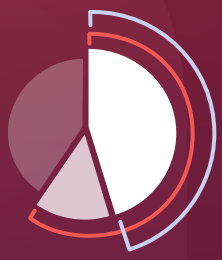
The Higher Ed State of Cybersecurity

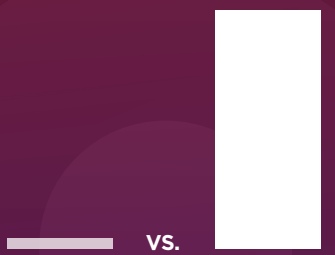
Why upgrading tech and security infrastructure is more important than ever for colleges and universities.

When you leave your home or office for an extended period, do you lock the door? Of course you do, because that simple turn of the lock safeguards your belongings and sensitive information. But in a world where most sensitive information is being stored digitally, physical security measures alone can't guarantee data safety.

Rising Cyber Threats to Higher Education



In 2021, 64% of colleges and universities reported ransomware attacks. 74% of those attacks succeeded.



$112,000 in ransom payments

$2.7 million per incident

Institutions pay $112,000 on average in ransom payments, but the total cost of recovery averages to about $2.7 million per incident.

Since the beginning of pandemic-driven remote learning, the higher education industry has been thrust into the cybersecurity spotlight and hasn't stepped out. In fact, according to Microsoft's Global Threat Activity tool, over 80% of all global malware encounters reported in the last 30 days have been attributed to the education industry. In addition, 64% of colleges and universities **reported experiencing a ransomware attack in 2021**. **And, of those ransomware attacks,** 74% succeeded.

Even more staggering than the sheer number of attacks is the amount of money higher education institutions have paid to resolve them. On average, **each attack** costs institutions $112,000 **in ransom payments.** However, the **overall cost to resolve and recover from these attacks** averages to about $2.7 million **per incident**, when you consider data recovery and liability costs.

Unfortunately, these aren't the only cybersecurity threats looming over colleges and universities.

Due to the nature of work being completed in these institutions, many have become targets for theft of intellectual property and research. And institutions with affiliated hospitals and those conducting medical research are especially at risk. We saw this come to fruition in June 2020 when hackers infiltrated the UCSF School of Medicine, costing the university $1.14 million in ransom payments alone.

The number of cyberattacks hitting higher education is no coincidence because, sadly, colleges and universities have historically been easy targets.

Why Higher Ed is an Easy Target

To promote more effective learning, higher education institutions were early adopters of computers and the internet. For many, however, that's where technology adoption stalled. With legacy devices and infrastructure in place, institutions limited their own ability to implement modern security measures. And when the pandemic hit in 2020, the scramble to go remote created fresh vulnerabilities.

Remote learning reinforced Bring Your Own Device (BYOD) policies, while introducing open-source learning platforms and various online conferencing solutions to higher education students and faculty. University information spread across the world with students almost overnight, and with little cybersecurity education in place, institutions became more vulnerable to cyberattacks than ever.

Today, in the wake of the remote learning boom, it's important for colleges and universities to evaluate their security infrastructure and invest in modern solutions to keep student, faculty, and institutional information safe.

Building Your Cyber Defense

he good news is, many institutions are embracing the need to be more proactive about cybersecurity. By upgrading devices, implementing secure digital infrastructure, and providing cybersecurity education, they're taking themselves out of the cybersecurity spotlight in a good way.

Here's how your institution can follow suit.

1. When it comes to cyberattack prevention, education is your greatest defense. So, provide regular training to help students and faculty identify a cyberattack, whether it comes in the form of a phishing email or text, malware pop-up, or infected USB drive.

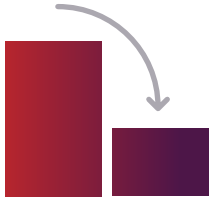
2. To back up this essential education, make sure you're using programs, tools, and devices built to protect users and data. For example, **ThinkShield technology from Lenovo** offers advanced security features, like presence sensing, which can detect if someone is looking over the user's shoulder and protect sensitive data.

