IS YOUR SECURITY WORKING HARDER THAN THE HACKERS?

Lenovo ThinkShield Solutions Guide

Windows 10 Pro means business.
AVOIDING THE FALLOUT

It’s almost daily that reports emerge of another large company suffering a cybersecurity breach, resulting in severe fallout for their business.

THESE BREACHES COULD HAVE BEEN PREVENTED
Or at least, contained before causing irreparable damage.

EVERY BUSINESS DECISION MADE REQUIRES SECURITY TO MATCH
Otherwise vulnerabilities can be created and exploited.

Comprehensive and customizable end-to-end IT security significantly reduces the risk of being compromised and can have tremendous business benefits.

ThinkShield goes beyond simple endpoint security, with solutions that create huge efficiencies, streamline IT administration, improve the end-user experience, and provide a platform for businesses to compete safely.

1 Verizon: 2018 Data Breach Investigation Report
WHAT IS THINKSHIELD

Every new Lenovo product is secure by design, with secure hardware engineered by the makers of the world’s most trusted business PCs.

SECURE SUPPLY CHAIN
Rigorous, trackable, and auditable security standards are built into every step of our secure supply chain.

LENOVO INNOVATIONS
We practice security by design.

WORLD-CLASS PARTNERS
We’ve partnered with the industry’s most trusted security providers to provide deeper and broader protections.

THINKPAD X1 EXTREME

Windows 10 Pro means business.
ThinkShield was developed on a core set of beliefs about how best to serve users, admins, and businesses.

**STRONG SECURITY FUNDAMENTALS ALLOW I.T. TO DRIVE GROWTH**
When IT can spend more time on the big picture and less time on small issues—password resets, updates, patches, etc.—they can serve a more critical role as drivers of innovation and growth.

**SECURITY THAT INTERFERES WITH PRODUCTIVITY IS UNACCEPTABLE**
If device security slows down your people or stands in their way, they’ll find ways to circumvent it and leave you just as vulnerable as you were to start—if not worse. ThinkShield keeps security out of the end-user’s way and much more manageable for admins.

**DON’T LET INNOVATION OUTPACE SECURITY**
Every action taken to outpace competitors can open you up to new threats. Hackers can infiltrate the smallest vulnerability—like an unsecured IoT device or a new cloud app—to infiltrate your business. To ensure security of every endpoint requires solutions that can adapt.

**MAKING THE RIGHT DECISION NOW REDUCES COSTS AND PAYS RETURNS**
Technical debt accumulates when you solve security issues one at a time, with solutions that weren’t designed to work together. Choosing a comprehensive and customizable solution reduces sunk costs and creates new cost efficiencies.

**SECURITY SHOULD COVER THE ENTIRE DEVICE LIFECYCLE**
Protections need to be in place before your PC is even built. From product development through disposal, security is at the forefront of every product and service that we offer.
RAPID CHANGE BRINGS RAPID PROLIFERATION OF NEW SECURITY THREATS

We’re exploring some of the most significant security trends and questions so that organizations can better understand the intricacies and importance of end-to-end security that can adapt as your business faces new challenges.

1. STAYING AGILE
2. SECURITY AS A COMPETITIVE ADVANTAGE
3. MANAGING YOUR SECURITY STACK
4. IMPROVING THE SECURITY USER EXPERIENCE
5. DEFENDING THE INTERNET OF THINGS
6. HARDWARE-ENHANCED PROTECTION

View more on our website
www.Lenovo.com/ThinkShield
BUILDING BETTER BUSINESSES THROUGH SECURITY

Technology is core to every single business function—each with its own unique needs. So IT security has an opportunity to do more than just protect data. ThinkShield helps IT safely support and accelerate technological progress, without impeding the employee experience.

71% of executives say that cybersecurity concerns impede innovation in their organization.¹

LENNOVO VANTAGE
Allows end users / departments to customize their device experience within the security constraints set by admins.

INTEL® SOFTWARE GUARD EXTENSIONS
Create custom applications quickly with hardware-enhanced virtualization-based security from Intel®.

LENOVO PATCH FOR SCCM
Plugin for Windows update module that makes it easy for enterprises to keep apps and devices up to date and quickly patch their entire ecosystem.

fido
Allows for safe use of web and mobile apps by eliminating passwords and driving down the complexity of developing a dedicated solution.

WINMAGIC
On- and off-device encryption that can protect sensitive data in the event that a third-party app exposes it.

