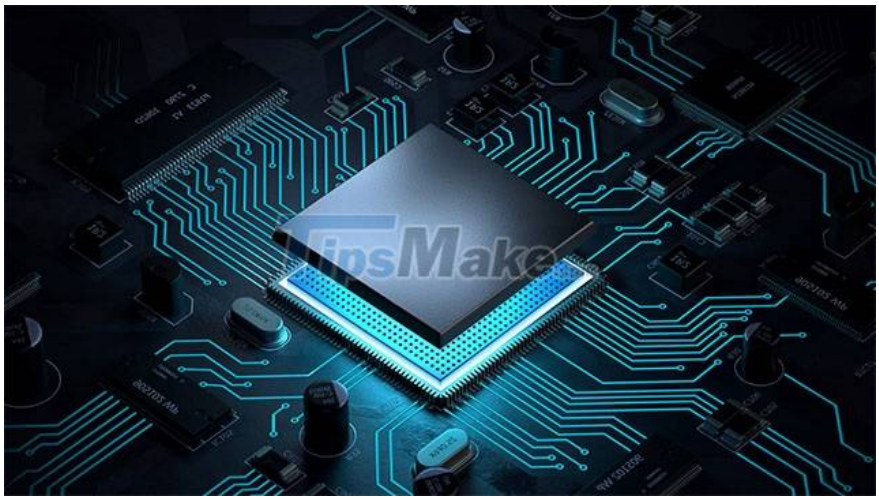
What is Microsoft's Pluton Security Processor? How does it work?

The first computers 'packaged' with Microsoft's Pluton secure processor will be available as soon as this 2022, accompanied by AMD Ryzen 6000 laptop CPUs.

This is a device that is expected to bring more optimal security to Windows PC systems by removing sensitive data such as encryption keys inside the CPU package.

In fact, Microsoft announced Pluton for PC at the end of 2020, but it will not be until 2022 that this security technology will make it to actual devices. In addition to AMD, Qualcomm also announced Pluton support with the Snapdragon 8cx Gen 3 SoC series. So what is the Pluton security processor really, and how does it work in practice? Let's find out right here.



What is Pluton?

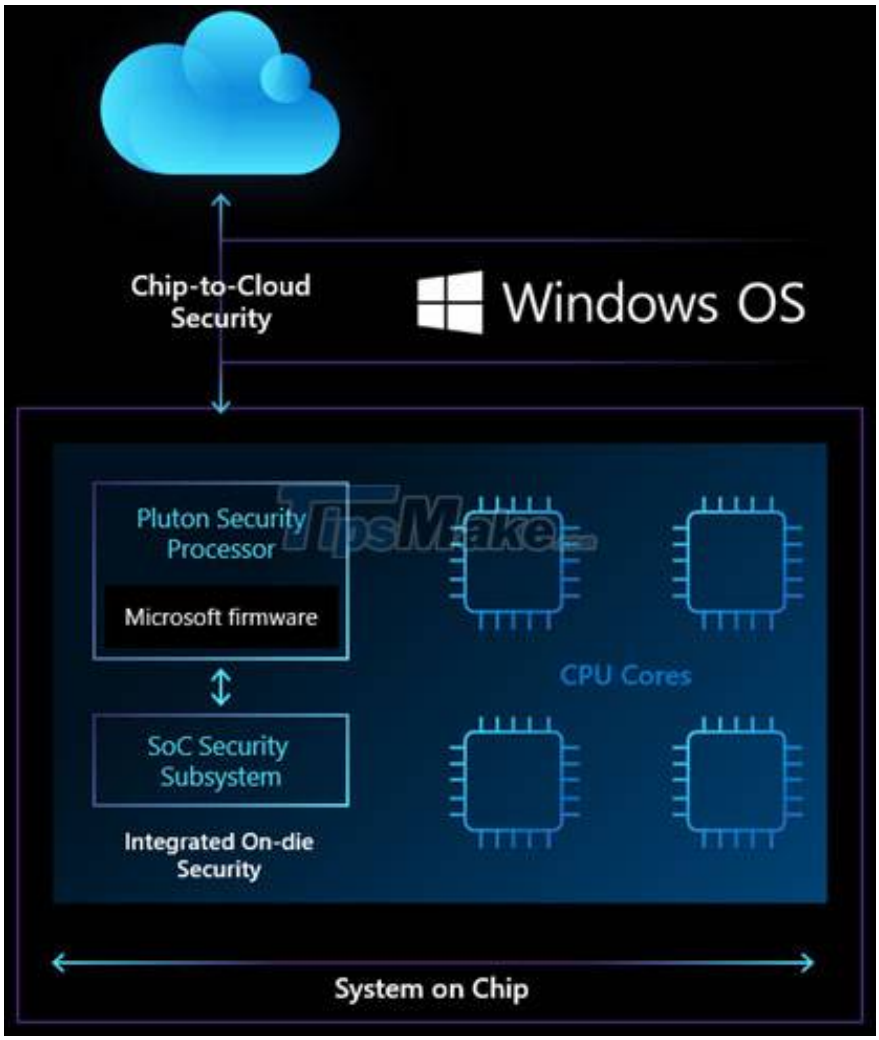
Pluton is built on the idea of ????a Trusted Platform Module (TPM) chip – a security measure that has almost prevented many old PC systems from being upgraded to Windows 11. TPM improves system security by preventing system security. the attackers tamper with the firmware, which in turn leads to an attack on data stored on the PC. TPM also enables advanced security features such as BitLocker disk encryption, and provides greater protection for biometric data used with Windows Hello.

TPM is a good start to the idea of ??a foundational security chip, and according to Microsoft, it forces attackers to spend more time and effort if they want to break into a target system. At this point, malicious actors start looking for weaknesses in the TPM system, and they focus on one specific weakness: The communication lines between the TPM hardware chip (usually found on motherboards) and the CPU .

Pluton addresses this weakness by removing the need for 'external' communication between the TPM and the CPU. Instead, the Pluton and its TPM-like functionality are a component built on top of the processor's own die. Microsoft says this makes it harder to extract sensitive information, even if attackers have actual ownership of a device. Even hackers will not be able to delete these data from Pluton even if they have installed malicious code to take complete control of the computer.

From within the CPU package, Pluton can emulate a TPM using existing Microsoft specifications and application programming interfaces (APIs).

However, replacing TPM is only part of the benefits Pluton can provide. Microsoft says the technology can also be used as a secure processor for system recovery in situations where TPM is not required.



Actual Uses of Pluton

With the Pluton chip integrated in the CPU, sensitive system data such as encryption keys, login information and user identities. will be better protected. It allows isolating critical information from the rest of the system with features such as Secure Hardware Cryptography Key (SHACK) technology. The idea with SHACK is that security keys are never exposed outside of protected hardware, and include Pluton's own firmware — the firmware a component needs to function.

In addition, the firmware of Pluton will also be updated through Windows Update like many other components on your PC. This means that new features based on Pluton can be deployed to older devices, and any emerging threats can be mitigated through regular security updates. This integration with the Windows Update system makes Pluton part of what Microsoft calls a 'chip-to-cloud' security solution.

In particular, Pluton for Windows computers will be linked to the Windows Update process in the same way that the Azure Sphere Security Service connects to IoT devices.

Above are the basic information you need to know about Pluton security technology, as well as the benefits it brings on Windows computers.