3. Another option is to implement a zero-trust security model. **Windows 11 Zero Trust** is designed to assume breach, encouraging institutions to analyze every laptop, desktop, or mobile device that enters their system. This may require a significant investment in technology and personnel, but in the end, it could save your institution millions.

4. Legacy PCs simply can't keep up with modern security demands. And while upgrading may seem like an unnecessary expense, it is far more expensive to resolve breaches on outdated devices than replace those devices with new solutions built for protection.

It's time for a technology upgrade that fits where, when, and how today's students learn.

Windows 11 Pro for Business



With a 58% drop in security incidents, Windows 11 Pro is the most secure Windows update to hit the market.

Lenovo recommends Windows 11 Pro for business to provide the power and protection your students and faculty need, on or off campus. With a reported **58% drop in security incidents, Windows 11 Pro is the most secure Windows update to hit the market.**

Windows 11 focuses on the most pressing concerns of higher education IT teams—security, manageability, and learning outcomes—so when it comes to safeguarding valuable data in the hybrid world, there's no comparison. This platform puts the latest advanced security at your fingertips, while constantly working behind the scenes to protect against evolving threats and ensure your digital security. Windows 11 also offers integrated hardware and software protection, straight out of the box, to ensure a secure hybrid learning experience.

Students and faculty agree, Windows 11 devices are ideal for modern learning with built for hybrid work features including:

Zero Trust-ready OS to protect data and access, anywhere.

Simple, powerful UX to improve educator productivity.

Customizable desktop, workflow automation, and snap layout for a personalized school day that supports learning objectives.

Smarter campus collaboration with Microsoft Teams.

At Lenovo, we're always in pursuit of integrated solutions that free up faculty, inspire learners, and simplify IT management without interruption for limitless learning. **Windows 11 Pro for business** checks all these boxes and more, making it an ideal upgrade choice for any institution looking to power secure hybrid learning.

Windows 11

Lenovo recommends Windows 11 Pro for business

Lenovo

Lenovo ThinkShield

Are you ready to take device, data, and user protection to the next level?

ThinkShield is a comprehensive portfolio of end-to-end security tools encompassing hardware, software, services, and processes to secure your tech at every touchpoint. **This holistic security solution allows IT teams to remotely manage entire fleets of devices with advanced features including:**

1. **Absolute® Persistence endpoint management** for visibility and access into every device in your network, no matter where it's operating.
2. **Self-healing BIOS** to automatically restore endpoint devices to a clean, pre-breach known good state in the event of an attack.
3. **Windows Autopilot** designed to simplify deployment with zero-touch device provisioning.
4. **Device as a Service** for deploying devices with security that is always up to date.
5. **Patch and update options** designed to significantly reduce IT workloads, including:
   - **Lenovo Patch**, a plugin that combines Lenovo BIOS, driver, and third-party software updates into one intuitive console.
   - **Lenovo Thin Installer**, a solution engineered to automatically install updates behind the scenes, eliminating the need to repackage updates or involve end users.
   - **Lenovo Commercial Vantage**, a central user portal that can be configured to manage hardware settings, set preferences, and check system updates.

ThinkShield is engineered to protect information with solutions that evolve with cyber threats, so your security solution will never be stuck in neutral. And because it's from Lenovo, you can be confident in the integrity of your technology and quality of the service you receive. We're here to provide the technology you can rely on and expertise you need, at every turn.

Moving Forward

Protecting student and faculty information has never been more essential or more challenging. But with the combined security power of Windows 11 Pro for business and ThinkShield, your institution can push past these barriers to achieve ultimate protection and peace of mind.

To equip your institution with these modern security solutions, contact your Lenovo representative.

CONTACT US

Windows 11

Lenovo recommends Windows 11 Pro for business

Lenovo