3 ways to safeguard your campus from ransomware attacks

Ransomware attacks are becoming more sophisticated and complex.

Cybercriminals have stepped up their efforts to gain valuable information, particularly from educational institutions. In January 2022, the education sector accounted for more than 80% of reported enterprise malware attacks.[1]

What can your campus do to stay safe? Play defensively against potential ransomware attacks. Consider the following when building a comprehensive security plan for your campus.

01. Protection is not "one and done."

Ransomware is best combated with a multilayered approach. Take steps to safeguard your institution's hardware, software, and data. When developing a security plan, choose solutions that offer protective layers:

- USB protection to prevent unauthorized data transfers
- Fingerprint readers and IR cameras for identification
- Data encryption
- Secure end-of-life disposal of devices

Windows 11 devices, including the ThinkPad® X1 Titanium Yoga — designed on the Intel® Evo™ vPro® platform — have built-in security features including ransomware scans, data encryption, and biometrics to protect your device. Beyond defensive measures, it's also important to consider features that allow you to get your devices back up and running in the event of a ransomware attack, like snapshot copies that can be used to restore a device.

Smarter technology for all

02. Remote management and devices must be part of the conversation.

Factor in security measures for remote devices. Borderless campuses present a series of unique challenges to IT professionals. You can't be everywhere at the same time, but with the right security features, your devices can work to protect themselves wherever learning happens. Three key areas to consider are silicon-level protections, firmware security, and software-level security.

Silicon-level protection serves as a first layer of security by validating code when devices boot up. It also protects the operating system. Device management tools like Absolute® for endpoints on and off your network can further help with tracking devices, monitoring device health, issuing critical updates, and managing user permissions.

Firmware protections form another layer of armor for your devices by stopping threats and even working to repair themselves. Some of the latest firmware security features include tamper switches, USB protection, and fingerprint readers.

Finally, software-level security helps safeguard devices from attacks below your operating system.

Lenovo's fleet of solutions and devices powered by the Intel vPro® platform for an unrivaled business PC solution, delivering silicon-level support plus integrated hardware, firmware-level protections, and software security features to detect, stop, and recover from threats.

intel vPRO PLATFORM

BUILT FOR BUSINESS

Smarter technology for all

Lenovo

03. Security should be forward-thinking.

Cybercrime is evolving every day. Criminals are getting smarter and finding new ways to exploit devices. The best investment for your campus security is to deploy a forward-thinking and flexible security system. What exactly does that look like? Consider a security solution that:

- Frees up IT professionals' time to focus more on security and less on time-consuming tasks like helping install software or reset passwords.
- Doesn't interfere with learning by slowing down students and faculty.
- Is customizable and can be adapted as new threats arise.
- Can quickly learn to identify threats through AI capabilities, like SentinelOne.®

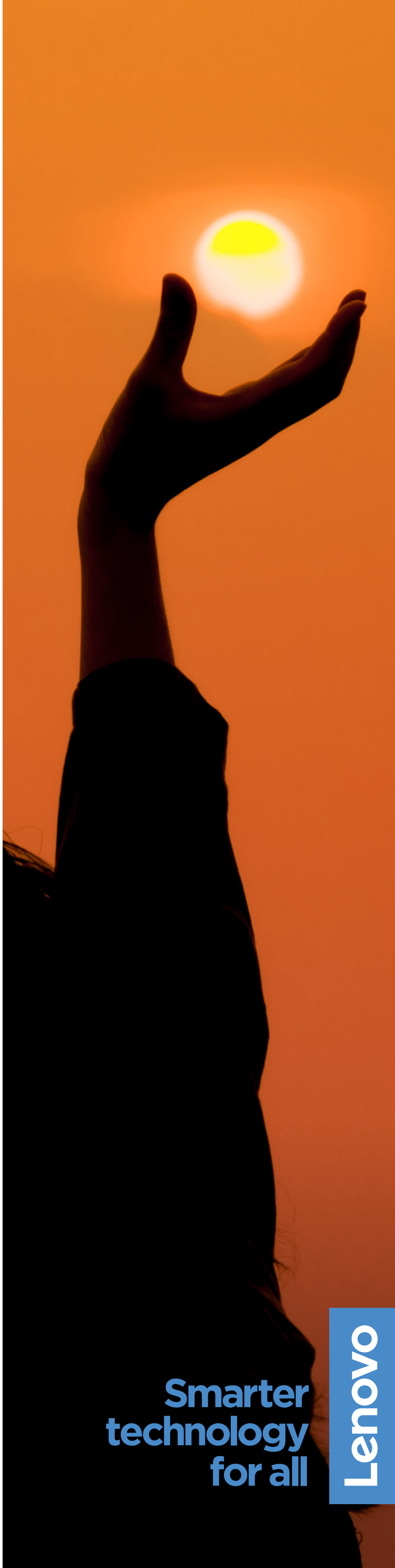
A robust solution like ThinkShield can enhance your campus safeguards against future attacks. ThinkShield, Lenovo's security portfolio of hardware, software, services, and processes, offers the most comprehensive protection with a modern Windows 11 device powered by the Intel vPro® platform, which provides built-in enhanced security features not found on other devices.

This customizable security platform can be tailored to your campus, offering a multilayered solution that stays one step ahead of cybercriminals by helping keep your devices secure, blocking unauthorized users, stopping hacks and online threats, and keeping data safe.

Educate students and faculty as security partners.

Even the best security systems and most knowledgeable IT teams can only do so much. That's why regular security training activities for students, faculty, and all users on and off campus is also a critical aspect of protecting your borderless campus.

Windows 11 features built-in collaboration tools such as Microsoft Teams and Microsoft SharePoint that make it easy to host informative sessions or share helpful reminder guides that users can easily access for a ransomware protection refresher.



intel vPRO PLATFORM
BUILT FOR BUSINESS

Source

1 Microsoft, "Global Threat Activity," January 2022

CHECKLIST

Defend your campus from ransomware attacks

Consider these key points when building out a security plan for your institution.

□ Are you employing a multilayered approach to security?

Security should be comprehensive and consider every stage of your device fleet's lifecycle — from active use to end of life. You should have security measures in place for everything from data encryption to proper disposal of devices.

□ What considerations are you making for remote devices?

With the shift to a borderless campus, how are you safeguarding the devices used by students and faculty outside your campus? How are you managing these devices?

□ What silicon-level protections do you have in place?

Are you backed by protection features like self-healing BIOS or trusted supplier programs? This is a vital first layer in keeping your systems safe and secure.

□ Are you using firmware security measures?

Is your campus utilizing firmware security features such as tamper switches, smart USB protection, or fingerprint readers and IR cameras? These features are available on the Intel vPro® platform for an unrivaled business PC solution tailored for the borderless campus.

□ What software-level security features are you equipped with?

Advanced measures like shadow stack security technology or AI and ActiveEDR help defend vulnerable software.

□ How are you keeping students and faculty educated on the latest security measures and tactics?

One of your best defenses from ransomware attacks is to keep your end users informed and educated on potential threats, the steps they can take to keep their data and devices safe, and how to identify and respond appropriately to social engineering attacks.

□ Is your current security strategy flexible?

As cybercrime evolves, so should cybersecurity capabilities to detect and defend against threats. If your security measures are not scalable and flexible, consider a comprehensive defense system such as the Lenovo ThinkShield security portfolio.

Lenovo is here to help.

We deliver technology to support faculty, staff, and students — no matter where learning happens.

Learn more at **www.lenovo.com/Education.**

intel vPRO PLATFORM

BUILT FOR BUSINESS

Smarter technology for all

Lenovo