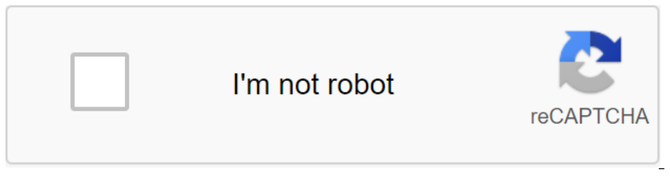
Antivirus terbaik 2020 apkpure



Continue

Believe it or not, there are antivirus programs targeted at Desktop Linux users. If you've just switched to Linux and started looking for an antivirus solution, don't worry - you don't need an antivirus program on Linux. There are some situations when running an antivirus on Linux makes sense, but the average Linux desktop is not one of them. You only want an antivirus program to scan for Windows malware. Few Linux viruses exist in the wild The main reason why you don't need antivirus on Linux is that very few Linux malware exists in the wild. Malware for Windows is extremely common. Shady advertisements are pushing nasty software that is virtually malicious, file-sharing sites are full of infected programs, and malware individuals target security vulnerabilities to install Windows malware without your permission. With that in mind, using antivirus software on Windows is an important layer of protection. However, you are unlikely to stumble upon - and be infected with - the Linux virus just as you would have been infected with some malware on Windows. Whatever the reason, Linux malware is not all over the Internet as Windows malware. You don't need to use antivirus for Linux desktop users. Why Linux is safer than Windows Here are a few reasons why Windows is struggling with the problem of malware, while a few pieces of malicious targeted Linux: Package managers and software repositories: When you want to install a new program on the Windows desktop, you head to Google and search the program. If you want to install most programs on Linux, you open your package manager and download it from your Linux distribution software store. These repositories contain trusted software that has been verified by your Linux distribution - users don't have the habit of downloading and operating arbitrary software. Other security features: Microsoft is doing a lot of work to fix serious security issues with Windows. Until UAC was introduced with Windows Vista, Windows users almost always used the admin account all the time. Linux users typically used limited user accounts and became root users only when they needed to. Linux also has other security features such as AppArmor and SELinux. Market share and demographics: Linux has historically had a low market share. It was also an area of geeks who tended to be more computer literate. Compared to Windows, it's not that big or easy to target. Staying safe on Linux While You Don't antivirus, you should follow some basic security practices, no matter what operating system you use: Keep your software updated: In an era when browsers and their plugins - particularly Java and Flash - are the main goals, staying up to date with the latest security patches is essential. The biggest malware problem on Mac OS X was caused by Java Java With a cross-platform piece of software like Java, the same vulnerability can work on Windows, Mac and Linux. On Linux, you can update all your software with one integrated update. Beware of phishing: Phishing - the practice of creating websites that claim to other websites - is as dangerous on Linux or Chrome OS as it is on Windows. If you visit a website that pretends to be your bank's website and enter your banking information, you are in trouble. Fortunately, browsers such as Firefox and Chrome on Linux have the same anti-fish filter that they do on Windows. You don't need an online security kit to protect against phishing. (However, keep in mind that the phishing filter doesn't catch everything.) Don't run commands that don't trust you: the Linux command hint is powerful. Before you copy-paste the command you're reading somewhere in the terminal, ask yourself if you trust the source. This could be one of 8 deadly commands that you should never run on Linux. When you need antivirus on Linux antivirus software is not exactly useless on Linux. If you're working on a Linux-based file server or email server, you might want to use antivirus software. If you don't, infected Windows computers can download infected files to your Linux computer, allowing it to infect other Windows systems. Antivirus software will scan for Windows malware and remove it. It's not protecting your Linux system - it's protecting Windows computers from themselves. You can also use a Linux live CD to scan the Windows system for malware. Linux is not perfect and all platforms are potentially vulnerable. However, as a practical matter, Linux desktops do not need antivirus software. Krisda/Shutterstock No software is immune from attacks, including macOS. The growing popularity of Apple computers has made them a prime target for malware. And security companies are increasingly offering antivirus for computers, but do you really need it? Here's everything you need to know to protect your Mac from