Besides Windows Defender, should users install other anti-virus and anti-malware software?

In addition to anti-virus software, security experts recommend that users use additional tools to detect and block malware, adware, spyware, adware.

Once Windows 10 is installed, users can use Microsoft's built-in antivirus software, Windows Defender. Accordingly, Windows Defender will automatically scan the programs you open, and at the same time allow users to deeply scan the entire system. The software also constantly automatically updates data about new viruses through the Windows Update feature.

However, the biggest plus of Windows Defender comes from the fact that this anti-virus software does not slow down your system - something some other anti-virus software does not usually do.

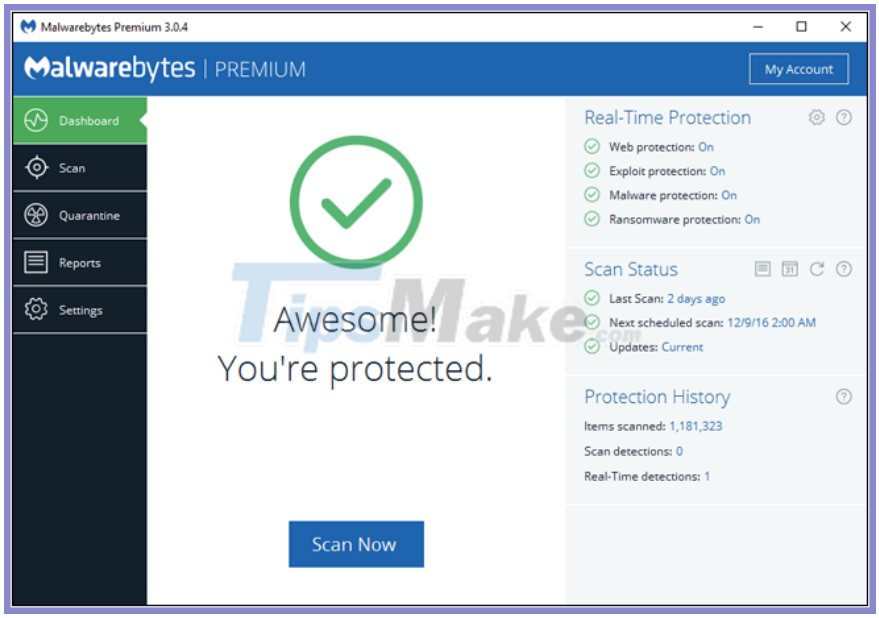
In general, according to security experts, Windows Defender possesses good enough protection with a free software, and is not too inferior to today's top anti-virus software. . In fact, in an April 2017 review by security firm AV-TEST, Windows Defender detected 99.9% of "common malware", along with 98.8% of zero attacks. - day.

Of course, if you hate Windows Defender for some reason and want to use another antivirus, you can use the top antivirus software from Bitdefender, Norton, Trend Micro or Kaspersky. The free versions of these software are all quite effective. However, if you want to use the full features, you will have to pay a large amount for monthly usage fees / year.

Just using anti-virus software is not enough

Using anti-virus programs is of course essential, but not enough if you want to keep your teeth safe!

Today, security experts recommend that users use additional tools to detect and block malware, adware, spyware, and adware. Among the tools available on the market, Malwarebytes is the software most appreciated by security experts.



Accordingly, unlike traditional anti-virus software, Malwarebytes is "good" at finding "potentially unwanted programs" (PUPs) and other junkware. Since version 3.0, Malwarebytes also integrates with Anti-Exploit (anti-exploit) feature.

This feature helps to block exploits of software vulnerabilities, including unprecedented Zero-day attacks. Besides, Malwarebytes also integrates anti-ransomware, to block ransomware like CryptoLocker.

It should be added that while Malwarebytes claims to be able to completely replace traditional antivirus software, many security experts disagree with this claim.

Specifically, Malwarebytes and anti-virus software use different protection strategies: anti-virus software blocks or quarantines harmful programs that find their way to your computer, while Malwarebytes tries to stop them. Malware hits your computer in the first place. Since Malwarebytes does not conflict with traditional anti-virus programs, users should run both programs for the best protection.

In case you want to run both Windows Defender and Malwarebytes, users need to go to Settings, click on the "Security" tab and turn off the option "Always register Malwarebytes in the Windows Security Center". When this option is disabled, Malwarebytes will not register itself as the system's default security application, and both Malwarebytes and Windows Defender will run at the same time.

Currently, users will have to spend about 3.33 USD for a month to use Malwarebytes on 1 device. However, you can also use the free version of Malwarebytes, which has integrated Scan and Quarantine (quarantine) functions of malicious files or software.