# Put Windows 11 at the center of your security strategy

Upgrade before the Windows 10 end-of-support deadline **October 14, 2025** for improved user experience, new productivity enhancements, and security innovations — all backed by Copilot* in Windows.

Windows 11

Lenovo recommends
Windows 11 Pro for Business.

Windows 11 multifactor authentication and advanced anti-malware tools help to thwart attacks and protect critical data, making educational institutions more resilient against cyberthreats.

Microsoft, Digital Defense Report 2023
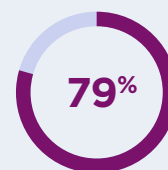
79% of institutions surveyed reported a ransomware attack in the previous year.

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.

Did you know 99+% of attacks are preventable?

According to Microsoft,[5] 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.

Lenovo Windows 11 devices lighten the load for IT on all these basics — plus added and enhanced capabilities like Copilot* in Windows with commercial data protection to make your institution more resilient. It's the perfect foundation for a modern cybersecurity strategy.

Consider starting the migration planning process now, well before the **October 2025** end of service for Windows 10, to make sure you're running a supported, updated OS. With Lenovo devices like the ThinkPad® family (including the X1 2-in-1 and P1 mobile workstation), you can gain all the advantages of Windows 11 as soon as possible.

This is the most secure Windows ever, backed by powerful protection, working in tandem with Lenovo ThinkShield to give IT teams a long-awaited edge.

Lenovo ThinkPad X1 2-in-1

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

58% drop in security incidents[6]

20% reduced risk of a successful attack[7,8]

3.1x fewer firmware attacks[6]

Windows 11

Lenovo recommends Windows 11 Pro for Business.

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. Lenovo 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.**[7]

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

Windows 11

Lenovo recommends
Windows 11 Pro for Business.

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%. Windows 11 equips you to be proactive and realize nearly 3x fewer identity theft incidents.[9]

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.

Intune Endpoint Privilege Management runs all users as standard, elevating privileges only when needed, to limit your attack surface.**

These features help you avoid phishing-related identity compromises. But they're just part of what the Zero Trust-ready Windows 11 offers to raise your security profile — from mission-critical application safeguards to Windows Firewall to silicon-assisted secure kernel.

Lenovo's 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. Lenovo Windows 11 Think devices deliver new vigilance now and prepare your institution for a stronger future.

Step up to new capabilities to be more secure

Lenovo places the highest priority on security. Our comprehensive ThinkShield solution is continuously evolving to stay ahead of the rapidly changing threat landscape. In strong partnership with Microsoft, we are delivering Windows 11 devices with layers of security from chip to cloud.

When you're ready for the next steps, we're here to help — with guidance, services, and technology that optimize the power of Windows 11 for a more secure and resilient digital future on your campus and beyond.

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.

** Microsoft Intune and Azure Active Directory (now called Microsoft Entra ID) required; sold separately.

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

Windows 11

Lenovo recommends Windows 11 Pro for Business.

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.** 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 is October 14, 2025.

☐ **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 your Windows 11 migration simple and successful.

Learn more and get started today.

Windows 11

Lenovo recommends
Windows 11 Pro for Business.

Smarter technology for all

Lenovo