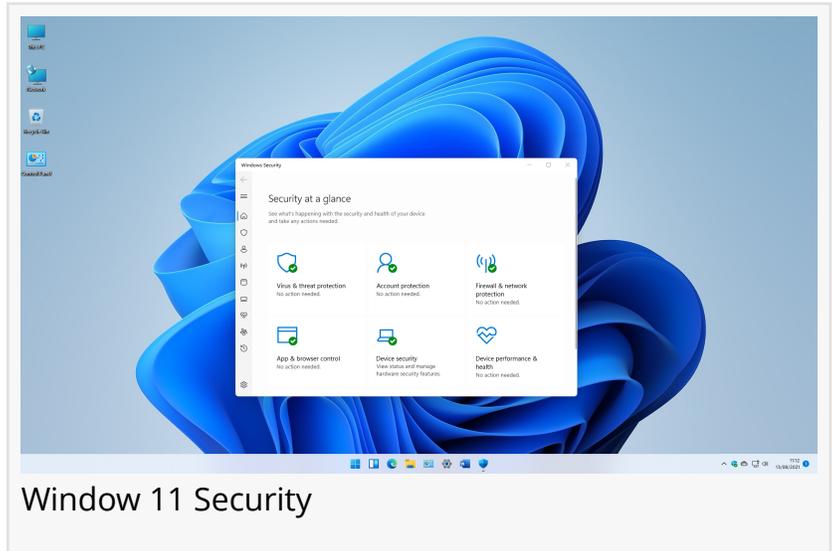


AV-Comparatives checks the interaction of Windows 11 and Internet Security Suites

AV-Comparatives has taken a look at how the new operating system will affect security for the average PC user.

INNSBRUCK, TIROL, AUSTRIA, August 15, 2021 /EINPresswire.com/ -- In June 2021, Microsoft announced that it is to release a new version of [Windows](#) for PCs, Windows 11, later this year. Aside from new features and an updated user interface, Microsoft is promoting the new security measures in Windows 11. We have taken a look at how the new operating system will affect security for the average PC user.



Window 11 Security

Which PCs can run Windows 11?

“

We are already running a preliminary AV-test with Windows 11 to check for compatibility issues. We will release an update soon.”

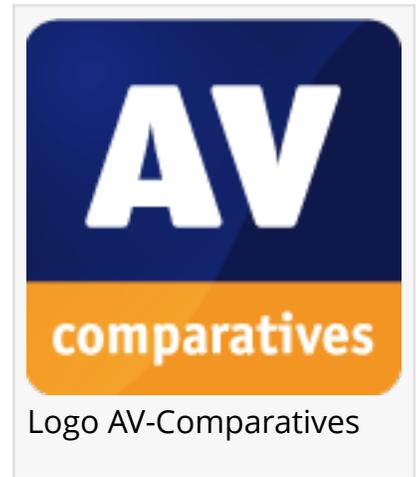
Peter Stelzhammer, co-founder, AV-Comparatives

One of the most controversial aspects of the new Windows version is the hardware requirements. As well as increased memory (RAM) and disk space, the release version of Windows 11 will need specific hardware-based security features to be present in the PC. These include a TPM (Trusted Platform Module) version 2.0 chip, and a recent processor with VBS (virtualization-based security) and HVCI (hypervisor-protected code integrity). UEFI firmware with the Secure Boot feature enabled is also necessary if you want to install Windows 11.

Current preview versions of Windows 11 do not enforce these requirements quite so strictly, meaning that it is possible to install them on some systems that will not be able to run the final version. However, it appears that the TPM 2.0 chip is essential to install even one of the preview builds.

Why is Microsoft doing this?

A recent blog post by David Weston, Director of Enterprise and OS Security at Microsoft, gives details of the security-related hardware requirements in Windows 11, and explains why they are necessary. Another Microsoft blog post aimed at Windows Insiders states that the hardware-based security measures demanded by Windows 11 can prevent 60% of malware attacks, according to their research. The net result of Microsoft's hardware policy for the new operating system is that a majority of PCs currently running Windows 10 will not be able to upgrade to Windows 11 by any means, including a clean install. Needless to say, this has not gone down well with the many users whose current Windows 10 machines will not be eligible for the upgrade.



