



ThinkShield

Smarter  
technology  
for all

Lenovo

**I.T. SECURITY ISN'T JUST  
MORE IMPORTANT THAN  
EVER. IT'S THE MOST  
IMPORTANT THING, PERIOD.**

Lenovo ThinkShield Solutions Guide



Powered by Intel® vPro™ platform



# AVOIDING THE FALLOUT

It's almost daily that reports emerge of another university suffering a cybersecurity breach, resulting in severe fallout for their institution.

Smarter  
technology  
for all

Lenovo

## THESE BREACHES COULD HAVE BEEN PREVENTED

Or at least, contained before causing irreparable damage.

## EVERY DECISION MADE FOR AN INSTITUTION REQUIRES SECURITY TO MATCH.

Otherwise vulnerabilities can be created and exploited.

We believe that comprehensive and customizable end-to-end IT security not only dramatically reduces the risks of being compromised but can also have a tremendous benefit to the institution.

ThinkShield goes beyond simple endpoint security, with solutions that create huge efficiencies, streamline IT administration, and improve the end-user experience.

<sup>1</sup> Verizon: 2018 Data Breach Investigation Report  
[https://enterprise.verizon.com/resources/reports/DBIR\\_2018\\_Report.pdf](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf)

2/3

of businesses that suffered  
a breach **DIDN'T EVEN  
KNOW THAT THEY'D  
BEEN BREACHED** for  
several months.<sup>1</sup>



Powered by Intel® vPro™ platform

## WHAT IS THINKSHIELD

ThinkShield is Lenovo's portfolio of secure Think devices, software, processes, and services – customizable to your institution's needs and budget to help keep you ahead of dangerous breaches.



## THINKPAD X1 EXTREME



### SECURE SUPPLY CHAIN

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



### LENOVO INNOVATIONS

Every new Lenovo product is secure by design, with secure hardware engineered by the makers of the world's most trusted PCs for campuses across the country.



### WORLD-CLASS PARTNERS

We've partnered with the industry's most trusted security providers to provide deeper and broader protections.



Powered by Intel® vPro™ platform



# DESIGNED FOR YOUR INSTITUTION PERFECTED FOR PEOPLE

ThinkShield was developed on a core set of beliefs about how best to serve users, admins, and institutions alike.

Smarter  
technology  
for all

Lenovo



## 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

Exploring new grounds in technology and innovation 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 institution.



## MAKING THE RIGHT DECISION NOW REDUCES COSTS AND PAYS RETURNS

Solving security issues one at a time with solutions that weren't designed to work together accumulates technical debt: the cost of rework caused by choosing a series of quick fixes instead of a more comprehensive approach—never mind the costs that come from suffering a breach if gaps emerge. ThinkShield is a customizable portfolio of solutions designed to work in tandem that will be added to with time.



## SECURITY SHOULD COVER THE ENTIRE DEVICE LIFECYCLE

Manufacturing sabotage as well as transit fraud and theft are real and growing threats to IT security. And lost or stolen devices have contributed to major breaches, as well. We view it as our responsibility to help secure what's out of your control, so ThinkShield covers the entire device lifecycle—from development through disposal.



Powered by Intel® vPro™ platform

# THE RAPID PACE OF ADVANCEMENT BRINGS THE RAPID PROLIFERATION OF NEW SECURITY THREATS

---

We're exploring some of the most prominent security trends and questions so that institutions can better understand the intricacies and importance of end-to-end security that can adapt as your campus faces new challenges

---

1. PREVENTING HUMAN ERROR
  2. TRUE END-TO-END PROTECTION
  3. SECURITY FOR GROWTH
- 

[View more on our website](http://www.Lenovo.com/ThinkShield)  
[www.Lenovo.com/ThinkShield](http://www.Lenovo.com/ThinkShield)

Smarter  
technology  
for all

Lenovo



Powered by Intel® vPro™ platform

# PREVENTING HUMAN ERROR

Smarter  
technology  
for all

Lenovo

Sometimes students or even professors make mistakes—losing devices, clicking on things they shouldn't, or even disabling protections that get in their way. But those mistakes—innocent as they may be—can bring down an entire institution. Given the prevalence of human errors, hackers use it as a key vector for “social engineering” tactics like imposter phishing emails. It's their easiest way of gaining access to your data.

