ThinkShield

THERE ARE TWO TYPES OF COMPANIES TODAY:

# THOSE THAT HAVE HAD SECURITY BREACHES, AND THOSE THAT DON'T KNOW THEY HAVE.

ThinkShield by Lenovo Solutions Guide

Powered by Intel® vPro™ Platform

# 2017 was the biggest year yet for cybercriminal activity—and the statistics are staggering.

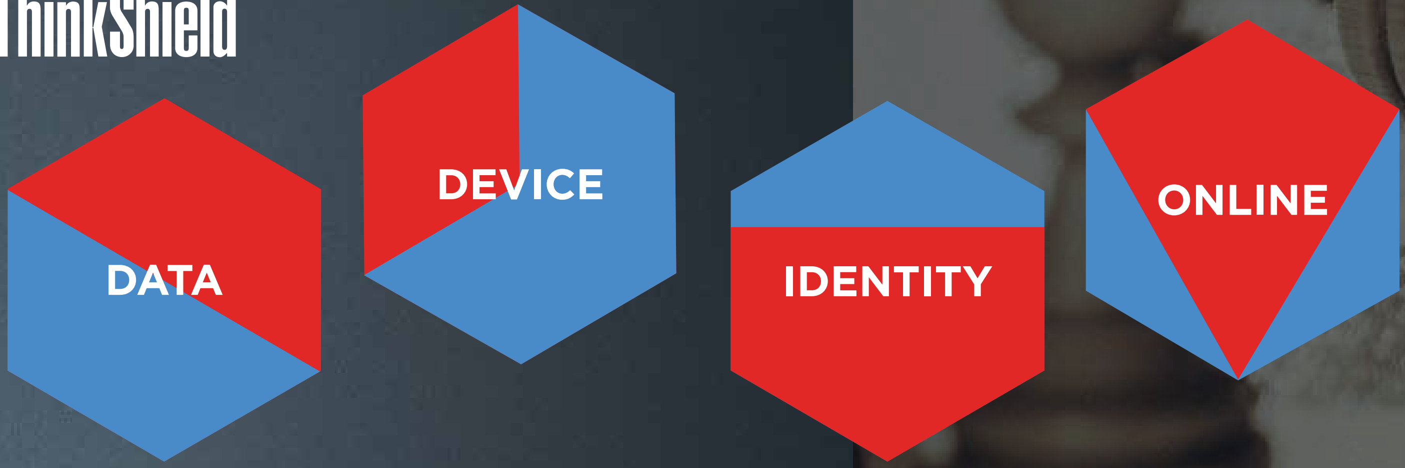
The number of cyberattacks is rising every day. And criminals are constantly developing more sophisticated and creative ways to expose vulnerabilities. For instance, there was one supply chain attack per month in 2017, as compared with four annually in prior years.[7] Every device is at risk, and companies must turn to technology providers they can trust to “out-innovate” the bad guys.

# Lenovo has you shielded from every angle.

ThinkShield by Lenovo is the most comprehensive suite of end-to-end security offerings for business on the market today. Scalable to meet your unique requirements, and encompassing device, data, identity, and online solutions, ThinkShield ensures you stay one step ahead of the criminals.

**ThinkShield provides four pillars of protection for your business. Don’t settle for anything less.**

ThinkShield



**2.6B**
records were compromised.[1]

Phishing schemes targeted
**3 IN 4** companies.[2]

**81%**
of data breaches involved stolen or weak passwords.[3]

**< 10%**
of people can tell legitimate and threat emails apart.[4]

Data breaches cost businesses an average of
**$3.62M**[5]

Companies lost around
**23 DAYS**
resolving ransomware attacks.[6]

intel

Powered by Intel®
vPro™ Platform

# ASK THE RIGHT QUESTIONS, AND ELEVATE YOUR COMPANY'S SECURITY.

Q/A

## What does "security by design" mean, and how does it affect my company's security?

At Lenovo, security is the foundation of everything we do. In product development, during manufacturing, and through the lifecycle of use, we are focused on preventing threats to your company's data, customers, and reputation.

- Our innovative device security features include the ThinkShutter camera shutter, built-in ePrivacy filter, and smart USB protection guards.
- Lenovo's industry-first FIDO®-certified authenticators ensure safer, password-free user logins to protect identity.
- With our trusted service provider certification, your system, equipment, and data stay secure during repair and service.
- WiFi Security with Coronet® technology and online sandboxing prevent online hacking.[8]

Q/A

## How do I know the devices I buy haven't been compromised during manufacturing?

You're right to be concerned. Criminals are increasingly targeting supply chains to introduce vulnerabilities.[9] Lenovo's uncompromising product supply chain and Trusted Supplier Program help keep devices secure.

