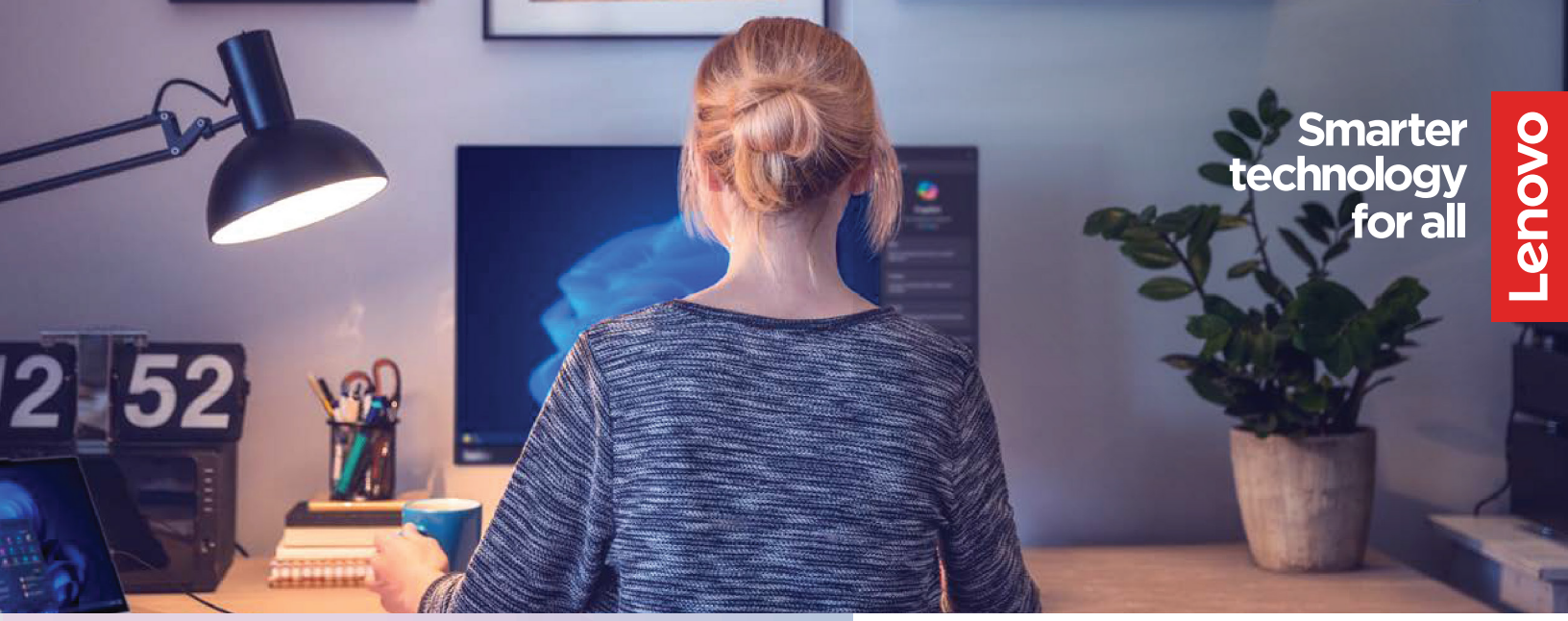


Future-proof and protect your fleet, starting with silicon to cloud security

Defend your business without impacting end-user productivity with Intel vPro® platform on Lenovo AI PCs that keeps your fleet secure with hardware-enhanced protection right out of the box. It comes with built-in remote management capabilities and can further optimize the AI-powered security features of Windows 11. Beyond the hardware and OS, Lenovo ThinkShield platform provides AI-enhanced end-to-end endpoint protection so that you can work from anywhere with extended detection and response against evolving cyberthreats.

Take advantage of this multilayered security protection by upgrading to Windows 11 on devices like Lenovo ThinkPad series powered by Intel® Core™ Ultra processor. The best time to do so is now – before the support for Windows 10 ends in October 2025.

Intel® Core™ Ultra 7 processor unlocks new AI experiences. Step up to Intel vPro®, Evo™ Edition that's designed for what IT needs and users want

"Today's attackers do not break in; they log in." Microsoft, Digital Defense Report 2023

Cybercriminals are hard at work devising more sophisticated, more damaging tactics, taking advantage of the new hybrid workplace and its vulnerabilities. In fact, human-operated ransomware attacks are up **more than 200%.**[1] And the average cost of a data breach has **exceeded $5 million.**[2] All told; the global cost of cybercrime is projected to hit an annual

$10.5 trillion by 2025.[3]

But technology industry leaders are hard at work, too — developing breakthrough security solutions and harnessing the power of AI to safeguard devices, data, and organizations. There's growing recognition of cybersecurity as an essential business requirement, not just a technology feature. Today's solutions should be secure out of the box, with protections enabled — security by design and by default.

