ThinkShield

CAN YOUR PCs DEFEND THEMSELVES?

THE INCREASINGLY IMPORTANT ROLE OF HARDWARE IN SECURITY

Hardware components are opening up new possibilities for hardening endpoints from attack, including everything from encryption to virtualization and BIOS protections.

ENCRYPTED SSDs
Built-in AES 256-bit self-encryption protects data at the hardware level.

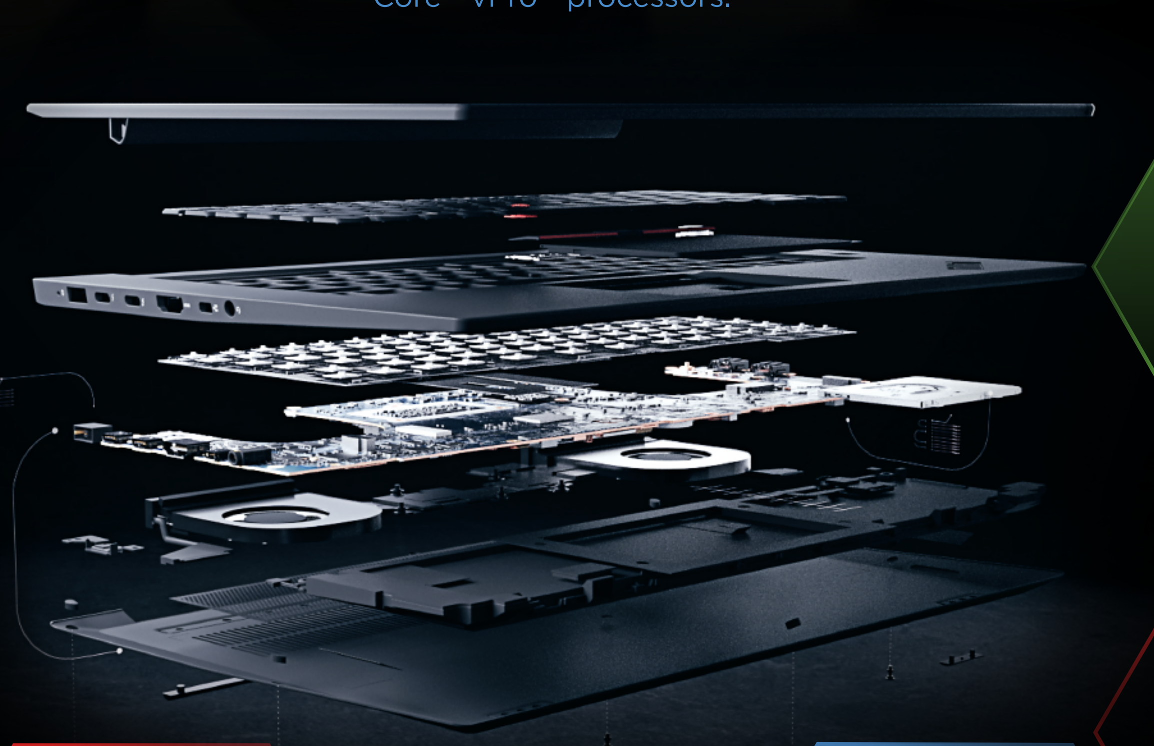
INTEL AUTHENTICATE SOLUTION
Hardware-enhanced multifactor authentication that strengthens identity protection—storing encrypted biometric data in a secure hardware enclave.

INTEL SOFTWARE GUARD EXTENSIONS
Allows for the creation of secure enclaves within memory, protecting sensitive data from snooping from other apps.

INTEL HARDWARE SHIELD
Protects against attacks on BIOS during boot and operation by locking the BIOS when software is running. Part of ThinkShield self-healing BIOS protections.

intel vPro™ Platform

Intel® vPro™ Platform Protections
ThinkShield is powered by the Intel vPro platform: a collection of hardware-enhanced security features powered by modern Intel® Core™ vPro™ processors.



TRANSPARENT SUPPLY CHAIN
Tracks and reports the authenticity of PC components to ensure devices are genuine and have not been tampered with.