Lenovo ThinkShield helps to prevent and contain human error before it turns into a devastating breach. Our solutions give IT admins more visibility into endpoints, offer self-healing capabilities and “one-click” fixes, provide easier and more secure authentication, and use intelligence to assess risk.

## ABSOLUTE

Provides persistent visibility into endpoints so that IT admins can apply remote security measures to protect each device and the data it contains.

## BITLOCKER ENCRYPTION<sup>4</sup>

Protects against loss of your institution's information by encrypting data on your devices, even when a device is lost or stolen.

## WINDOWS DEFENDER SYSTEM GUARD<sup>5</sup>

Ensures that only trusted software can run during start-up, isolates sensitive services and data, and makes certain low-level tampering can be detected and remediated without impact.

## INTEL® AUTHENTICATE SOLUTION

81% of breaches used weak or stolen passwords.<sup>6</sup> Intel® Authenticate Solution enforces authentication rules and tokens in hardware, where information is more difficult to expose—with up to 8 modes of authentication (from geo-location authentication to facial recognition via Windows 10).

## LENOVO WI-FI SECURITY

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

**48%**

of breaches originate from  
**HUMAN ERROR.**<sup>2</sup>

### LEADING BIOS SECURITY

With Intel® Hardware Shield

Leveraging the power of the Intel® vPro™ platform, Lenovo ThinkShield provides BIOS that can self-heal in the event of corruption by human error or attack. And unlike other PC manufacturers, we did not build in a backdoor, so BIOS can be administered securely. If you're skeptical, you can arrange a look through the 2,000,000+ lines of code in our secure BIOS Reading Room,<sup>3</sup> which can then be assigned a unique signature for the BIOS you reviewed for deployment.

In 2015,  
one click from an  
employee at Anthem  
**EXPOSED THE PERSONAL  
DATA OF 78 MILLION PEOPLE,**  
costing the company  
an estimated

**\$100+**  
million.<sup>1</sup>

<sup>1</sup> Fortune: “Anthem's Historic 2015 Health Record Breach Was Likely Ordered by a Foreign Government.”  
<http://fortune.com/2017/01/09/anthem-cyber-attack-foreign-government/>

<sup>2</sup> Kaspersky: “Small Business IT Security Practical Guide.”

[https://go.kaspersky.com/rs/802-IJN-240/Images/Small\\_Business\\_Practical\\_Guide.pdf?aiid=466030355](https://go.kaspersky.com/rs/802-IJN-240/Images/Small_Business_Practical_Guide.pdf?aiid=466030355)

<sup>3</sup> BIOS Reading Room service is available for additional charge

<sup>4</sup> Requires TPM 1.2 or greater for TPM-based key protection

<sup>5</sup> Windows Defender System Guard's boot time integrity protection requires the use of UEFI 2.31 or greater with Secure Boot. The optional remote integrity validation capability using the Windows Defender System Guard cloud service requires TPM 1.2 or greater and a management system that supports remote attestation capabilities (e.g., Intune and System Center Configuration Manager).

<sup>6</sup> 2017 Verizon Data Breach Investigations Report

<https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf>



Powered by Intel® vPro™ platform

# TRUE END-TO-END PROTECTION

Smarter  
technology  
for all

Lenovo

It's impossible to secure every single moment of a device's lifecycle. But Lenovo ThinkShield goes further to secure the moments that are out of your control—starting with trusted suppliers and secure manufacturing. PCs can face threats before they ever arrive at your door. So we built rigorous, trackable, and auditable security standards into every step of our secure and transparent supply chain.

At Lenovo, security begins with development and continues through the supply chain and the full lifecycle of every device—from development through disposal.

## DEVELOPMENT

Every Think device is engineered from the ground up for security. And every smart component comes from a trusted supplier.

## LENOVO TRUSTED SUPPLIER PROGRAM

A secure process built into the development, manufacture, and delivery of our products. The supply chain begins with the management and control of a qualified supplier base, which provides qualified and secure components for use in development and manufacturing.

## SECURE PACKAGING

Physical security via tamper-evident packaging, qualified transportation, and secure tracking.

## SECURE DISPOSAL

At a device's end-of-life, we wipe drives and securely recycle parts.

## REMOTE FEATURES

Solutions like Windows Information Protection<sup>3</sup> and others allow for remote wiping of disks. ThinkShield also allows for remote patching of vulnerabilities and "one-click" fixes pushed in bulk.

