Windows, Linux or macOS: Which is the safest operating system?

Overall comparison Windows, Linux and macOS - Which operating system is better secure? Which operating system is the most secure today?

In the previous article, you already know that NSO Group hacking iOS is very simple, or that hackers exploit the 0-day vulnerabilities bought in the black market to help 'professional' hackers attack any device / OS. in a very simple way.

Along with that, countries have viewed the current Internet space as a new battlefield, making security firms / criminal groups even more aggressive in weaponizing their cyber attack tools.

Ironically, most of these legitimate tools are being distributed and used inadvertently or intentionally by hackers or government-sponsored illegal citizen surveillance groups.

Therefore, the concept of an absolutely secure operating system is not possible, only the operating system supports security consolidation in the best overall environment.

We call together the open source operating systems developed from Linux as an OS: Calling Linux for easy comparison with the other two operating systems, which are: Windows and macOS.

In this article, I objectively evaluate between the OSs together (the latest version) based on specific security criteria to ensure fairness, not for the purpose of advertising for this or that. .

Because of course, macOS users don't like anyone who criticizes the macOS operating system they are using, and Windows and Linux too.

You should remember that more than 80% of network attacks are 'social engineering / human attacks' rather than attacks on the operating system, thus forcing us to judge based on technical components with specialized terms, hope you actively Google about them!

1. Built-in antivirus

Windows Defender is too familiar to Windows 10 users, and most Vietnamese users often do not have the habit of buying copyrighted software to use.

Especially when Windows has built-in Windows Defender - a free anti-virus software that is quite effective, there is no reason to buy more 3rd-party antivirus software.

Famous Internet Security Virus removal programs such as Kaspersky, Bitdefender, ESET, . have a preliminary license price of 300 - 500k. A pretty expensive price compared to our average income.

	Antivirus Software	# Reviews Rating (1-5)	# Licenses	Best Price
	Kaspersky	579 Reviews 4.0 Stars	3 Licenses	$24.90
	Bitdefender	88 Reviews 3.0 Stars	3 Licenses	$59.99
	Norton 360	1,327 Reviews 4.0 Stars	3 Licenses	$39.00
	BullGuard Premium	2 Reviews 3.0 Stars	1 Licenses	$65.18
	AVG Antivirus	29 Reviews 3.5 Stars	3 Licenses	$35.26
	ESET NOD32	22 Reviews	3 Licenses	$38.88

	Antivirus Software	# Reviews Rating (1-5)	# Licenses	Best Price
	Kaspersky	579 Reviews 4.0 Stars	3 Licenses	$24.90
	Bitdefender	88 Reviews 3.0 Stars	3 Licenses	$59.99
	Norton 360	1,327 Reviews 4.0 Stars	3 Licenses	$39.00
	BullGuard Premium	2 Reviews 3.0 Stars	1 Licenses	$65.18
	AVG Antivirus	29 Reviews 3.5 Stars	3 Licenses	$35.26
	ESET NOD32	22 Reviews	3 Licenses	$38.88

Although with very basic virus detection and removal technologies: Signature inspecting, YARA rule matching, Repucation Checking, but thanks to Windows Defender proactively checking, as well as the wider range of activities on Windows makes it more effective than the 3 macOS: Gatekeeper, XProtect, Malware Removal Tool.

Linux-based operating systems often do not have an antivirus built in, I only know ClamAV, but the last time I used it, I found that the way to configure and launch it was very manual, it was difficult for ordinary users to use it. proficient.

=> This section Windows dominates!

2. Sandboxing: Run the program in an independent environment

This concept lies deep in the operating system, the user does not have to install or modify anything, simply put, this is the operating system's ability to isolate the processes / programs that are launched in a multitasking environment.

The general spirit is which program uses the resources (RAM, CPU, .) of this program, especially to prevent repairing system files.

Even browsers like Chrome, Firefox, . all have their own sandbox for websites / tabs that users visit, so if there are malicious JavaScript codes running in that tab, you can not do much about the operating system, The principle of 'sandbox' is so!

Windows and macOS both 'sandbox / isolate' apps installed from the Microsoft Store / App Store, but if the user downloads files from the Internet and then installs them themselves, this problem is difficult to control.

