ThinkShield

Windows 10

Windows 10 Pro means business.

IDENTITY THEFT ISN'T "THEIR" PROBLEM. IT'S YOURS.

Shield your company.

ThinkShield by Lenovo is the most comprehensive suite of end-to-end security offerings for business on the market today. Our distinctive identity solutions ensure you stay one step ahead of the criminals. Choose a unique multi-factor authentication process for employees from our robust offerings, including Windows 10 Hello, many of which are supported by Intel® Autenticate.

- Network security
- Geo-fencing security
- Secure NFC tap-to-log-on
- Facial recognition with Windows 10 Hello
- Password and pins
- Match on Chip fingerprint reader
- Physical smart card insertion
- Bluetooth phone proximity authentication

Get additional protection with the premium ThinkPad X1 family with Windows 10, including the X1 Carbon and X1 Yoga, which provides the safest version of Windows available today.

X1 Carbon

69% of data breaches in 2017 were identity thefts.[2]

2.6B records were stolen in 2017.[3]

81% of data breaches in 2017 involved stolen or weak passwords.[4]

Lenovo has the industry's first FIDO®-certified authenticators for safer, password-free logins.

Fast Identity Online (FIDO) authenticates identities on sites like PayPal®, Google™, and Dropbox® using secure fingerprint technology. Employees use their fingerprints as a second factor when logging in to corporate networks and other business resources, making employees less vulnerable to common attacks like credential theft and phishing.

Smart USB protection guards USB ports from unauthorized use.

BIOS-based USB protection on ThinkCentre desktops lets you configure USB ports to respond only to keyboards and pointing devices, preventing thieves from stealing your company's data.

This is no time to compromise.
With ThinkShield by Lenovo, you won't have to.

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

Lenovo

1,2,3 https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf
4 https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf