ThinkShield

TRUST NOTHING.
VERIFY EVERYTHING.

Solid advice—but how do you get there? Companies who want to improve their ability to defend against cyberthreats operate on a zero trust basis. But it's a daunting task, especially across a large enterprise. ThinkShield provides tools to help you build your zero trust environment.

THINKSHIELD CAN PROTECT YOUR DATA

Persistent Endpoint Management
Visibility and access to every endpoint, no matter where it's operating. Ensures that safeguards like encryption and anti-malware are active and the device is up to date with patches, etc.

Data Encryption
Whether data lives on a device hard drive or in the cloud, ThinkShield can encrypt it from end to end so sensitive data can be safely shared.

Multifactor Authentication
Windows Hello[2] and the Intel® Authenticate Solution combine biometrics and other factors like GPS location to restrict device access to only authorized users.

Lenovo Wi-Fi Security
Uses behavioral rules and defined lists to notify users when connecting to untrusted public networks by warning them of suspicious access point behavior.

WINDOWS INFORMATION PROTECTION[1]
Control how your employees use your business data—preventing them from copying customer or financial data into social media apps, for example— while ensuring all business data is encrypted and accessible only by those who need it.

INTEL® SSDs
Self-encrypting Intel Pro SSDs seamlessly integrate with Windows BitLocker, allowing IT to encrypt devices while retaining control of encryption keys. Intel® Remote Secure Erase then also allows IT to securely wipe Intel® Pro SSDs in seconds.

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.

intel vPro™ Platform Windows 10
Windows 10 Pro means business.

Learn more at **www.lenovo.com/ThinkShield**.

Smarter technology for all

Lenovo

1 Windows Information Protection requires either Mobile Device Management (MDM)* or System Center Configuration Manager* to manage settings.
2 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.