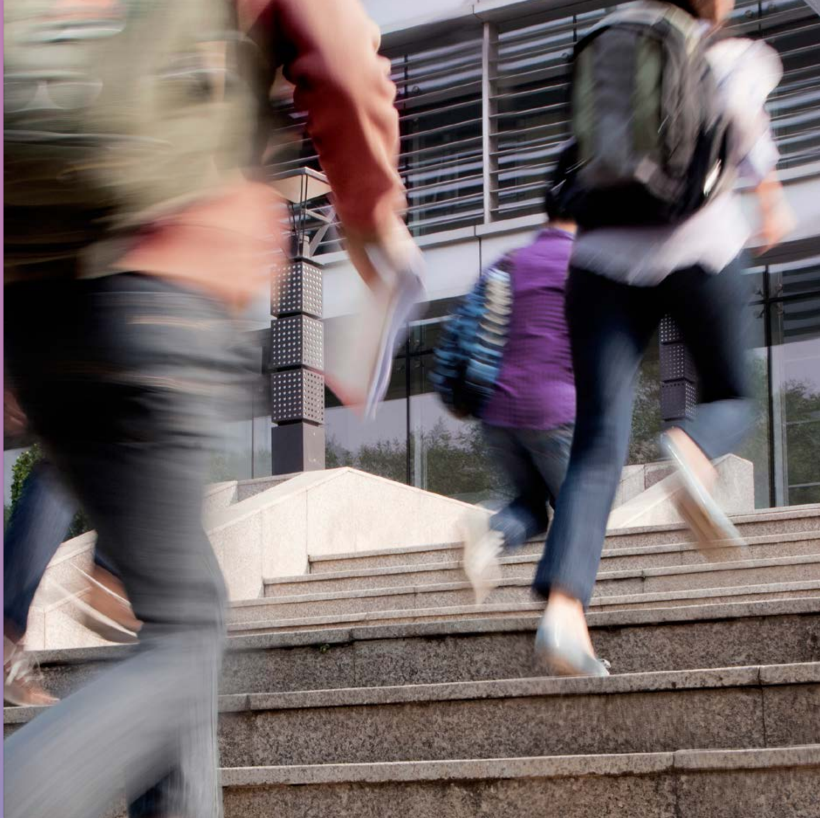
Enhance K-12 education security with Windows 11

Robust cybersecurity. Advanced AI. Tailored for education.



Cybercriminals are increasingly targeting vulnerable systems, and educational institutions are not immune. Schools face the dual challenge of protecting sensitive student data and maintaining a secure learning environment.

With the rise of digital learning tools and hybrid classrooms, the attack surface has expanded, making schools attractive targets for cybercriminals. Human-operated ransomware attacks have surged by over 200%,[1] and the average cost of a data breach now exceeds $5 million.[2] Globally, cybercrime is expected to cost $10.5 trillion annually by 2025.[3]

Fortunately, technology leaders like Microsoft are developing innovative security solutions using advanced AI to protect devices, data, and educational institutions. Windows 11 brings these cutting-edge security features to the forefront, offering a robust foundation to safeguard K-12 environments against the ever-evolving threat landscape. This is not just an upgrade; it's a proactive step toward a more secure and resilient digital future for schools.

> 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**

Human-operated ransomware attacks have surged by over

200%

The average cost of a data breach now exceeds

$5M

Windows 11

Secure and scalable IT

Smarter technology for all

Lenovo

Did you know 99+% of attacks are preventable?

Microsoft reports that most cyberattacks can be prevented by adopting basic security practices such as Zero Trust principles, multifactor authentication, extended detection and response (XDR), keeping systems updated, and protecting data.[1]

Lenovo Windows 11 Pro devices simplify these security fundamentals for school IT departments, adding enhanced capabilities like Copilot* in Windows with commercial data protection to boost resilience. It's the ideal foundation for a modern cybersecurity strategy in education.

Start planning your migration to Windows 11 now, ahead of the Windows 10 end of service in **October 2025**, to ensure your systems are supported and updated. With Lenovo devices like the ThinkPad® family (including X1 Carbon, X1 2-in-1, T14, and T16), you can benefit from the Windows 11 advantages immediately.

Windows 11 is the most secure Windows ever, providing powerful protection in collaboration with ThinkShield to give school IT teams a significant edge.

Windows 11

Secure and scalable IT

Lenovo ThinkPad X1 Carbon

Windows 11: Easy upgrade, major gains for K-12 schools

58% drop in security incidents[4]

20% reduced risk of a successful attack[5]

3.1x fewer firmware attacks[4]

