# Microsoft explains why Windows 11 requires TPM 2.0

The minimum requirements to install Windows 11 have made TPM 2.0 the focus. While TPM 2.0 has been on PCs for years, it wasn't until this week that the technology became widely known.

Accordingly, David Weston, Microsoft's OS Security Manager, explains the importance of TPM 2.0. Besides, he also mentioned some other security benefits of Windows 11.

"All tested Windows 11 systems will come with a TPM 2.0 chip to ensure customers can benefit from security backed by hardware root of trust," Weston said.

TPM is a chip that is integrated with the motherboard on the PC or added to the CPU. TPM not only helps protect user data, credentials, and encryption keys, but also protects PCs from malware and ransomware attacks, which are becoming increasingly common.

Specifically, according to Weston, TPM 2.0 is a key element in providing security for Windows Hello and BitLocker to help customers better protect their identities and personal data.


According to him, Azure Attestation is also supported in Windows 11. This allows anyone to enforce Zero Trust policies with supported mobile device management features.

In addition, Windows supports virtualization-based security, built-in Secure Boot, and Hardware-enforced Stack Protection for hardware provided by Intel and AMD.

Suffice to say, his explanations for security professionals and those interested in device security are interesting. However, for others, they see the reason that Windows 11 requires TPM 2.0 is not arbitrary.

It should be noted that, for Windows 11, the minimum requirements for soft floor and hard floor are different. People can still run Windows 11 on devices with TPM 1.2 chip, but we still need to wait for more specific information.

Mr. Weston played a significant role in Microsoft's security, including launching secure core PCs and spending $1 billion a year on security.