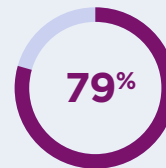


Smarter
technology
for all

Lenovo



Lenovo ThinkPad L14



79% of institutions surveyed reported a ransomware attack in the previous year.

Higher education remains highly attractive and highly vulnerable to cyberattacks, with 79% of institutions surveyed reporting a ransomware attack in the previous year.¹ In fact, according to Malwarebytes, 2023 was the worst ransomware year on record.² The average cost of a data breach for the education and training sector has reached \$3.65 million.³ Not surprisingly, data security was ranked the second most pressing risk faced by college leaders.⁴

Protecting student privacy, sensitive research data, and the continuity of academic and administrative work has never been more important or more challenging.

Intel® Core Ultra processors and Intel vPro® bring unmatched security capabilities and manageability to your institution, making it easier to manage your devices and let the educators and students shine.

Strengthen and simplify security across your higher education institute

Protect your borderless campus while improving user experience and enhancing productivity with Lenovo devices powered by Intel® and Microsoft.

Lenovo makes it simple for you to future-proof your campus fleet with innovative devices powered by up to Intel® Core™ Ultra processors and Windows 11 Pro, and a full suite of trusted services to simplify deployment and management.

Our devices are optimized for Windows 11, enabling you to easily take advantage of the new AI-enhanced security and productivity features.



intel
vPRO

Intel® Core Ultra unlocks new AI experiences. Step up to Intel vPro® for an unrivaled business PC solution.



Did you know that more than 99% of attacks are preventable?

Research says that the vast majority of successful cyberattacks could be thwarted by implementing fundamental security practices like Zero Trust principles, multifactor authentication, extended detection and response (XDR), up-to-date systems, and data protection.⁵

Lenovo offers a wide range of powerful and accessible devices running on up to Intel® Core™ Ultra processors devices and Windows 11 Pro that come with robust security features to lighten the load for IT on all these basics. They do so through hardware-enabled security by Intel® and adding enhanced capabilities like Copilot* in Windows with commercial data protection to make your higher education institute more resilient. It's the perfect foundation for a modern cybersecurity strategy.

The first step to making sure you're staying ahead and protected from the ever evolving cyberthreats is to make sure your device fleet is running a supported, updated OS like Windows 11. And when you choose Lenovo as your trusted technology partner, we help you seamlessly gain the advantages of the most secure Windows OS to date - with our innovative devices like the ThinkPad series running on up to Intel® Core™ Ultra processors devices and optimized for Windows 11 Pro.

The most secure Windows ever, Windows 11 provides powerful protection that works in tandem with software to silicon security from Intel® and the comprehensive ThinkShield suite to give IT teams a long-awaited edge.



Lenovo ThinkPad E14

Future-proof your higher education institution and take control of the IT environment with Lenovo devices running on up to Intel® Core™ Ultra processors and Windows 11 Pro



58% drop in security incidents⁶



20% reduced risk of a successful attack^{7,8}



3.1x fewer firmware attacks⁶



intel
vPRO

Intel® Core Ultra unlocks new AI experiences. Step up to Intel vPro® for an unrivaled business PC solution.

Smarter
technology
for all

Lenovo

Proactive, intelligent protection

Windows 11 is designed with layers of protection, many of them turned on by default, so you don't have to think about security settings. And neither do your students, faculty, researchers, and staff, who remain secure wherever they're working. Hardware and software components from Lenovo, Intel® and Microsoft 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.**⁷



Layer upon secure layer

Cloud

- ✔ Protecting school information
- ✔ Protecting student and staff 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
vPRO

Intel® Core Ultra unlocks new AI experiences. Step up to Intel vPro® for an unrivaled business PC solution.

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 users prime phishing targets. Credential theft is the most prevalent attack vector at 50%.⁹

Lenovo adopts a comprehensive approach to security that delivers new vigilance now and prepares your institution for a stronger future. Our innovative devices powered by up to Intel® Core™ Ultra processors devices and Windows 11 Pro feature ThinkShield protection, detection, and alerting on BIOS-level attacks to secure firmware and hardware. Lenovo's Zero Trust Supply Chain solution protects against tampering right from the factory floor.

Windows 11 offers a Zero Trust-ready, comprehensive security profile, comprising mission-critical application safeguards, Windows Firewall, and silicon-assisted secure kernel, to strengthen security posture across your borderless campus, mitigate risks and help protect your students, faculty, and staff.

Build a stable learning environment that's more secure with our professional-grade PCs backed by Intel vPro® for enhanced protections and remote manageability. Empowering staff with the tools they deserve, our devices ensure smooth transitions between tasks and devices. Rest easy with seamless manageability and protection.

Stay protected from silicon to software

Intel® processors are secure at the core, designed to meet specific challenges centered around three key priorities:

- ④ Foundational security: critical protection to help verify trustworthiness of devices and data
- ④ Workload and data protection: trusted execution for hardware-isolated data protection
- ④ Software reliability: platforms that help protect against a range of cybersecurity threats

AI-enhanced security is evolving

Artificial intelligence is making its mark on higher education, from compute-intensive coursework and research to administrative insights and efficiencies. AI also benefits cybersecurity — by automating and augmenting threat detection, response, analysis, and prediction. And there are many new capabilities on the horizon.

* 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 Sophos, "State of Ransomware in 2023," July 2023
- 2 Malwarebytes, "2024 State of Ransomware in Education," January 2023
- 3 IBM Security, "Cost of a Data Breach Report," 2023
- 4 High Ed Dive, "Here are the top risks college leaders are worried about this year," January 2023
- 5 "Microsoft Digital Defense Report," October 2023
- 6 Windows 11 results are in comparison with Windows 10 devices. Techaisle, "Windows 11 Survey Report," February 2022
- 7 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.
- 8 Microsoft Intune and Azure Active Directory required; sold separately.
- 9 Verizon, "2023 Data Breach Investigations Report," 2023

© Lenovo 2025. All rights reserved. v1.00 March 2025.



intel
vPRO

Intel® Core Ultra unlocks new AI experiences. Step up to Intel vPro® for an unrivaled business PC solution.

Smarter
technology
for all

Lenovo



Action steps on the path to security resilience

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

- 1.** Deploy the latest Lenovo devices powered by Intel and Windows 11 Pro to benefit from future-forward security features that keep your students, staff and faculty safe.
- 2.** Implement passwordless authentication for all your students, faculty, staff, and researchers. This is one of the most effective steps you can take to thwart identity compromise. Take it one step further with training on email and online best practices for identity protection.
- 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 institution, and choose proven technology solutions vetted to integrate seamlessly.
- 5.** If you are headed for significant AI application and model deployment, gain a thorough understanding of the risks and rewards. Evaluate whether an AI trust, risk, and security management (TRISM) program is appropriate.

Lenovo can help make Windows 11 migration across your higher education institute simple and successful.

Learn more at edvision.lenovo.com/a-smarter-way-to-learn

© Lenovo 2025. All rights reserved. v1.00 March 2025.



intel
vPRO

Intel® Core Ultra unlocks new AI experiences. Step up to Intel vPro® for an unrivaled business PC solution.

Smarter
technology
for all

Lenovo