Technology Topic Summary

What Is a Trusted Platform Module (TPM)?

A trusted platform module (TPM) is a security chip on a computer's CPU. It provides hardware-based protection of sensitive information stored on PCs, like credentials and passwords, against malware and sophisticated cyberattacks. TPM 2.0 is required for all Windows 11 users.

TPM at a Glance

Security challenges:

- Cyberattacks are becoming more frequent and advanced.
- Businesses must protect sensitive information stored on PCs from external attacks.
- Securing laptops across an enterprise is a time-intensive process.

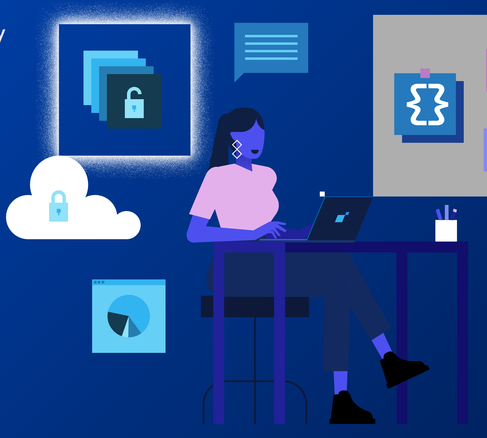
Solution:

- TPMs use cryptography to securely store critical data behind a hardware barrier.
- TPM 2.0 technology is built into most newer PCs but must be activated.
- TPM 2.0 is a Windows 11 security requirement that helps safeguard PCs.

Benefits of TPM

TPMs enhance PC security protections to proactively combat cyberattacks.

- **Secured credentials:** Prevents unauthorized access to system credentials to mitigate the risk of data breaches.
- **Hardware-based trust:** Protects against advanced software-based attacks, as the TPM is a component of the motherboard or processor.
- **Preinstalled protection:** PCs purchased in the past few years likely already have a TPM capable of running TPM 2.0.



Reasons to Upgrade to TPM 2.0

- Cyberattacks occur more often and are more sophisticated.
- Recovery costs from a security breach can easily force a company out of business.
- Windows 11 requires PCs to have TPM 2.0 installed and enabled.
- TPM is prebuilt into newer PCs and is easy to enable, depending on the make/model of the PC.

Protect the future of your business with hardware-based security

Learn more at intel.com/content/www/us/en/business/enterprise-computers/overview.html