# IS WINDOWS DEFENDER GOOD ENOUGH?

Windows 10 won't hassle you to install an antivirus program like Windows 7 did. Windows now includes a built-in free antivirus called Windows Defender. But is it really the best for protecting your PC–or even just good enough?

Windows Defender was originally known as Microsoft Security Essentials back in the Windows 7 days when it was offered as a separate download, but now it's built right into Windows and it's enabled by default. Many people have been convinced to believe that you should always install a third-party antivirus, but that isn't the best solution for today's security problems, like ransomware.

### What's the Best Antivirus?

What you need is a great team: Malwarebytes + Windows Defender. To keep your system secure:

- **Use the Built-in Windows Defender for traditional antivirus** – the criminals have moved on from regular viruses to focus on Ransomware, zero-day attacks, and even worse malware that traditional antivirus just can't handle. Windows Defender is built right into the operating system, blazing fast, doesn't annoy you, and does its job cleaning old-school viruses.
- **Use Malwarebytes for Anti-Malware and Anti-Exploit** – all of the huge malware outbreaks these days are using zero-day flaws in your browser to install ransomware to take over your PC, and only Malwarebytes provides really excellent protection against this with its unique anti-exploit system. There's no bloatware and it won't slow you down.

### Is Windows Defender Good Enough?

Windows Defender automatically scans programs you open, downloads new definitions from Windows Update, and provides an application you can use for in-depth scans. Best of all, it doesn't slow down your system, and mostly stays out of your way—which can't be said about most other antivirus programs.

For a short while, Microsoft's antivirus fell behind the others when it came to comparative antivirus software tests—way behind. It was bad enough that most experts recommended something else, but it's since bounced back, and now provides very good protection.

So in short, yes: Windows Defender is good enough (as long as you couple it with a good anti-malware program, as was mentioned above.)

Windows Defender caught 99.9% of the "widespread and prevalent malware" in April 2017, along with 98.8% percent of the zero-day attacks.

Furthermore, security is about more than raw protection scores. Other antivirus programs may occasionally do a bit better in monthly tests, but they also come with a lot of **bloat**, like **browser extensions** that actually make you less safe, **registry cleaners** that are terrible and unnecessary, **loads of unsafe junkware**, and even the ability to track your browsing habits so they can make money. Furthermore, the way they hook themselves into your browser and operating system often causes more problems than it solves. Something that protects you against viruses but opens you up to other vectors of attack is *not* good security.

Windows Defender does not do any of these things—it does one thing well, for free, and without getting in your way. Plus, Windows 10 already includes the various other protections, like the SmartScreen filter that should prevent you from downloading and running malware, whatever antivirus you use.

**Antivirus Isn't Enough: Use Malwarebytes, Too**

Antivirus is important, but these days, it's more important that you use a good anti-exploit program to protect your web browser and plug-ins, which are the most targeted by attackers.

Unlike traditional antivirus programs, Malwarebytes is good at finding "potentially unwanted programs" (PUPs) and other junkware. It also contains an anti-exploit feature, which aims to block common exploits in programs, even if they are zero-day attacks that have never been seen before. It also contains anti-ransomware, to block extortion attacks. The latest version of Malwarebytes combines these three tools into one easy-to-use package for $40 per year.

Malwarebytes (hyperlink) claims to be able to replace your traditional antivirus entirely, but most experts disagree. It uses completely different strategies for protecting you: antivirus will block or quarantine harmful programs that find their way to your computer, while Malwarebytes attempts to stop harmful software from ever reaching your computer in the first place. Since it doesn't interfere with traditional antivirus programs, you should consider running *both* programs for the best protection.

Note that you can get some of Malwarebytes' features for free, but with caveats. For example, the free version of Malwarebytes program will only scan for malware and PUPs on-demand—it won't scan in the background like the premium version does. In addition, it doesn't contain the anti-exploit or anti-ransomware features of the premium version.