Which is More Secure: Windows, Linux, or macOS?

February 21, 2019
by SentinelOne

When admins go to battle over which operating system is the most secure, it's time to turn to our guide on endpoint security. The real answer is here!

their money. It is reasonably competent at detecting commodity malware through the use of signatures, YARA rules and reputation checks, although it will not protect the enterprise against more advanced attacks, and it is also subject to various PowerShell bypasses. Despite that, it's a lot better than Apple's rudimentary trio of application security technologies, Gatekeeper, XProtect and Malware Removal Tool. Linux doesn't come with any built-in AV, although there are free packages like ClamAV available for it, just as there are for the other platforms. Round 1 to Windows then.

Sandboxing

A sandbox is a closed or jailed environment in which a process is executed. The beauty of sandboxes is they protect the rest of your computer from untrusted processes, as the sandbox effectively prevents the process from reading and writing to other files, interacting with other processes or changing system settings. This is especially important for web browsers that can run JavaScripts. If a malicious script on a website can break out of the browser's sandbox, it could infect the rest of the computer.

Windows and macOS both sandbox apps installed from their own App Stores by default, but there's nothing to stop apps installed from other sources from running uncontained. Linux has a wealth of options to sandbox any process, so long as you're something of a power user. SELinux and AppArmor are readily available on major distros, and this might explain why some Linux users believe Linux is more secure than Windows and macOS. One on the scoresheet for Linux systems.

Codesigning

Codesigning is an authentication technology that ensures that an application or process has come from the source it says it has come from. In addition, codesigning ensures that the executable, package or bundle has not been tampered with since it was digitally signed.

Windows, Linux and macOS all make use of codesigning to some degree, though all platforms ship with some unsigned code, too. The problem with unsigned code is that bad actors can replace a binary with their own or inject malicious code directly into an unsigned, running process.

On Macs and Windows machines, codesigning checks are made not just on installation but also on first run of the application. This extra security is missing on Linux boxes. No clear winner, but arguably Linux is lagging behind the other two on this one.

System Protection

You want an OS with protection from rootkits and malware that tries to modify or replace the core system utilities, and in this category macOS comes out on top. Apple's System Integrity Protection (SIP) is built-in and entirely transparent to the user. The effect of this is that even root cannot change some things – a situation many Linux power users would find intolerable, but which is a great defence against certain kinds of malware behaviors. Windows has secure boot and trusted boot to protect the system prior to any AV solution kicking in, but these are not even close to being as solid as Apple's SIP and the additional secure enclave that exists on touchbar-equipped Macs.

The Popular (and Wrong) Arguments

As can be seen, there's some variance in the main security features offered by each OS, but overall none is a standout winner or loser when it comes to features. Even so, adherents of one platform or another tend to have a favorite argument or two to back up their position. Let's take a look at these and see how convincing they are.

1. Windows is the Least Secure Because of its Install Base

There's no doubt that Windows is the most targeted of all the operating systems simply because the size of the install base makes it the most efficient to attack. If you're writing malware that can run on 88% of the machines being used in the enterprise, you're much more likely to achieve a compromise. While that's statistically true, that doesn't mean Windows is inherently less secure than other OSs. One could just as equally argue that the popularity of Windows means Microsoft have the most experience of defending against malware attacks. The real point here is that there's more malware aimed at Windows, and that means you definitely need a good endpoint security solution, but that turns out to be true regardless of which OS you're running.

2. Linux is the Most Secure Because it's Open Source

We see people arguing this all the time. The many eyes theory of security is patently flawed. As SentinelOne researcher Dor Dankner recently showed, Linux has a little-recognised privilege escalation vulnerability that was introduced to the Linux kernel in 2004. Despite the code having been reviewed, nothing was done to ameliorate it. Likewise, openssl contained the Heartbleed bug for over two years before eventually being discovered.

3. macOS is the Most Secure Because Apple!

Apple have done well to position themselves in the minds of the public as being "security conscious", in large part thanks to the closed nature of their mobile platform, iOS, and some very public battles with the FBI about security and privacy. It's not clear how far this perception extends towards macOS, though. Apple's marketing certainly makes a big deal of security being "built in", but the truth is that Mac security features like Gatekeeper, XProtect, and MRT are easily defeasible and not particularly comprehensive. Again, one could argue that having less experience in defending against malware, Apple are not as well-schooled as Microsoft in the art of building a hardened OS.

4. Linux is the Most Secure Because it's Highly Configurable

It's true that something like SELinux probably has more ways to 'harden' the system than macOS or Windows, but very few enterprises are going to be able to deploy a locked down SELinux install as the desktop OS of choice for their staff, at least not if they want to get any useful work done. It's rather like saying a vault with no door is the safest vault money can buy. Sure it is, but it's also practically useless. Security and usability go hand-in-hand, and users will often make less secure decisions if they have to fight against the OS just to get their work done.

Security isn't a Feature of Your OS

Given that there's neither an overall blend of technologies nor any knock-down argument that establishes one OS as "more secure" than the others, what is the best way to answer the question?

Despite what some OS vendors claim, security is not a feature you can build in to an operating system for the simple reason that security isn't a commodity that you can "add" or "take away". While features like codesigning, sandboxing and system protection are all part of a good security posture, enterprise security is ultimately a practice or set of practices that need to be in your organizational DNA.

Businesses need not only OSs with security features, they need integrated security software solutions and employees who follow security best practices. It's no use having a system policy that prevents the execution of untrusted software if a local user can be convinced – and has the ability – to simply override it.

The truth of the matter is that regardless of which platform your admins prefer, every OS has its vulnerabilities and it's likely that your network contains a mixture of operating systems and a mixture of vulnerabilities. With over 80% of pentesters, hackers and hacktivists saying that they leverage social engineering in cyber attacks, it's clear that choice of OS is really not that significant.

What is most important is that you have solid endpoint security with automated detection and prevention capabilities across your entire fleet, regardless of OS. You also need visibility across your network in order to identify and search for attack indicators. With a single agent solution like SentinelOne that protects Linux, macOS and Windows alike, it really shouldn't matter what your admins personally prefer to use, or which they claim is the most secure.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Evaluating Endpoint Security Products: 15 Dumb Mistakes to Avoid
- The Enemy Within – Top 7 Most Disturbing Data Breaches in 2018
- 5 Ways a CISO Can Tackle the CyberSecurity Skills Shortage Now
- How Malware Can Easily Defeat Apple's macOS Security

Company

Our Customers
Why SentinelOne
Platform
About
Partners
Support
Jobs
Legal
Security & Compliance
Contact Us

Resources

Blog
Labs
Press
News
Resources

Global Headquarters

605 Fairchild Dr.
Mountain View, CA 94043

+1-855-868-3733

sales@sentinelone.com

Sign Up For Our Newsletter

Business Email >

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Policy. SentinelOne will not sell, trade, lease, or rent your personal data to third parties.

Privacy Policy Terms of Service