www.theverge.com

Why Windows 11 is forcing everyone to use TPM chips

Tom Warren

7-9 minutes

Microsoft's security effort is complicated

- By
- on June 25, 2021 1:10 pm

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.

Microsoft announced yesterday that Windows 11 will require TPM (Trusted Platform Module) chips on existing and new devices. It's a significant hardware change that has been years in the making, but Microsoft's messy way of communicating this has left many confused about whether their hardware is compatible. What is a TPM, and why do you need one for Windows 11 anyway?

"The Trusted Platform Modules (TPM) is a chip that is either integrated into your PC's motherboard or added separately into the CPU," explains David Weston, director of enterprise and OS security at Microsoft. "Its purpose is to protect encryption keys, user credentials, and other sensitive data behind a hardware barrier so that malware and attackers can't access or tamper with that data."

So it's all about security. TPMs work by offering hardware-level protection instead of software only. It can be used to encrypt disks using Windows features like BitLocker, or to prevent dictionary attacks against passwords. TPM 1.2 chips have existed since 2011, but they've typically only been used widely in IT-managed business laptops and desktops. Microsoft wants to bring that same level of protection to everyone using Windows, even if it's not always perfect.

A dedicated TPM chip you probably don't actually need for Windows 11.

Microsoft has been warning for months that firmware attacks are on the rise. "Our own Security Signals report found that 83 percent of businesses experienced a firmware attack, and only 29 percent are allocating resources to protect this critical layer," says Weston.

That 83 percent figure seems huge, but when you consider the various phishing, ransomware, supply chain, and IoT vulnerabilities that exist, the broad range of attacks becomes a lot clearer. Ransomware attacks hit the headlines weekly, and ransomware funds more ransomware so it's a difficult problem to solve. TPMs will certainly help with certain attacks, but Microsoft is banking on a combination of modern CPUs, Secure Boot, and its set of virtualization protections to really make a dent in ransomware.

Microsoft is trying to play its part, particularly as Windows is the platform that's often most affected by these attacks. It's widely used by businesses worldwide, and there are more than 1.3 billion Windows 10 machines in use today. Microsoft software has been at the core of devastating attacks that made global headlines, like the Russia-linked SolarWinds hack and the Hafnium hacks on Microsoft Exchange Server. And while the company isn't responsible for forcing its clients to keep its software patched, it's trying to be more proactive about protection.

Microsoft is pushing modern Windows 11 PCs.

Microsoft has a habit of struggling to move Windows into the future in both hardware and software, and this particular change hasn't been explained well. While Microsoft has required OEMs to ship devices with support for TPM chips since Windows 10, the company hasn't forced users or its many device partners to turn these on for Windows to work. That's what's really changing with Windows 11, and combined with Microsoft's Windows 11 upgrade checker, it has resulted in a lot of understandable confusion.

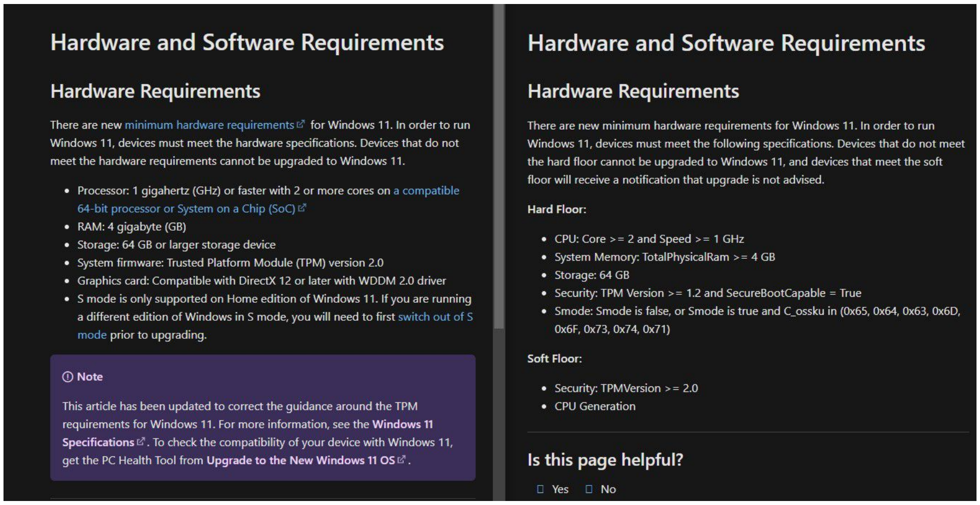
Microsoft's Windows 11 website lists the minimum system requirements, with a link to compatible CPUs and a clear mention that a TPM 2.0 is required at a minimum. The PC Health Check app that Microsoft asks people to download and check to see if Windows 11 runs will flag systems that do not have Secure

Boot or TPM support enabled or devices that have CPUs that aren't officially supported (anything older than 8th Gen Intel chips).