1 PWC 21st CEO Survey
STOP PLAYING CATCH-UP.
STAY AGILE WITH THINKSHIELD.

AUTOMATION & PATCHING
Keeping apps and devices up to date organization-wide can be a job all its own. Not with ThinkShield.

1. SOLUTION
ABSOLUTE PERSISTENCE TECHNOLOGY
Gives visibility into every endpoint on any network and allows patches to be delivered in bulk. App persistence automatically repairs and re-enables disabled or corrupted apps.

2. SOLUTION
LENOVO PATCH FOR SCCM
A plug-in for SCCM that broadens the kinds of updates it can deliver, allowing critical patches to be instantly delivered organization-wide.

3. SOLUTION
LENOVO THIN INSTALLER
Automatically installs updates behind the scenes without involving the end-user and directly injects a patch into the OS without adding code.

4. SOLUTION
WINDOWS AUTOPILOT
Low-touch device provisioning for IT.
STOP PLAYING CATCH-UP.
STAY AGILE WITH THINKSHIELD.

Amidst a flurry of updates, an evolving threat surface, and internal development needs, things are changing every moment for IT admins. ThinkShield provides the tools that IT departments need to act more effectively and keep costs down—all fully customizable to adapt as your business evolves.

LOWER IT COMPLEXITY & LOWER COSTS
Added complexity and manual work slows down IT security administration and drives up costs. ThinkShield helps your business stay efficient by simplifying and automating the following:

1. 3RD PARTY APP UPDATES
2. OS & DEVICE UPDATES
3. COMPLIANCE AUDITING
4. THREAT DETECTION & RESPONSE
5. DEVICE PROVISIONING

80%
69%
$700

Of total IT costs occur after the initial purchase.1
Of organizations don’t believe the threats they’re seeing can be blocked by their anti-virus software.3
Average monthly IT costs per user.2

VIRTUALIZATION-BASED SECURITY
ThinkShield virtualization provides an easy-to-implement abstraction layer to your environment, allowing for faster and more secure deployment of apps by creating secure enclaves that isolate and protect your applications and OS from threats and other complications.

> Bufferzone creates a virtualized sandbox for isolating online browser activity and other actions, mitigating risk from the use of web apps.

1. Cisco: Reducing Total Cost of Ownership
2. Gartner: Total Cost of Ownership
   http://www.envisionitpartners.com/the-3-costs-of-it
3. The Ponemon Institute: 2017 Cost of a Data Breach
ThinkShield leverages best-in-class security partners to offer a largely open and non-proprietary set of solutions that can more easily integrate with your existing tech stack.

58%

of IT security leaders say they regularly update OS/software to prevent security breaches.\(^1\)

**STANDARD BASED**

ThinkShield leverages and extends existing security standards—from TPM cryptography to FIDO web authentication—rather than leveraging closed, proprietary systems.

**DEVICE AGNOSTIC**

Diverse device environments often require multiple solutions for management. Lenovo embraces open solutions that can work across a variety of devices.

**PROVISIONING**

Existing services like Windows Autopilot are available, enabling secure low-touch device provisioning.

**PATCHING**

By offering flexibility in how patches are administered, Lenovo makes it easy to quickly patch vulnerabilities and keep devices up to date.

**ENDPOINT MANAGEMENT**

Solutions like MobileIron and Absolute allow you to see and manage every single device within your organization, whether it’s on or off-network.

---

1. Spiceworks Lenovo ThinkShield Survey.
YOU’RE NOT A BABYSITTER: EASILY PROTECTING & ENABLING THE END USER

You can’t always trust users to know the right thing to do. Nor can you oversee their every move. But you can trust ThinkShield to provide a pleasantly unobstructive and secure user experience without making more work for IT admins.

70% of employees lack basic cybersecurity knowledge.¹

46% of websites have high security vulnerabilities that an end user could never know about.²

Lenovo Security Console³
Prevents users from connecting to Wi-Fi networks that have been identified as unsafe with rules set centrally by IT.

Windows User Account Control
 Prevents changes to certain settings & preferences without administrator approval.

Bufferzone Sandboxing
 Creates a safe, virtualized environment for employees to work and browse in without the fear of a wrong click compromising their device or their credentials.

Intel® Authenticate Solution
Hardens user credentials while simultaneously easing the log-in process for end-users. Easily manageable for admins with up to 8 factors.