### INTEL® TRANSPARENT SUPPLY CHAIN

In addition to our own rigorous manufacturing oversight and work with trusted suppliers, Lenovo ThinkShield is proud to be the first to partner with Intel to provide Intel® Transparent Supply Chain.<sup>4</sup> This new service option provides visibility into the authenticity of your PCs, from factory to delivery, and traceability to give you confidence that components have not been tampered with.

In 2016, a doctor lost an unencrypted laptop, **EXPOSING PATIENTS TO IDENTITY FRAUD.**<sup>1</sup>

**30,972**

**41%**

of all breaches from 2005 to 2015 were **CAUSED BY LOST DEVICES.**<sup>2</sup>

1 Computer World: "Idaho utility hard drives and data turn up on eBay." <https://www.computerworld.com/article/2555144/idaho-utility-hard-drives----and-data----turn-up-on-eBay.html>

2 Trend Micro: "Follow the Data: Dissecting Data Breaches and Debunking the Myths." <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data>

3 Windows Information Protection requires either MDM or System Center Configuration Manager to manage settings. Sold separately.

4 Intel® Transparent Supply Chain is available for additional charge



Powered by Intel® vPro™ platform



# HOW DOES INVESTING IN SECURITY IMPACT YOUR INSTITUTION?

Smarter  
technology  
for all

Lenovo

Choosing more efficient and reliable IT security partners drives productivity, innovation, and growth in three ways.

## PRODUCTIVITY

Lenovo ThinkShield lets you make better use of IT resources. With solutions that automate and simplify—including self-healing patches, easy-to-implement multifactor login, and automatic Wi-Fi security monitoring—ThinkShield frees up IT's time to focus on more strategic tasks.

**1K+**  
**HOURS**

### TAKE BACK TIME

Organizations are spending more than 1,000 hours a week to detect and contain insecure endpoints.<sup>1</sup>

**68%**

### FOCUS ON THE FUTURE

68% of malware containment doesn't require human intervention and can be automated.<sup>2</sup>

## INNOVATION

Stronger security is a platform for progress, enabling the use of new and emerging technologies without compromising data safety. ThinkShield protects the entire endpoint ecosystem so that as IoT and other technologies grow the threat surface, IT can cover more ground, more effectively.



## GROWTH

A breach can snowball beyond its immediate impact and into exponential consequences. In addition to the cost of repairing the damaged technology ecosystem and restoring data, consider: the cost of notifying and assisting those affected; the impact to costly actions needed to rectify the effects; HIPPA, GDPR, or other regulatory fines; and the cost of upgrading your security retroactively.

The incremental costs of end-to-end security pale in comparison to the average cost of a data breach: over \$4 million.<sup>3</sup>

**30%**

### NEVER STOP THE CLOCK

Three out of ten organizations say a single hour of production downtime costs \$1 million or more.<sup>4</sup>

**23**  
**DAYS**

### FIND MORE MONTHS IN THE YEAR

An average of 23 days are lost recovering from every ransomware attack.<sup>5</sup>

1,2 Ponemon Institute: The Cost of Insecure Endpoints (<http://bit.ly/InsecureEndpoints>)  
3 Ponemon Institute: 2018 Cost of a Data Breach (<http://bit.ly/CostofDataBreach>)  
4 ITIC: 2019 Cost of Hourly Downtime  
5 IBM: 2017 Global COB Report Final (<http://bit.ly/GlobalCOBReport>)



Powered by Intel® vPro™ platform



# WORKING TOGETHER TO FORTIFY YOUR INSTITUTION

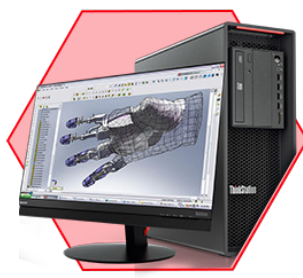
Smarter  
technology  
for all

Lenovo

Lenovo's ThinkShield, Intel, and Microsoft link arm-in-arm to defend your institution 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 campus protected.



[Explore ThinkPad  
& ThinkCentre](#)



[Explore Workstations](#)



[Explore ThinkSmart](#)



[Explore Data Center](#)

## DON'T LEAVE YOUR INSTITUTION UNPROTECTED

We'll help customize the right solution for you.

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

[Request A Consultation](#)



Powered by Intel® vPro™ platform