Linux is superior with SELinux and AppArmor to help 'sandbox' programs proactively / passively quickly, especially when you have root / admin rights on your computer.

=> This section gives Linux one point!

3. Codesigning: Digital signature, identity verification

This is an authentication technique that ensures the program you install on your computer is exactly the same as its publisher, and that the installer / executable file has not been modified or injected with malicious code.

The principle is that when releasing the software, the developer attaches the digital signature and identity information, as well as a way to check the integrity of the installer (itegrity checking).

You can rest assured that thanks to modern encryption and public authentication technologies, it is very difficult to forge the above credentials - if not impossible, learn more about PKI, Hash, and code. turned AES, . to see if I said it right or not.

On MacOS or Windows, there is a codeigning class process: from the start of the installation to the time the application is opened. Meanwhile, Linux, up to now, has not been equipped with this process completely.

You can imagine a slightly changed setup file (file setup) in the input address could cause the user to lose an important account like playing, so the OS without codesigning is very unsafe. !

=> In this section, MacOS and Windows each one more points!

4. System Protection: OS level protection

Want to have a safe OS (operating system) not only depends on each user, but the OS itself must have mechanisms to prevent malware / viruses specialized in sabotage or located in the OS such as Rootkits.

In this clause, macOS does very well with Apple System Integrity Protection (SIP), inheriting the mechanism from Linux, but especially with macOS, users cannot arbitrarily adjust or disable this component, even if they have root / power user rights.

Windows has Trusted Boot and Secure Boot to protect the operating system before other security software starts working.

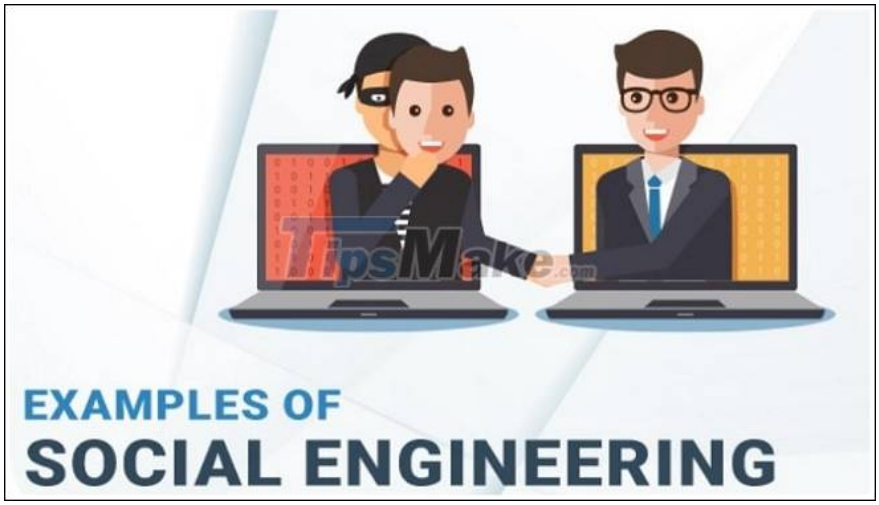
But security experts rate Apple SIP higher than the two components above of Windows.

=> In this section, macOS wins 1 more point, Windows is trying hard to receive 0.5 bonus points

5. Conclusion

From a technical perspective, all 3 operating systems have all the basic security features, one OS has self-developed, the other OS also has or is working on an equivalent protection component.

The secure operating system is not only based on the company itself: Microsoft, Apple, RedHat, . but also the overall story where users are at the center.



Good OS, good anti-virus software, but most likely users were tricked into turning them off, or users running cross-platform emulators themselves that caused macOS to get virus on Windows (to some extent) and then again. blame macOS for insecurity, .

In general, we are finding the most comprehensive operating system, rather, I choose Windows 10 because of the rich number of applications, games, hardware compatibility very well.

I use it carefully so until now I still do not see what Windows "less-secure" is like, although I still forgot to pay ESET Internet Security license fees ^^!

How about your opinion?

You finished reading the article "**Windows, Linux or macOS: Which is the safest operating system?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