That's left many trying to figure out if their device supports TPM or not, confusion with BIOS settings, and even people rushing to buy separate TPM modules they don't need. Some are even scalping TPM 2.0 modules on eBay!

It also didn't help that Microsoft originally had a second webpage with contradictory information, one which it changed a couple hours after we published this story. According to the original version of the page, the true minimum requirements were TPM 1.2 and a 64-bit dual-core CPU that's 1GHz or greater, but the new page now clarifies it requires TPM 2.0 and a processor that Microsoft has explicitly certified as compatible — which might mean everything before an 8th Gen Intel Core and AMD Ryzen 2000 won't work.

We're still waiting for explicit confirmation from Microsoft on the CPU requirement, but a rep confirms that TPM 2.0 will be mandatory, and that the original information on that page was wrong. "The referenced docs page was a mistake that has since been corrected," an MS rep tells *The Verge.*



Hardware and Software Requirements

Hardware Requirements

There are new minimum hardware requirements for Windows 11. In order to run Windows 11, devices must meet the hardware specifications. Devices that do not meet the hardware requirements cannot be upgraded to Windows 11.

- Processor: 1 gigahertz (GHz) or faster with 2 or more cores on a compatible 64-bit processor or System on a Chip (SoC)
- RAM: 4 gigabyte (GB)
- Storage: 64 GB or larger storage device
- System firmware: Trusted Platform Module (TPM) version 2.0
- Graphics card: Compatible with DirectX 12 or later with WDDM 2.0 driver
- S mode is only supported on Home edition of Windows 11. If you are running a different edition of Windows in S mode, you will need to first switch out of S mode prior to upgrading.

Note

This article has been updated to correct the guidance around the TPM requirements for Windows 11. For more information, see the **Windows 11 Specifications**. To check the compatibility of your device with Windows 11, get the PC Health Tool from **Upgrade to the New Windows 11 OS**.

Hardware and Software Requirements

Hardware Requirements

There are new minimum hardware requirements for Windows 11. In order to run Windows 11, devices must meet the following specifications. Devices that do not meet the hard floor cannot be upgraded to Windows 11, and devices that meet the soft floor will receive a notification that upgrade is not advised.

Hard Floor:

- CPU: Core >= 2 and Speed >= 1 GHz
- System Memory: TotalPhysicalRam >= 4 GB
- Storage: 64 GB
- Security: TPM Version >= 1.2 and SecureBootCapable = True
- Smode: Smode is false, or Smode is true and C_ossku in (0x65, 0x64, 0x63, 0x6D, 0x6F, 0x73, 0x74, 0x71)

Soft Floor:

- Security: TPMVersion >= 2.0
- CPU Generation

Is this page helpful?

□ Yes □ No

New vs. old.

Screenshot by Sean Hollister / The Verge

Microsoft is promoting TPM 2.0 and performing checks for 8th Gen or newer Intel chips because these are the requirements for certified OEM hardware — the machines you'll find in stores with an inevitable Windows 11 sticker. But it's no longer clear whether the Windows 11 update will work on older machines either, and Microsoft is suggesting to us that it won't. We understand Microsoft is currently putting together a blog post that will explain the minimum requirements in more detail.

But that doesn't mean your existing PC is out of luck just because you're having issues with Microsoft's compatibility tool. Unless your CPU is *very* old, it probably already has baked-in TPM 2.0 support.

If you're having issues with the PC Health App checker for Windows 11, make sure you have "PTT" on Intel systems enabled in the BIOS, or "PSP fTPM" on AMD devices. The company's system checker should also be less confusing now: shortly after we published this story, Weston tweeted that the tool will now be more specific about why your PC isn't passing muster.

What Microsoft is trying to achieve here will benefit the Windows ecosystem in years to come, alongside its new efforts for Xbox-like security on Windows. Microsoft just totally dropped the ball on explaining that to everyone on day one.

Update, 2:26PM ET: *Added that Microsoft updated its PC Health Check app, shortly after we published this story, to be more specific about why your computer isn't meeting Windows 11 system requirements.*

Update, 3:53PM ET: *Added that Microsoft has changed its compatibility page to mention TPM 2.0 as a requirement instead of TPM 1.2, and that specific CPUs may be a requirement. We're getting to the bottom of this now.*

Correction, 8:06PM ET: *This story originally stated Windows 11 would likely still install on PCs with access to TPM 1.2 and older CPUs, because that's what we read in Microsoft's documentation. Microsoft has now corrected those documents to specify TPM 2.0 is a minimum requirement for Windows 11.*