ThinkShield

Your remote security checklist

Essential technology to protect the 2021 workforce

AMD

Smarter
technology
for all

Lenovo

The workplace of the future

At this point, it's safe to say that the remote work floodgates have opened.

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]

While we may not have predicted this phenomenon a few years ago, remote work is largely viewed as a success:

94%

of employers report that company productivity has been the same or higher since employees began working from home at the start of the pandemic.[2]

Remote workers are

35%–40%

more productive than their in-office counterparts.[3]

>50%

More than half of US employees who transitioned to remote work during the pandemic said they wanted to continue working remotely even after it became safe to return to the office.[4]

The pandemic proved that technology was ready for remote work — with powerfully portable devices, efficient software, and effective collaboration tools.

Securing the remote workforce

This shift to remote work represents an entirely new set of challenges for the IT leaders charged with securing devices and data:[5]

61%

of global organizations have experienced a jump of 25% or more in cyberthreats or alerts since the start of the pandemic.

>50%

More than half of global organizations are struggling to protect both company-owned devices and the personal devices employees use in their remote environments.

96%

of global organizations are grappling with cybersecurity policy changes to support remote work.

Not to worry. Security technology is keeping pace with protections designed to fortify the remote workplace, securing devices and the ways in which those devices access your network.

In the following sections, we'll explore the **top three security threats** confronting employees as they work from anywhere — and highlight tools IT leaders can use to protect employees and the devices they use. *Do you have these security features on your cybersecurity checklist?*

THREAT 1

Device theft

CISOs were ominously warned in 2017 that a laptop was stolen every 53 seconds.[6] Research from the University of Pittsburgh subsequently found that a laptop has a one in 10 chance of being stolen — and only a 2% chance of recovery.[7]

With 87% more employees working remotely by 2025,[8] those figures may one day represent the easy days of device security.

Today, millions more company-owned devices are deployed at kitchen tables and outdoor cafes — corresponding accordingly with millions more opportunities for loss or theft. The following security protections will block intruders and lock data if a hacker physically gets ahold of a device.

Lenovo AMD

The checklist

- ✓ **Lenovo tamper switch**
  Alerts IT if the back cover is opened
- ✓ **Smart Thunderbolt/USB protection**
  Configures ports to block storage devices and unauthorized data transfer
- ✓ **AMD Memory Guard**
  Scrambles encryption keys stored in system memory so hackers can't use them to unencrypt the hard drive
- ✓ **IR camera**
  Enables facial recognition with Windows Hello
- ✓ **Fingerprint reader**
  Enables easy biometric authentication — Lenovo's match-on-chip and match-on-network fingerprint readers are the most secure in the industry

THREAT 2

Silicon and firmware attacks

Firmware security was already on every CISO's radar, especially after Gartner announced that 70% of organizations without a firmware upgrade plan could expect to be breached by 2022.[9] Hackers are increasingly targeting devices below the OS, gaining access to the system by compromising it with malicious code as the device boots up.

Firmware and silicon-level breaches are hard to detect and repair, which makes them particularly insidious in the remote work environment where employees don't have access to onsite tech support.

The following below-the-OS security protections ensure devices can detect breaches, prevent attacks, and autonomously repair damage. All this means employees don't have to reinstall hardware, replace devices, or lose productive work time.

2

The checklist

- ☑ **Lenovo self-healing BIOS**
  Automatically recovers from BIOS corruption or attack, relieving IT from remediation tasks and minimizing user interruption
- ☑ **AMD modern security architecture**
  Engineered to validate silicon-level instructions and expose attack vectors before they can be executed; locks out known threats and requires fewer patches
- ☑ **AMD Secure Processor**
  Enables root-of-trust secure boot-up, creating a safe handshake from the silicon to the BIOS to the operating system
- ☑ **ThinkShield Engine**
  Custom chip embedded within Lenovo Think devices that performs security functions completely isolated from the software

THREAT 3

Online and email attacks

When the pandemic hit, working remotely was an entirely new experience for 49% of employees.[10] That meant nearly half of remote workers were at heightened risk for logging into compromised Wi-Fi, clicking unsafe email attachments, and inadvertently downloading malware.

By the fall of 2020, 51% of organizations had, in fact, reported that malware made it through their corporate defense systems. Of those attacks, credential theft and phishing attacks were the most common approaches.[11]

To protect a remote workforce, security measures must extend beyond the device itself and actually create a safe working environment. The following critical security features help do that, locking out cyberattacks caused when employees inadvertently open the door.

Lenovo AMD

3

The checklist

- ☑ **Lenovo WiFi Security**
  Warns users of suspicious behavior with a “safe/not safe to connect” alert message
- ☑ **SentinelOne AI-powered endpoint protection**
  Predicts, prevents, and stops zero-day attacks; alerts the network to new virus and malware threats and rolls devices back to a clean pre-breach state
- ☑ **Secured-core PC**
  Leverages root-of-trust collaboration between the CPU, the BIOS, and the Microsoft OS to ensure devices always boot up securely
- ☑ **AMD Control-flow Enforcement Technology**
  Provides the processor alignment required to enable Microsoft’s shadow stack technology, which blocks return-oriented programming (a technique that hackers use to exploit a device’s legitimate software code)
- ☑ **Webcam privacy shutter**
  Integrated physical webcam cover protects against visual hacking
- ☑ **BUFFERZONE sandbox safety**
  Creates a virtual environment to safely contain email sessions and web browsing activity, which completely isolates devices from attack

Remote security checklist: At a glance

1 Device theft

- Lenovo tamper switch
- Smart Thunderbolt/ USB protection
- AMD Memory Guard
- IR camera
- Fingerprint reader

2 Silicon and firmware attacks

- Lenovo self-healing BIOS
- AMD modern security architecture
- AMD Secure Processor
- ThinkShield Engine

3 Online and email attacks

- Lenovo WiFi Security
- SentinelOne AI-powered endpoint protection
- Secured-core PC
- AMD Control-flow Enforcement Technology
- Webcam privacy shutter
- BUFFERZONE sandbox safety

Lenovo AMD

Protect your team with Lenovo ThinkShield + AMD PRO security

All Lenovo Ryzen™ PRO devices are protected by ThinkShield + AMD PRO security. ThinkShield and AMD security features work together to build a unified, multilayer system of defense, locking data and protecting devices from today's most sophisticated threats.

Contact your Lenovo Account Representative or local Business Partner

Visit www.lenovo.com/ThinkShield

Follow us on Twitter @Lenovo

SOURCES

1 "What's next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries," McKinsey Global Institute, November 2020

2 "90% of employers say working remotely hasn't hurt productivity," CNN Business, August 2020

3 "Advantages of Agile Work Strategies for Companies," Global Workplace Analytics

4 "How Coronavirus Will Change the 'Next Normal' Workplace," Gallup, May 2020

5 "Future of Secure Remote Work Report," Cisco

6 "The mobile device conundrum: Employee flexibility and security at odds," CIO Dive, March 2017

7 "A Lost Laptop is a Cybersecurity Threat," Grand Canyon University Engineering and Technology blog, November 1, 2019

8 "Future of Workplace Pulse Report," Upwork, December 2020

9 "Firmware Attacks: What They Are and How I Can Protect Myself," Hashed Out by the SSL Store, February 25, 2020

10 "Increasing Cybersecurity Gaps and Vulnerabilities due to Remote Work During COVID-19," Security, June 10, 2020

11 "New Security Report Breaks Down Increase in Cyber Attacks Due to Remote Work," CPO Magazine, October 16, 2020