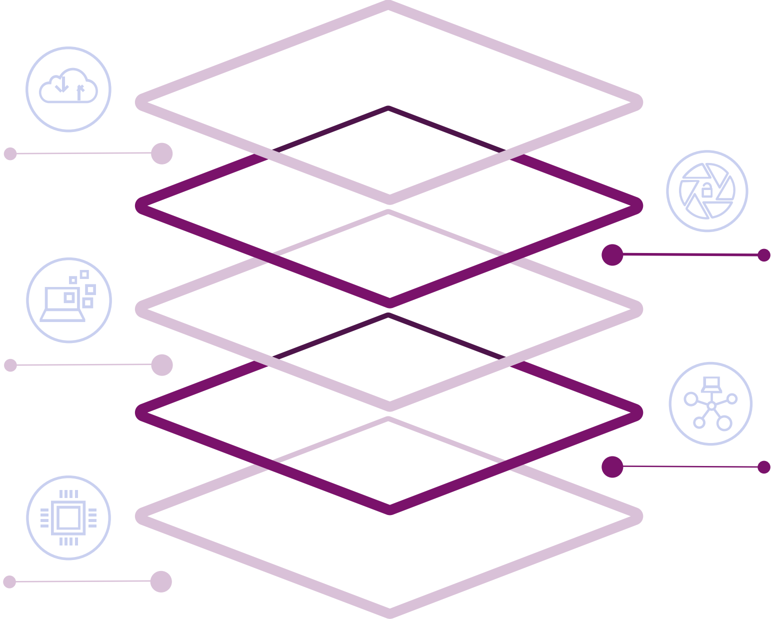
Smarter technology for all

Lenovo

Proactive, intelligent protection

Windows 11 is built with multiple layers of protection, many enabled by default, so school staff don't need to worry about security settings. Lenovo and Microsoft hardware and software work together to protect endpoints and sensitive data — enhancing IT operational productivity. In fact, **49% of K-12 schools using Microsoft Windows devices report reduced IT support and maintenance costs.[6]**

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

Windows 11

Secure and scalable IT

Smarter technology for all

Lenovo

Heading off the biggest threats

74% of all breaches are due to human error, privilege misuse, stolen credentials, and social engineering, making students and staff prime phishing targets. Credential theft is the most common attack vector at 50%. Windows 11 reduces identity theft incidents by nearly 3x.[7]

Windows Hello and TPM 2.0 protect identities with passwordless authentication, offering options from PIN codes to fingerprints to facial recognition. Enhanced phishing protection with Microsoft Defender SmartScreen alerts users when they enter Microsoft credentials into a malicious application. **Intune Endpoint Privilege Management** ensures users run with standard privileges, elevating only when needed, to minimize attack surfaces.**

These features help avoid phishing-related identity compromises, but they're just part of the Zero Trust-ready Windows 11 comprehensive security profile. It also includes mission-critical application safeguards, Windows Firewall, and silicon-assisted secure kernel.

Lenovo's comprehensive approach to security provides ThinkShield protection, detection, and alerting on BIOS-level attacks to secure firmware and hardware. Lenovo's Zero Trust Supply Chain solution protects against tampering from the factory floor. Lenovo Windows 11 Think® devices offer new vigilance now and prepare schools for a secure future.

Windows 11

Secure and scalable IT

Step up to new capabilities

Lenovo prioritizes security, continuously evolving our ThinkShield solution to stay ahead of threats. In partnership with Microsoft, we deliver Windows 11 devices with security from chip to cloud.

When you're ready to take the next steps, we're here to help with guidance, services, and technology to optimize the power of Windows 11 for a secure and resilient digital future.

AI-enhanced security

Artificial intelligence is transforming cybersecurity — automating and enhancing threat detection, response, analysis, and prediction. However, risks exist to compliance, privacy, and more if AI deployment is rushed. A well-researched approach, potentially including a trust, risk, and security management (TRiSM) program, can integrate governance from the start and help schools succeed.

* Timing of feature delivery and availability vary 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 Microsoft, "Digital Defense Report," October 2023
2 SonicWall, "2024 SonicWall Cyber Threat Report," 2024
3 Cybercrime, "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 Microsoft Intune and Azure Active Directory required; sold separately.
6 Commissioned study delivered by Forrester Consulting, "The Total Economic Impact™ of Microsoft Windows Devices For K-12 Education," July 2023
7 Verizon, "2023 Data Breach Investigations Report," 2023

Smarter technology for all

Lenovo

CHECKLIST

9 steps toward K-12 education security resilience

Here's an action plan for your strategic cybersecurity planning.

- □ **1. Start your Windows 11 migration now.** Ensure your school's IT infrastructure is secure and up to date by migrating to Windows 11 before Windows 10 support ends on October 14, 2025. Early adoption will allow your school to benefit immediately from the latest security features and innovations.

- □ **2. Implement passwordless authentication.** Transition all teachers, staff, and students to passwordless authentication methods such as PIN codes, fingerprints, or facial recognition. This significantly reduces the risk of identity theft and makes logging in easier and more secure for users.

- □ **3. Develop a cybersecurity education program.** Educate students, teachers, and staff about basic cybersecurity practices and the importance of maintaining secure online behaviors. Regular training can reduce the likelihood of human error that leads to security breaches.

- □ **4. Prioritize critical security updates.** Ensure all school devices and systems are regularly updated with the latest security patches. This helps protect against known vulnerabilities and keeps your IT environment resilient against emerging threats.

- □ **5. Leverage AI for threat detection.** Utilize AI-driven security solutions to automate and enhance threat detection, response, and analysis. This can help your IT team manage security more effectively and focus on proactive measures.

- □ **6. Implement Zero Trust principles.** Adopt a Zero Trust security model, ensuring that all users, devices, and applications are continuously verified before granting access. This helps protect sensitive data and systems from unauthorized access.

- □ **7. Collaborate with trusted partners.** Work with reliable technology partners to integrate hardware and software solutions that are proven to work seamlessly together. This ensures a cohesive security strategy that covers all aspects of your IT infrastructure.

- □ **8. Establish a response plan for security incidents.** Develop and regularly update an incident response plan to quickly and effectively address any security breaches. Having a clear protocol helps minimize damage and recover swiftly from potential attacks.

- □ **9. Assess and manage AI deployment risks.** Before implementing AI applications widely, evaluate the associated risks and benefits. Consider adopting a trust, risk, and security management (TRiSM) program to ensure responsible and secure AI deployment.

Lenovo can help make your Windows 11 migration simple and successful.

Learn more and get started today.

Windows 11

Secure and scalable IT

Smarter
technology
for all

Lenovo