Did you know 99+% of attacks are preventable?

It's easy to harden security across your entire fleet with the latest Lenovo AI PCs – such as the ThinkPad X1 Carbon – running on the Intel vPro® platform and Windows 11.

Designed for a dispersed remote workforce, Intel vPro® enables IT teams to protect PCs effortlessly – with remote management features to keep devices patched and updated with the latest security measures at all times. All Lenovo AI PCs are equipped with ThinkShield comprising an extensive portfolio of secure solutions, software, and services. Powered by AI, ThinkShield evolves with the modern threat landscape to protect your business and adapt to the needs of the workforce. You can also rest assured that with Lenovo's Zero Trust Supply Chain, all hardware components and software in devices are protected against tampering, from the factory floor straight to your employees' hands.

Gain all the advantages of the Intel vPro® platform and more when you're running Windows 11. Make the move before Windows 10 end of support in October 2025 – and with Lenovo devices like the ThinkPad X1 Carbon, you gain all the advantages of Windows 11 as soon as possible. Intel® Core™ Ultra processor unlocks new AI experiences. Step up to Intel vPro®, Evo™ Edition that's designed for what IT needs and users want.

Lenovo ThinkPad X1 Carbon

Big benefits from the big (but easy) upgrade to Windows 11

58% drop in security incidents[4]

20% reduced risk of a successful attack[5, 6]

3.1x fewer firmware attacks[4]

intel CORE ULTRA 7

intel vPRO EVO EDITION

Intel® Core™ Ultra 7 processor unlocks new AI experiences. Step up to Intel vPro®, Evo™ Edition that's designed for what IT needs and users want

Smarter technology for all

Lenovo

Proactive, intelligent protection

Your employees can work smarter, faster and more securely with Lenovo AI PCs running on the Intel vPro® platform. From intelligent threat detection to automated responses, our AI PCs are packed with robust protection against emerging cyber threats.

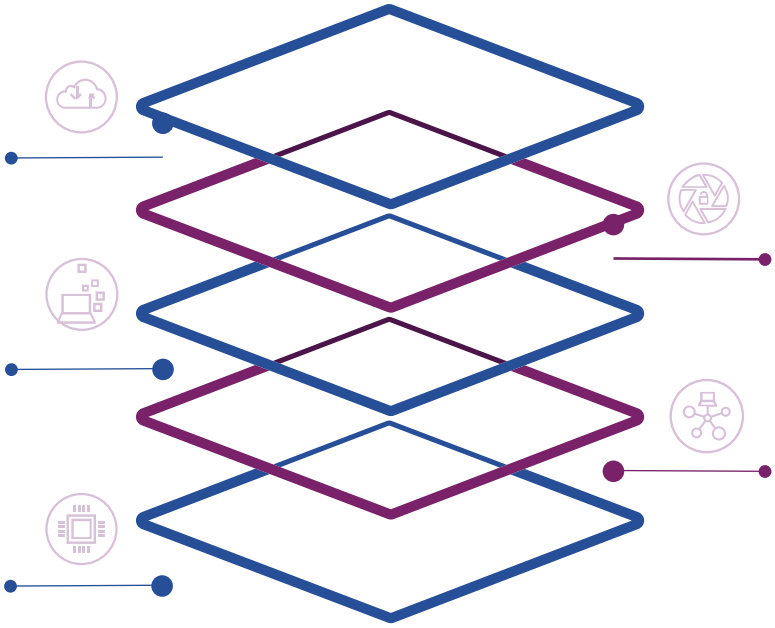
Engineered to support remote work through zero-trust security principles, Intel vPro® ensures users are authenticated and assesses the health of each device and access to applications. This is further enhanced with the multi-layered, end-to-end protection from Lenovo ThinkShield and AI-driven security features on Windows 11. Lenovo, Intel® and Microsoft hardware and software work together to protect endpoints and sensitive data from the PC chip to the cloud — a streamlined solution that contributes to **25% better productivity for IT and security teams.**[5]

Layer upon secure layer

Cloud
- Protecting work information
- Protecting personal information

Application
- Application and driver control
- Application isolation

Hardware (chip)
- Hardware root of trust
- Silicon-assisted security



Identity
- Passwordless sign-in
- Advanced credential protection
- Privacy

Operating system
- Encryption and data protection
- Network security
- Virus and threat protection
- System security

intel CORE ULTRA 7

intel vPRO EVO EDITION

Intel® Core™ Ultra 7 processor unlocks new AI experiences. Step up to Intel vPro®, Evo™ Edition that's designed for what IT needs and users want

Smarter technology for all

Lenovo

Targeting the top-dog threat

74% of all breaches are due to human error, privilege misuses, stolen credentials, or social engineering — all of which make your employees prime phishing targets, with credential theft the most prevalent attack vector at **50%**.[7]

Intel Threat Detection Technology (TDT) helps prevent attacks including ransomware and cryptomining by using hardware-based monitoring to detect and prevent malicious activity. It works by gathering and analyzing raw data to help identify polymorphic malware, cryptomining, fileless scripts, and other targeted attacks in real time, and with minimal end-user impact.

