate potential attack vectors, avoid shady places on the web, don't touch unknown USB drives, break bad habits and develop security habits well, there won't be much benefit from antivirus software.

Why doesn't Linux need a firewall?

This answer is much more concise.

A firewall is simply a filter that determines what network packets (i.e. data) can enter your computer from the Internet and vice versa. It is mainly used to allow and/or disallow incoming connections. Outgoing connections are rarely filtered.

For most Linux desktop users, a firewall is not necessary.

The only case where you need a firewall is if you are running some kind of server application on your system. This can be a web server, an email server, a game server, etc.

In this case, the firewall restricts incoming connections to certain ports, ensuring that they can only interact with the appropriate host application.

If you are not running any server applications, the firewall has no effect. If no server is running, then your system is not listening for incoming connections and if it is not listening for incoming connections nothing can connect.

Most Linux desktops run no server applications. Again, there's no harm in enabling the firewall on your Linux machine. You don't have to be too extreme. All I'm saying is that you'll probably be fine without an antivirus or firewall on Linux.

Despite all these reasons, you may still want to install antivirus or firewall software on Linux - and that's not a bad thing either. Even if you've never been infected with a single piece of malware, there's no harm in having anti-virus software on hand. Careless, no worries, right? After all, Linux is not as secure as many people think.

Like any other software, there are several antivirus applications on Linux that you can install and try for free.