# Microsoft announced a standard for Windows 10 security

Microsoft has just released a new standard for Windows 10 devices to be safe. These standards include hardware that must have the same software requirements.

Microsoft has just released a new standard for **Windows 10** devices to be safe. These standards include hardware that must have the same software requirements.

## Hardware standards

Hardware standards are divided into 6 categories: microprocessor generation, architecture of microprocessor, virtualization, microchip TPM (Trusted Platform Modules), boot and RAM authentication.

**Microprocessor:** Microsoft recommends the use of 7th-generation Intel & AMD processors. When asked why, the chief of Windows Offensive Security Team and Windows Device Security Dave Weston said that 7th-generation CPUs contain MBEC. (Mode based execution control - temporarily translated as mode control implementation), provides a more secure kernel.

**Processor architecture** : should be 64-bit for Windows to take advantage of VBS - Virtualizatoin-based security (virtualization security), use Windows virtual machine. This virtual machine only supports 64-bit processors.

**Virtualization** : is an important element of the Windows Security framework. Windows 10 devices that want high security should support Intel VT-d, AMD-Vi or ARM64 SMMU to take advantage of the IOMMD virtualization management unit (Input-Outpur Memory Management Unit). To use SLAT (Second Layer Address Translation), the processor needs to support Intel Vt-x with EPT (Extended Page Tables) or AMD-v with RVI (Rapid Virtualization Indexing).

See also: 6 remarkable security features on Windows 10 Fall Creators Update

**TPM (Trusted Platform Module)** : this is a hardware module that is integrated in the motherboard or purchased separately to support the circuit board, manage the security of the encryption keys, the storage, generate random numbers and hardware authentication.

**Boot authentication** : This feature prevents the computer from downloading the firmware designed by the system manufacturer, preventing attackers from downloading malicious firmware onto the device. You can use Intel Boot Guard in Verified Boot or AMD Hardware Verified Boot mode.

**RAM** : finally memory, 8GB minimum recommended.

*Microsoft hardware and firmware standards recommended for Windows 10 security*

# The firmware standard

The firmware of the device also needs to meet some requirements:

1. UEFI (Unified Extension Firmware Interface) 2.4 or newer.
2. UEFI Class 2 or UEFI Claas 3.
3. Driver must be compatible with HVCI (Hypervisor-based Code Integrity).
4. Supports UEFI Secure Boot and is enabled by default.
5. Secure MOR 2.
6. Support Windows UEFI Firmware Capsule Update.

## It is not expensive to meet these standards

After reading, you may think that a computer that meets this standard must be expensive. But the reality is not. However, many computers cannot respond 100% because there is no TPM module. So when buying a device, choose a machine with a motherboard with a TPM socket to install the TPM module.

See also: How to speed up Windows 10 by turning off the application that runs in the background