Why you don’t need another Antivirus

Many PC users have become accustomed to paying for antivirus software, and for a good reason, Microsoft’s antivirus offered minimal protection and the free third-party alternatives were not up to the task. Back in 2013, Microsoft Defender was so bad that antivirus testing agencies used it as the baseline for junk-lever performance.

But in the years that passed, Microsoft ramped up its efforts in endpoint security, and in 2019 Windows Defender was built-in with Windows 10. Since then, Windows Defender has been the gold standard for antivirus programs, often outperforming paid services.

How do they compare?

Two of the biggest testing houses, AV-comparatives and AV-tests, rank Windows Defender among the best both labs have tested. Out of all sixteen products tested, Microsoft Defender was one of four vendors that blocked all malware on its system.

In this June 2019 Antivirus group test, AV-test ranked Windows Defender as a top-product. Defender ranked 6 out of 6, catching every piece of malware the agency tested while reporting zero false positives.

A snapshot of the AV-test June 2019 roundup: (next page...)

BitDentify

AV-TEST

Producer	Version	Protection	Performance	Usability
Windows Defender	4.18	6	6	6
AhnLab V3 Internet Security	9.0	4	6	6
Avast Fre AntiVirus	19.5	5.5	6	6
AVG Internet Security	19.5	5.5	6	6
Avira Antivirus Pro	15.0	5.5	5.5	6
Bitdefender Internet Security	23.0	5.5	6	6
Bullguard Internet Security	19.0	4.5	5.5	6
Comodo Internet Security Premium	12.0	4.5	4	5.5
F-Secure SAFE	17.0	6	6	6
GDATA Internet Security	25.5	5.5	5.5	5.5
K7 Total Security	15.1	5.5	5.5	5.5
Kaspersky Internet Security	19.0	6	6	6
Malwarebytes Premium	3.7.1	2	5	6

McAfee Internet Security	22.3	5	6	6
eScan Internet Security Suite	14.0	4.5	6	6
Norton Security	22.17	6	6	6
PC Matic	3.0	4.5	6	3.5
Trend Micro Internet Security	15.0	6	5.5	6
VIPRE AdvancedSecurity	11.0	5.5	6	6
Webroot SecureAnywhere	9.0	2	5.5	4

Windows Defender also gets perfect scores on performance; this is important since a lot of antivirus programs tend to slow down your computer while looking for threats. With Defender being built right into Windows 10, it's performance is better than third-party antivirus solutions.

The problems with free Antivirus

- **Antivirus programs have Administrator privileges**

  Antivirus programs always operate with high access privileges.
  This means that to find viruses, they need to be able to access everything on the computer, just like a computer administrator. That is what makes them especially dangerous when they don't function as intended, and a coding error could lead to a non-functioning computer or even opening the doors for a hacker.

- **Free antivirus want to keep you afraid**

  Most free antivirus programs operate on the same principle; fear. Once installed, the program will keep annoying the user with popups about new threats, trying to get the user to install additional tools or pay for their premium protection.

- **Free antivirus is financed with ads**

  To provide free services, many free antivirus tools come with ads. Some of them install third-party applications in your browser, such as toolbars or "internet security" plugins that serve you ads while browsing. Some of them even change your default search engine or home screen to serve ads.

- **Free antivirus can steal your data**

  The free antivirus solution by Avast was recently caught stealing data about their customers and selling it for profit, all without consent. Browsing history from over 100 million devices was sold trough a subsidiary called Jumpshot, since the news broke Avast terminated Jumpshot data collection business.

- **Free antivirus is not as effective**

  All antivirus solutions depend on frequently updated malware/virus-signature files; it's these files that tell the program what to look for. Free antivirus solutions tend to have less-frequently updated signature files than their paid counterparts. The free versions also tend to provide slightly less performance when scanning for viruses.

- **Free antivirus can be a open door for hackers**

  A poorly programmed antivirus made with a lack of good security practices can open up gaping security holes on millions of computers. Googles Project Zero security research team disclosed a major vulnerability in security product by Symantec.
  Panda recently had a mishap both in its free and paid antivirus, which made the program delete important system files from the user's computer, leaving it inoperable if rebooted.

But I still “feel” more secure with another Antivirus

Adding another antivirus program to your system should not be necessary but in theory, it will give you some extra protection, and it might make you feel more secure.

Running two antivirus programs was, historically, considered a bad idea, but with Windows 10 this is no longer an issue. You can configure Defender to run alongside your third-party solution of choice:

(Go to Settings > Update & Security > Windows Security, then click on Virus and threat protection. Scroll down to Windows Defender Antivirus options and make sure periodic scanning is toggled on.)

As for what third-party antivirus you should choose, we would recommend Bitdefender since it’s very unobtrusive and was top ranked by AV-tests. Once you’ve installed it you will forget it’s there, as you should with a good antivirus.

So what should I do?

1. Uninstall all other antivirus & internet security applications (especially Avast).

   (1.2. Optional) Install Bitdefender.

2. Restart your computer.

3. **Don’t worry so much.**