



Lenovo recommends
Windows 10 Pro for Business.

SECURITY REPORT 2021

The future of remote device management

ThinkShield



It's time for devices to help secure themselves

Experts estimate that 20% of the global workforce could continue to work remotely at least three days per week. That's three to four times more remote employees than before the pandemic.¹

This shift to remote work represents an entirely new set of challenges for the IT leaders charged with securing devices and data.

To meet the challenges, critical advances at the **silicon**, **firmware**, and **software** levels are ushering in a new baseline in device security. Designed for the workforce of the future, the newest and most advanced technology features, like those available on the built-for-business Intel vPro® platform, are optimized to work together. They protect devices against the most sophisticated threats with a unified, multilayered system of defense — woven seamlessly from CPU to OEM to OS.

Smarter
technology
for all

Lenovo




Silicon-level protections

Because 63% of companies experienced a hardware- or silicon-level security breach within the last 12 months,² processor security forms the first protective layer in a modern secured device.

Security-first CPUs are designed to validate code during the boot-up process, protecting the integrity of the Windows operating system and ensuring a smooth handshake from silicon to BIOS to OS. Look for processors that support root-of-trust secure boot.

Advanced features enable reliable hardware-based endpoint management, lock the BIOS against malicious firmware updates, and provide hardware-level backup to ensure device and OS integrity.



The built-for-business Intel vPro® platform provides silicon-level support for layers of security on Lenovo Think® devices.



Lenovo recommends
Windows 10 Pro for Business.

Smarter
technology
for all

Lenovo





OEM security

Firmware attacks have increased 750% since 2016,³ but advances in OEM security and the Intel vPro® platform are fending them off with features that not only detect and block threats but can even repair devices autonomously.

Self-healing BIOS automatically restores endpoint devices to a clean, pre-breach known good state. It helps mitigate attacks aimed at the BIOS and stops “bricking” if a BIOS update is interrupted or fails.

New advances also separate firmware-level security from the software layer, completely isolating critical security functions from potential breach.

Device-based security features form a suit of armor, protecting access points if a device is lost or stolen.

They include:

- A tamper switch that notifies IT admins when the back cover of a device is opened
- Smart USB protection to block unknown storage devices and prohibit the unauthorized transfer of data
- Fingerprint readers and IR cameras for easy biometric authentication



Lenovo hardware- and firmware-level protections detect, block, and self-heal from malware threats or device theft.



Lenovo recommends
Windows 10 Pro for Business.

Smarter
technology
for all

Lenovo



Software-level security


Defending the vulnerable software layer requires deep integration and alignment with both silicon and OEM security.

Due out this year, shadow stack security technology will block return-oriented programming (ROP), which hackers use to exploit a device's legitimate software code. The new technology creates a "shadow" stack stored on the processor to verify against the call stack in memory and confirm it hasn't been tampered with.

Secured-core PCs guard against attacks aimed below the operating system, keeping malicious code out of the BIOS and away from the network. Deep integration with the

hardware and firmware leverage root-of-trust boot processes to validate code before execution. Boot-up is aborted if any movements deviate from the norm.

AI and ActiveEDR are being tapped to predict, prevent, and stop zero-day attacks. AI-powered protection alerts the network and rolls devices back to a clean pre-breach state. Full forensics and global intel are subsequently available to the network. Endpoint detection and response (EDR)-based solutions are more advanced than legacy antivirus software and much more effective at catching evasive attacks, which target the computer firmware and below-OS components.



The Intel vPro® platform team partnered closely with Microsoft to provide the processor alignment required to enable shadow stack technology on Windows 10.



Windows 10

Lenovo recommends
Windows 10 Pro for Business.

Smarter
technology
for all

Lenovo



The power of multilayered protection

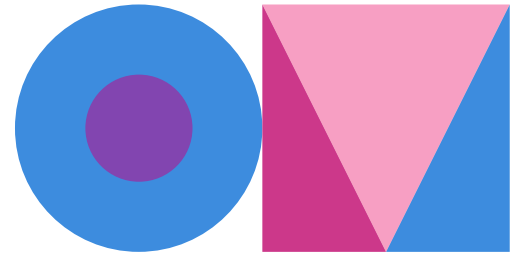
With a unified, multilayered system of defense, devices help protect themselves and empower the workforce of the future. IT leaders should expect technology features to be optimized to work together, from CPU to OEM to OS.

Using both static and behavioral AI, SentinelOne makes autonomous decisions and executes automatic, instant responses.

Evolve and thrive with ThinkShield security

ThinkShield is Lenovo's security portfolio of hardware, software, services, and processes — fully customizable solutions to secure your critical data and business technology. Get the most comprehensive protection with a modern Windows 10 Pro device powered by the Intel vPro® platform.

Learn more at www.lenovo.com/PursueTheNew.



Lenovo recommends
Windows 10 Pro for Business.

Smarter
technology
for all

Lenovo



Sources

- 1 Susan Lund, et al., "What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries," McKinsey Global Institute, mckinsey.com, November 2020
- 2 Josh Fruhlinger, "Top cybersecurity facts, figures and statistics," CSO report, csoonline.com, March 2020
- 3 "Five questions to evaluate and improve your firmware security posture," Eclipsium *Assessing Enterprise Firmware Security Risk* blog, eclipsium.com, January 2020



Lenovo recommends
Windows 10 Pro for Business.

Smarter
technology
for all

Lenovo