- Lenovo oversees the security of suppliers who build intelligent components, making sure they conform to our rigorous Trusted Supplier Program guidelines and best practices. For an extra layer of transparency, our Quality Engineers can audit suppliers at any point.
- We work with Intel® to align with its Transparent Supply Chain, enabling any user to validate the authenticity of PCs running 8th Generation Intel Core™ vPro™ processors.

Q/A

## With data breaches so widespread, how do I make sure my company's sensitive data stays secure?

With ThinkShield by Lenovo, your data is protected while devices are in use, when they're being serviced, and at end of life.

- The ThinkPad PrivacyGuard integrated screen filter prevents shoulder surfing with gaze and presence detection.[10]
- With secure recycling, we wipe your devices' drives and securely recycle the parts, so data stays protected.
- If you need to replace the drive of a device, our Keep Your Drive service allows you to retain the old drive, ensuring that sensitive information never leaves your workplace.[11]

intel® Powered by Intel® vPro™ Platform

Q/A

## I'm worried that exposure to malware will infect my company's networks. How do I make sure employees stay safe online?

With innovative features that protect against unsafe WiFi networks, ThinkShield offers solutions that identify threats and contain them before they spread.

- Lenovo WiFi Security, which comes standard on all Think PCs, detects threats and notifies users when they're about to connect to an unsafe network. This helps prevent scammers from accessing passwords and other confidential information.
- Lenovo Endpoint Management, powered by MobileIron®, provides a secure, simple way to unify cloud and endpoint security across multiple devices—an ideal security solution for the modern workplace. Companies can securely share data, allowing on-the-go workers to do their jobs anywhere, anytime. Lenovo Endpoint Management keeps personal information private (by creating a zone of trust around clouds and Lenovo devices) and enables "bring your own device" programs (by letting IT professionals wipe business data while leaving personal data intact). With Lenovo Endpoint Management, you can adapt to the needs of your mobile workforce while remaining secure.[12]

Q/A

## How can employees protect their identities without using passwords that are hard to remember or easy to hack?

With Intel Authenticate and the industry's first integrated FIDO®-certified authenticators, ThinkShield by Lenovo blocks hackers from every angle.

- ThinkShield provides multiple factors of authentication, many of which are supported by Intel® Authenticate. These include Intel AMT Location, Protected Bluetooth Proximity, Bluetooth Proximity, Protected Fingerprint, Fingerprint, Face Recognition, and Protected PIN.
- Lenovo is the first vendor to integrate FIDO-certified authenticators directly into Microsoft® Windows® PCs. FIDO authenticates identities on sites like PayPal®, Google™, and Dropbox® using secure fingerprint technology. It's also a highly secure and private way for employees to use their fingerprints as a second factor when they log in to corporate networks and other connected business resources. Before, implementing this type of authentication came with risk, privacy concerns, and complex management. But Lenovo's FIDO-certified authenticators make secure fingerprint authentication a reality.
- Our match-on-chip fingerprint reader uses cutting-edge Synaptics® technology to perform authentication completely in the reader, protecting identity credentials from attack.
- BIOS-based smart USB protection allows you to configure USB ports to respond only to keyboards and pointing devices. This means your IT department can prevent employees from downloading data onto unsecured devices and stop criminals from walking off with your company's data.
- Smartcard readers give an extra level of security for companies using employee badges for authentication.
- With ThinkShutter, the built-in camera shutter on our newest ThinkPad laptops, employees can make sure they're not being watched when their cameras aren't in use.

## A cyberattack is coming for you. This is no time to compromise. With ThinkShield by Lenovo, you won't have to.

For more information, contact your account representative or visit **www.lenovo.com/ThinkShield**.

[1] https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf

[2] https://www.wombatsecurity.com/state-of-the-phish-2018

[3] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

[4] https://newsroom.intel.com/editorials/expert-caught-phishing-net/

[5,6] https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

[7] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf

[8] Sandboxing is available through BUFFERZONE, currently a paid offering in North America

[9] https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-global-threat-intelligence-report-v2-uea.pdf?sfvrsn=c761dd4d_10

[10] Both presence and gaze protection require a computer model with an infrared camera.

[11] Keep Your Drive is a paid service. Learn more at https://www.lenovo.com/us/en/services/pc-services/lifecycle-support/warranty-protection/.

[12] Lenovo Endpoint Management is a paid service.

Powered by Intel®
vPro™ Platform