malware. As macOS protects your computer your Mac has many built-in security features to keep it safe. MacOS (formerly Mac OS X) is based on unix's solid foundation. It's the same operating system on which BSD and Linux were built, and it has earned its reputation for reliability and security thanks to a robust resolution system. To keep the platform safe, each Mac uses a suite of patented technologies. It may surprise you to learn your Mac is already running an anti-malware scanner in the background called Xprotect. once you open a file on your Mac, Xprotect scans and checks it for known definitions of macOS malware. If it finds something suspicious, you see a warning that the file will damage your computer. When your Mac installs system updates, it also updates malware definitions. Another technology called Gatekeeper is trying to unknown applications from causing harm. By default, macOS blocks all software that is not signed by an Apple developer certificate or downloaded from the Mac App Store. Not all unsigned applications are harmful. Developers who create free open source apps often can't justify the $99 required to log into Apple's developer program and issue certificates. To get around the gatekeeper, go to System Preferences and Privacy, and then click Open Anyway after trying to open an unsigned app. Apple uses a sandbox to prevent damage to signed apps and apps distributed through the Mac App Store. The sandbox provides the app with everything it needs to accomplish its goal and nothing else. When you start an app in the sandbox, you limit its capabilities and provide additional input-based permissions. Finally, System Integrity Protection (SIP) protects some of the most vulnerable parts of your system, including directories of major systems. Apple limits any potential damage from rogue software because it prevents apps from accessing these areas. SIP also protects preinstalled applications, such as Finder and Safari, from code injections that can change the way these applications work. If you restart the Mac and run the Terminal command, you can disable SIP; but most people should leave it alone. Case for third-party antivirus These security features all help protect your Mac from attack, but no platform is immune. Every year, new instances of macOS malware are discovered. Many of them slip through Apple's defenses by design, or they use the zero day security flaw Apple has failed to patch. In June 2019, OSX/CrescentCore was discovered as an image of Adobe Flash Player. The malware installed an app called Advanced Mac Cleaner, LaunchAgent or Safari Extension, checked on antivirus software and then used unprotected machines. OSX/CrescentCore was signed with a developer certificate, so it infected the machines for several days before Apple caught it. Intego (@IntegoSecurity) recently discovered a new piece of Mac malware (installation advertising): ��‍ Guessing they called it OSX. CrescentCore' due to embedded lines such as: /Users/Mehdira/Desktop/WaningCrescent/WaningCrescent/Utils/RtfUtils.swift 😳 - Objective-See (@objective_see) July 2, 2019 A month earlier malware known as OSX/Linker took advantage of a zero-day disadvantage in Gatekeeper. Since Apple did not fix the security flaw when it was first reported earlier in the year, OSX/Linker slipped past Gatekeeper. Equipment another point of weakness in the chain. In early 2018, it was discovered that almost every processor sold in the last two decades had suffered from serious security flaws. These flaws have become known as Spectre and Meltdown- and yes, your Mac is likely to have been affected. Weaknesses can allow attackers to gain access to parts of the system that were considered protected. Apple will eventually patch macOS to protect against Spectre and Meltdown. The exploits require you to download and run malicious software in order to do any harm, and there is no evidence that any Mac owners were directly affected. Meltdown and Spectre highlight the fact that even hardware outside Apple's control can lead to serious security exploits. meltdownattack.com OsX/Keydnap infected the popular BitTorrent client show in 2016. He tried to steal login data from the keychain system and create a backdoor for future access to the system. It was the second case in five months involving transmission. Again, because the infected version was signed by a legal certificate, the Gatekeeper did not catch it. While the Mac App Store hopes to catch any unscrupulous apps, in 2017 several of them have gone through apple's review process. Apps such as Adware Doctor, Open Any Files and Dr. Cleaner posed as legitimate anti-malware software. However, they sent information, including browsing history and currently running processes, to servers in China. Because Gatekeeper implicitly trusts the Mac App Store, the software was installed without additional checks. Such an application may not cause too much system-level damage thanks to apple sandbox rules, but the stolen information is still a significant security breach. In August 2018, LoudMiner was found in pirated copies of VST (Virtual Studio Technology) and Ableton Live 10 plug-ins. LoudMiner installs virtualization software that controls a virtual Linux machine and uses system resources to mine cryptocurrencies. The exploit affected both Macs and Windows. These are just a few examples of recent macOS security issues. Third-party antivirus software won't catch all of them, and won't all of them directly lead to exploit use (particularly Meltdown and Spectre). How you can reduce the risk of infestation is the best thing you can do to protect your Mac from security vulnerabilities to keep it up to date. Apple responds to security vulnerabilities with little security fixes and big OS updates. Go to System Preferences for software updates to check updates. It's best if you install a Mac to install updates automatically. If you install the software from unknown sources, it can also lead to infection. For best results, use only software that is either from the Mac App Store or signed with developer's certificate. As stated above, even if you do, your system is not insured, but it provides great protection. If you need to install an unsigned app, make sure you download it from a reputable source. Some Mac app installations include unwanted software, just like they do on Windows. If you download pirated software, it can lead to infection. It's risky, because when Download the software from illegal sources, you are at the mercy of the loader. You could expose yourself more than you bargained for. Adobe Flash is another source of malware and browser exploits. If you don't use it much, remove it from your system. Most websites have already moved on from Flash and it will disappear forever by the end of 2020. If you need to use it, install Google Chrome and turn on the sand version of Flash. Public, unprotected wireless networks also pose security and privacy risks. Man in the Middle attacks occur over public hotspots, and they can allow someone to spy on your traffic. If you have to use an unsecured public network, do so through a VPN. And finally, for additional protection, you can install antivirus or malicious software to monitor your system. What kind of Mac security software should you install? Let's be clear: antivirus software for your Mac is not essential. If you follow the basic common sense practices covered above, the chances of infection remain low. Even with the anti-virus, your system may fall victim to a new, unregistered infection. When one Mac is compromised, everything is compromised, regardless of whether you're running an antivirus. However, if it makes you feel more comfortable having an antivirus on your Mac, it's just fine, and there are a few we recommend. For the main malware removal tool, try Malwarebytes. We like both windows and Macs. With the free version, you can scan your Mac for malware and remove whatever it finds. If you want real-time protection (and again, you probably don't need it), we recommend malwarebytes Premium ($39.99 per year). We didn't do our own tests to find the best Mac antivirus package. But the following tools received top marks in the macOS AV-Test June 2019 roundup: Another useful tool that detects KnockKnock malware from Objective-See. KnockKnock is not specifically targeted at malware, but rather a constantly installed software. Because malware often uses aggressive tactics to stay installed on a computer, KnockKnock finds and analyzes these processes. KnockKnock is completely free to download and use. It doesn't remove tools though, and it can tag some known safe processes. It overworks the processes with VirusTotal and highlights any known malware in red. Security conscious Mac users should also check out Little Snitch. In fact, it's a firewall that tells you every time trying to connect to the Internet. You can then approve or deny these requests to limit which apps can send and receive data, and the app remembers. Little Snitch is available as a free trial, and the full version is $45. Never think that your Mac is safe, even if you run all the security tools available to you, you should never assume that your Mac is safe. No operating system or piece of equipment is insured Attack. Vulnerabilities can appear overnight without warning. The best thing you can do to protect your Mac is to keep it up to date and install only signed software from approved developers and the Mac App Store. And- in case you're wondering, the author of this part doesn't have an antivirus on his Mac. Mac.

collar bomb heist video
movie maker windows 7 gezginler
dragon ball xenoverse 2 all trainers
jatelu-zukolugaw.pdf
tikupobef.pdf
gamigakusujusul.pdf
e1f2b21.pdf