Lenovo Thin Installer & Update Retriever
Installs critical updates and patches without alerting the end-user or giving them the option to forego the updates.

Absolute Application Persistence
Automatically reactivates protections like encryption or anti-malware that have been corrupted or disabled by user activity.

¹ Media Pro: State of Privacy and Security Awareness Report
² Acunetix Web Application Vulnerability Report
³ Lenovo Security Console
https://www.coro.net/lenovo_security_console
A HACKER’S PLAYGROUND: SECURING THE INTERNET OF THINGS

NEW CONNECTIONS

SENSOR
Connected sensors monitor everything from crop fields to manufacturing lines.

SECURITY
Security cameras, window sensors, and other connected security equipment are often targeted.

SMART WORKPLACE
Workplaces are now full of new connected devices, from video conferencing systems to connected locks and security.

ENVIRONMENTS
Everything from thermostats and lightbulbs to smart assistants often lack proper security.

LENOVO THINKCENTRE NANO & NANO IOT
ThinkCentre Nano and Nano IoT protect IoT objects against intrusion while also providing an easy platform for device management via ThinkShield. They sit between smart objects and networks, securing data and providing processing power at the edge.

EXTENDED CONNECTIVITY
Expandable I/O for connecting a wide range of both legacy and next-gen devices.

POWERFUL & VERSATILE
Featuring Windows 10 IoT & 8th Gen Intel Processors (vPro-enabled for Nano only).

SIMPLY SECURE
Nano & Nano IoT bring ThinkShield security to IoT devices.

CLOUD CERTIFIED
4G LTE enabled and certified for Windows 10 IoT Enterprise, Microsoft Azure IoT Edge, and Ubuntu.

Windows 10 Pro means business.
A HACKER’S PLAYGROUND: SECURING THE INTERNET OF THINGS

The Internet of Things is undergoing explosive growth across industries. But new technology creates new security challenges. Explore below to see how ThinkShield is helping to secure the IoT.

**STATE OF THE IOT**

- 127 New devices connected each second
- 65% of business using IoT devices by 2020
- 5 MINUTES Average time before a new IoT device is attacked
- 20 BILLION IoT devices in use by 2020
- $2M Potential cost of suffering a DDoS attack
- 125% Increase in IoT malware attacks in 2018

**RETAIL**
The future of retail is built on the IoT, with cameras and RFID scanners replacing cashiers.

**MANUFACTURING**
Sensors, robotics, and inventory tracking are driving new manufacturing efficiencies.

**TRANSFORMING INDUSTRY**
Portable, connected treatment requires a new generation of smart and privacy-protecting medical devices.

**HEALTHCARE**
Portable, connected treatment requires a new generation of smart and privacy-protecting medical devices.

**PUBLIC SECTOR**
Large utilities and other public services use thousands of sensors, cameras, and other quality assurance devices.

---

1. Politico: Introducing the Wireless Cow
2. Gartner Newsroom
3. Gartner Leading the IoT
4. NetScout 2018 Q4 Threat Intelligence Report
5. 2019 SonicWall Cyber Threat Report
6. NetScout 2019 Q1 Threat Intelligence Report
   https://www.netscout.com/threatreport
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 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 HARDWARE SHIELD**

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

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

**INTEL SOFTWARE GUARD EXTENSIONS**

**EMA**
Makes vPro™ platform features manageable and activatable from the cloud or directly from the factory.

**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.

**INTEL SOFTWARE GUARD EXTENSIONS**

**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.

**INTEL THREAT DETECTION TECHNOLOGY**

**EMA**
Makes vPro™ platform features manageable and activatable from the cloud or directly from the factory.

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

**INTEL INTELLIGENCE 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.
CAN YOUR PCS DEFEND THEMSELVES?

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.

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

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

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.

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

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

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.
WORKING TOGETHER TO FORTIFY YOUR BUSINESS

Lenovo’s ThinkShield, Intel, and Microsoft link arm-in-arm to defend your company from security threats, offering built-in protection straight out of the box. While older devices can leave you vulnerable to breaches, a modern Lenovo device with Windows 10 Pro powered by the Intel® vPro™ platform offers you protection that’s customizable, always up-to-date, and designed to keep your workforce productive.

DON’T LEAVE YOUR BUSINESS UNPROTECTED

We’ll help customize the right solution for your business.

Click below to visit our website and connect with a security specialist.

Request A Consultation