Why is Windows 11 so much more secure than Windows 10?

Windows 11 will be a more secure operating system than Windows 10. Microsoft's new focus on security in Windows 11 will revolve around a few key features.

Windows 10 already has security issues. From Specter and Meltdown to the recent Print Spooler bug, the list of Windows 10 vulnerabilities is 'rich'. It is therefore a relief to see Microsoft double down on security in Windows 11.

Windows 11 will be a more secure operating system than Windows 10. Microsoft's new focus on security in Windows 11 will revolve around a few key features. So let's take a look at the key security features that strengthen Windows 11's defenses.

1. Trusted Platform Module (TPM)

Ever since Microsoft announced that Windows 11 requires support for Trusted Platform Module (TPM) 2.0, this topic has become controversial. Although TPM chips have been around for more than a decade, device manufacturers and users have so far not taken them seriously.

The TPM chip is a cryptographic vault that stores encryption keys, passwords, and certificates. The TPM chip uses stored entries to identify and authenticate devices, software, and users.

For example, in Windows 11, Windows Hello works with the TPM 2.0 chip to secure the sign-in process. The TPM 2.0 chip stores a secret associated with Windows Hello and uses that secret to authenticate the user.

According to Microsoft on Windows Blogs, the reason to use the new TPM 2.0 instead of the older TPM 1.2 is because TPM 2.0 supports better cryptographic algorithms.

In other words, the TPM 2.0 chip will ensure that Windows 11 PCs are authenticated and not compromised.

2. Virtualization-Based Security (VBS)

Microsoft has included the Virtualization-Based Security (VBS) feature in Windows 11. This feature aims to protect security solutions against exploit attacks, by storing these solutions inside a partition Segment of system memory is isolated and secured.

In simpler terms, VBS takes a portion of system memory, isolates it from the rest of the operating system, and uses that space to store security solutions. By doing this, Microsoft is protecting the security solutions that are the main target of most cyberattacks.

Although VBS support is available in Windows 10, it is not used by default. Microsoft is changing this with Windows 11. The company has announced that it will enable VBS on most versions of Windows 11 by default next year.

3. Hypervisor-Protected Code Integrity (HVCI)

Hypervisor-Protected Code Integrity is a feature of VBS that protects the isolated system memory environment that VBS creates. HVCI ensures that the Windows kernel, or the brains of the operating system, is not compromised.

Since many exploits rely on using kernel mode to gain access to the system, HVCI does an important job in ensuring that the kernel is secure and cannot be used to attack the system.

HVCI makes sure the brain of Windows (kernel) doesn't do something stupid that could compromise the security of the system.

Windows 10 comes with HVCI. But it reduces the performance of older CPUs quite a bit. This is one reason why Microsoft requires 8th Gen AMD CPUs or later and Zen 2 or later, as it has HVCI-specific hardware.

In short, Windows 11 will be significantly more secure than Windows 10 by default through the use of HVCI and VBS.

5. UEFI Secure Boot

Before talking about UEFI Secure Boot, let's make one thing clear: All Windows security tools and protocols can't do anything if your system is compromised before booting.

Simply put, if Windows boots with malicious code, the exploit attack can bypass all security measures. UEFI Secure Boot ensures this doesn't happen by verifying that the computer boots only with code from a trusted source. This source can be the PC manufacturer, chip manufacturer, or Microsoft.

All Windows 11 machines will come with UEFI Secure Boot from the start. This will give Windows 11 machines a significant amount of security compared to Windows 10 devices.

Microsoft is making sure that the new operating system is secure from the start. Security-focused hardware like TPM 2.0 and newer CPUs enable features like VBS and UEFI Secure Boot to protect users against exploit attacks.

However, most Windows users are still using older machines. So Microsoft had to convince people to buy a new PC. And that won't be easy.