Is Microsoft justified in strictly defining which PCs can run Windows 11? Well, there's no arguing with David Weston that the hardware security features he describes do make a real difference to computer security. Some people have argued that many older processors, not on Microsoft's current Windows 11 hardware compatibility list, do in fact already have all of the security features required. However, Microsoft has taken note of this and is considering adding some slightly older CPUs to the Windows 11 compatibility list.

Will upgrading to Windows 11 make my PC more secure?

The answer is not as simple as you might think. A recent ZDNet blog post by Jason Perlow states that Windows 10 version 20H2, released the best part of a year ago, is already able to use the hardware security features just as well as Windows 11 will. You might need to enable them manually, by going to the Device Security tab of the Windows Security window, whereas in Windows 11 they will be activated by default. Still, this means that if your Windows 10 PC is up to date and has the hardware security features needed for Windows 11, these can already be used just as effectively as if you had installed the newer Windows version.

The best answer to the question "Will Windows 11 be more secure than Windows 10?" is thus "Yes and No". A PC with modern hardware security features is more secure than a PC without them, but if your PC has these features, you can take advantage of them with a recent version of Windows 10. However, new security features in Windows 11 are not limited to support for the relevant hardware. For example, the new OS will include "Windows Hello for Business", which enables password-free sign-on in enterprise environments. For business customers at least, this is a security feature that's unique to Windows 11. But for many home users, simply upgrading from an up-to-date Windows 10 to Windows 11 might well not be a game-changer, security-wise.

What about antivirus software for Windows 11?

Of course, for all of us here at [AV-Comparatives](#), the subject of malware protection software for Windows 11 is particularly important. We are already running a preliminary AV-test with the new operating system to check for compatibility issues. Windows 11 is expected to come with

Microsoft's built-in anti-malware software, Windows Defender Antivirus. Of course, many people prefer to use a third-party security program – that's why AV-Comparatives exists. Initial testing with popular consumer AV products on preview versions of Windows 11 indicates that these will work just as well on the new platform as they did on earlier ones. Of course, if you try out beta releases of any software you do so at your own risk, especially where security issues are concerned. So, if you're running a preview version of Windows 11, don't rely on any antivirus, Microsoft or otherwise, to protect any mission-critical data.

If you do install a third-party antivirus program on a Windows 11 preview version, you will probably find one tiny change under the new OS. Most AV applications add their own scan entries to the Windows Explorer context menu (this is the menu shown when you right-click on a drive, folder or file in File Explorer or on the Windows Desktop). Along with a whole host of Microsoft menu items, the antivirus scan entries have migrated to the "overflow", and can be accessed by clicking "Show more options".

Of course, there is plenty of time between now and the final release of Windows 11 for things to change, so not every program that works on preview builds will necessarily run perfectly on the RTM (release to manufacturing) version. In any event, we will keep you updated with further Windows 11 security news as it arises. Please check www.av-comparatives.org for our latest news.

AV-Comparatives is an independent testing lab based in Innsbruck, Austria, and has been publicly testing computer security software since 2004. It is ISO 9001:2015 certified for the scope "Independent Tests of Anti-Virus Software". It also holds the EICAR certification as a "Trusted IT-Security Testing Lab".

SOURCES

<https://www.microsoft.com/security/blog/2021/06/25/windows-11-enables-security-by-design-from-the-chip-to-the-cloud/>

<https://blogs.windows.com/windows-insider/2021/06/28/update-on-windows-11-minimum-system-requirements/>

<https://www.zdnet.com/article/windows-11-has-advanced-hardware-security-heres-how-to-get-it-in-windows-10-today/>

Peter Stelzhammer

AV-Comparatives

+43 720 115542

media@av-comparatives.org

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/548776819>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.