Intel TDT uses machine learning (ML) heuristics to reduce false-positive alerts. It also helps improve the performance of endpoint detection and response (EDR) solutions that continuously monitor endpoint devices, such as Microsoft Defender for Endpoint, CrowdStrike, and Fidelis. It does this by offloading memory scanning functions from the CPU to an auxiliary graphics processing unit (GPU), making security software solutions less resource-intensive and providing a better overall employee UX.

With Intel TDT, EDR solutions can gain between 4x and 7x in memory-scan performance over the CPU, allowing for a broader use of scanning when needed.[8]

Lenovo
ThinkPad X1 2-in-1

AI-enhanced security is evolving

Artificial Intelligence is making its mark on cybersecurity — by automating and augmenting threat detection, response, analysis, and prediction. And there are many new capabilities on the horizon. But there can be risks — to compliance, privacy, and more — when companies short-circuit the learning curve in the rush to jump into production. A well-researched approach, possibly including a trust, risk, security management (TRiSM) program, can integrate governance from the start and help you succeed.

Windows Hello and TPM 2.0 work together to shield identities. Passwordless authentication frees you from the risk of lost or stolen passwords with options from device-specific PIN codes to fingerprints to facial recognition. Enhanced phishing protection with Microsoft Defender SmartScreen is built directly into the OS and alerts users when they're entering Microsoft credentials into a malicious application.

Step up to new capabilities to be more secure

Our pocket-to-cloud suite of AI-powered Lenovo Digital Workplace Solutions can help you create a more secure and productive hybrid workplace that elevates employee experience. Our comprehensive security includes ThinkShield protection, detection, and alerting on BIOS level attacks to secure your firmware and hardware. And Lenovo's Zero Trust Supply Chain solution protects against tampering right from the factory floor. Our innovative devices running on Intel® Core™ Ultra processors and Windows 11 comes with layers of security from chip to cloud to deliver new vigilance now and prepare your organization for a stronger future.

Discover more

Intel® Core™ Ultra 7 processor unlocks new AI experiences. Step up to Intel vPro®, Evo™ Edition that's designed for what IT needs and users want

Smarter technology for all

Lenovo

Action steps on the path to security resilience

Here's a checklist of things to consider in your strategic planning for cybersecurity.

- ☐ **1. Start** your Windows 11 migration now to ensure the security of a supported OS and benefit immediately from the innovations and future-forward security features. End of support for Windows 10 is October 14, 2025.
- ☐ **2. Implement** passwordless authentication for all your users — this is one of the most effective steps you can take to thwart identity compromise.
- ☐ **3. Consider** developing a return on mitigation (ROM) framework to help prioritize your actions and identify those that could deliver high impact with low effort or resources.
- ☐ **4. Understand** how hardware and software work together to secure your organization and choose proven technology solutions vetted to work together seamlessly.
- ☐ **5. Gain** a thorough understanding of the risks and rewards if you are headed for significant AI application and model deployment. Evaluate whether a trust, risk, security management (TRiSM) program is appropriate.

Lenovo ThinkPad T14

* Timing of feature delivery and availability varies by market and device. Use Copilot with a Microsoft Account or use Copilot with commercial data protection at no additional cost by signing into a work or school account (Microsoft Entra ID) with Microsoft 365 E3, E5, F3, A3 or A5 for faculty, Business Premium, and Business Standard. Coming to more Entra ID users over time.

Sources

1 "Microsoft Digital Defense Report," October 2023

2 SonicWall, "2024 SonicWall Cyber Threat Report," 2024

3 Cybercrime Magazine, "Cyberwarfare In The C-Suite," November 2020

4 Windows 11 results are in comparison with Windows 10 devices. Techaisle, "Windows 11 Survey Report," February 2022

5 Commissioned study delivered by Forrester Consulting, "The Total Economic Impact™ of Windows 11 Pro Devices," December 2022. Note: Quantified benefits reflect results over three years combined into a single composite organization that generates $1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices.

6 Microsoft Intune and Azure Active Directory required; sold separately

7 Verizon, "2023 Data Breach Investigations Report," 2023

8 IOActive. "13th Generation Intel Core Attack Surface Study." Commissioned by Intel. March 2023.

Intel® Core™ Ultra 7 processor unlocks new AI experiences. Step up to Intel vPro®, Evo™ Edition that's designed for what IT needs and users want

Smarter technology for all