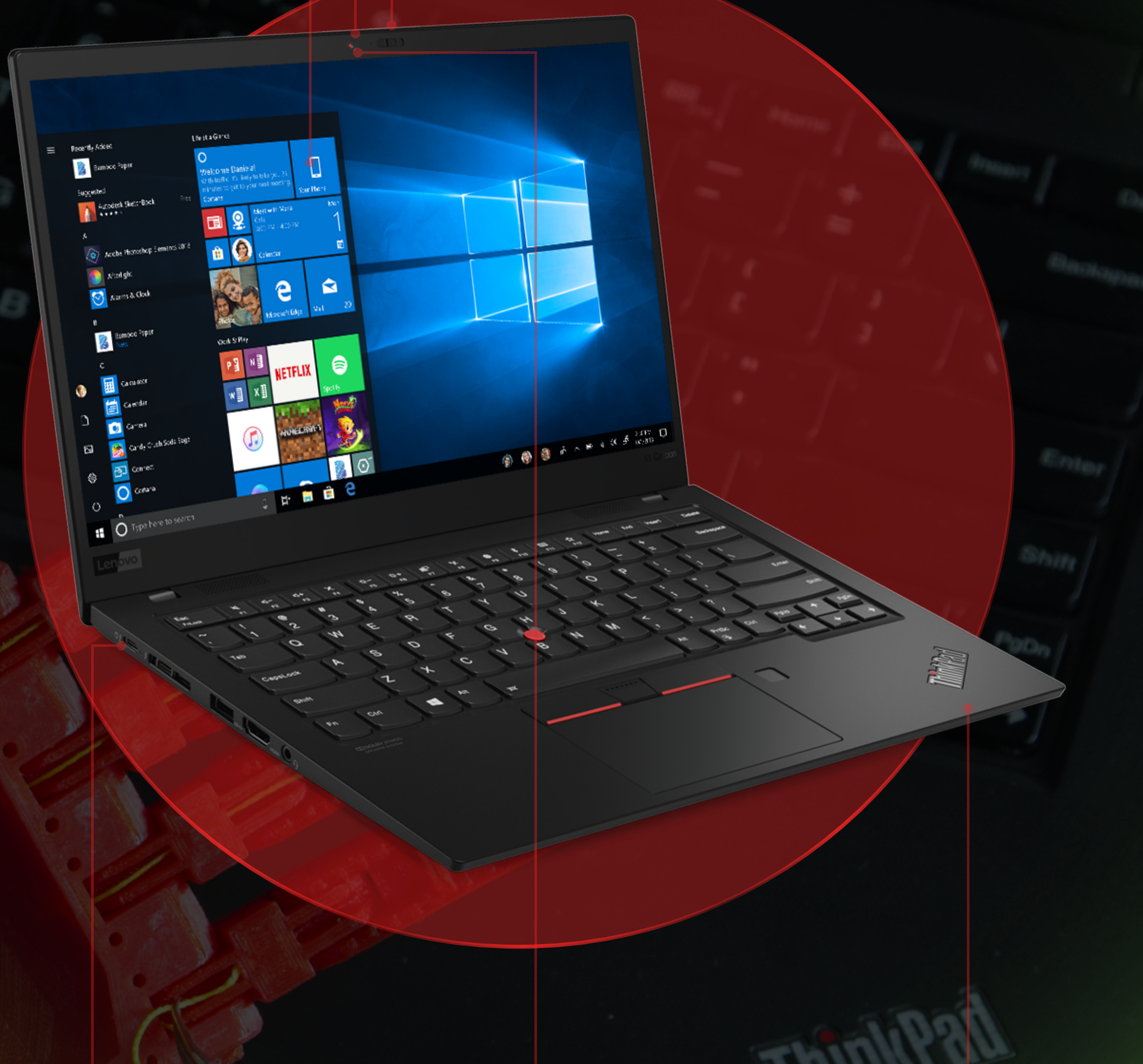
INTEL THREAT DETECTION TECHNOLOGY
Uses the graphics engine for aggressive security scanning of downloads and attachments while leaving the CPU free for user productivity.

ACTIVE MANAGEMENT TECHNOLOGY
Silicon-level platform management features for secure out-of-band access to continually manage and recover devices back to a healthy state.

INFRARED CAMERA
Integrated IR cameras enable security features like biometric authentication, and presence detection that issues a privacy alert when being shoulder-surfed and locks the device when the user is away.

PRIVACY GUARD
ePrivacy filter that restricts the field of view when electronically activated.

THINKSHUTTER
Integrated physical webcam cover provides assurance that the webcam is not in use.



WINDOWS HELLO[1]
Advanced authentication with biometric facial scanning and other factors for hardening credentials against theft.

SMART THUNDERBOLT / USB PROTECTION
Restricts access to hardware ports, restricting data transfer and allowing only non-storage peripherals such as mice and keyboards.

USB SECURE HARD DRIVE
The ThinkPad USB Secure Hard Drives offers high-level, 256-bit AES security, as well as a keypad for entering an 8- to 16-digit password.

THINK ENGINE
A custom chip embedded within Lenovo Think devices that performs security functions that are completely isolated from software.

ThinkShield is Lenovo's portfolio of secure Think devices, software, and services—fully customizable to keep your business ahead of dangerous breaches. Get the most comprehensive protection with a modern Windows 10 Pro device powered by the Intel® vPro™ platform.

1 To use Windows Hello with biometrics specialized hardware, including fingerprint reader, illuminated IR sensor, or other biometric sensors is required. Hardware based protection of the Windows Hello credential/keys requires TPM 1.2 or greater; if no TPM exists or is configured, credentials/keys protection will be software-based.

intel vPro™ Platform Windows 10

Learn more at www.lenovo.com/ThinkShield.

Smarter technology for all

Lenovo