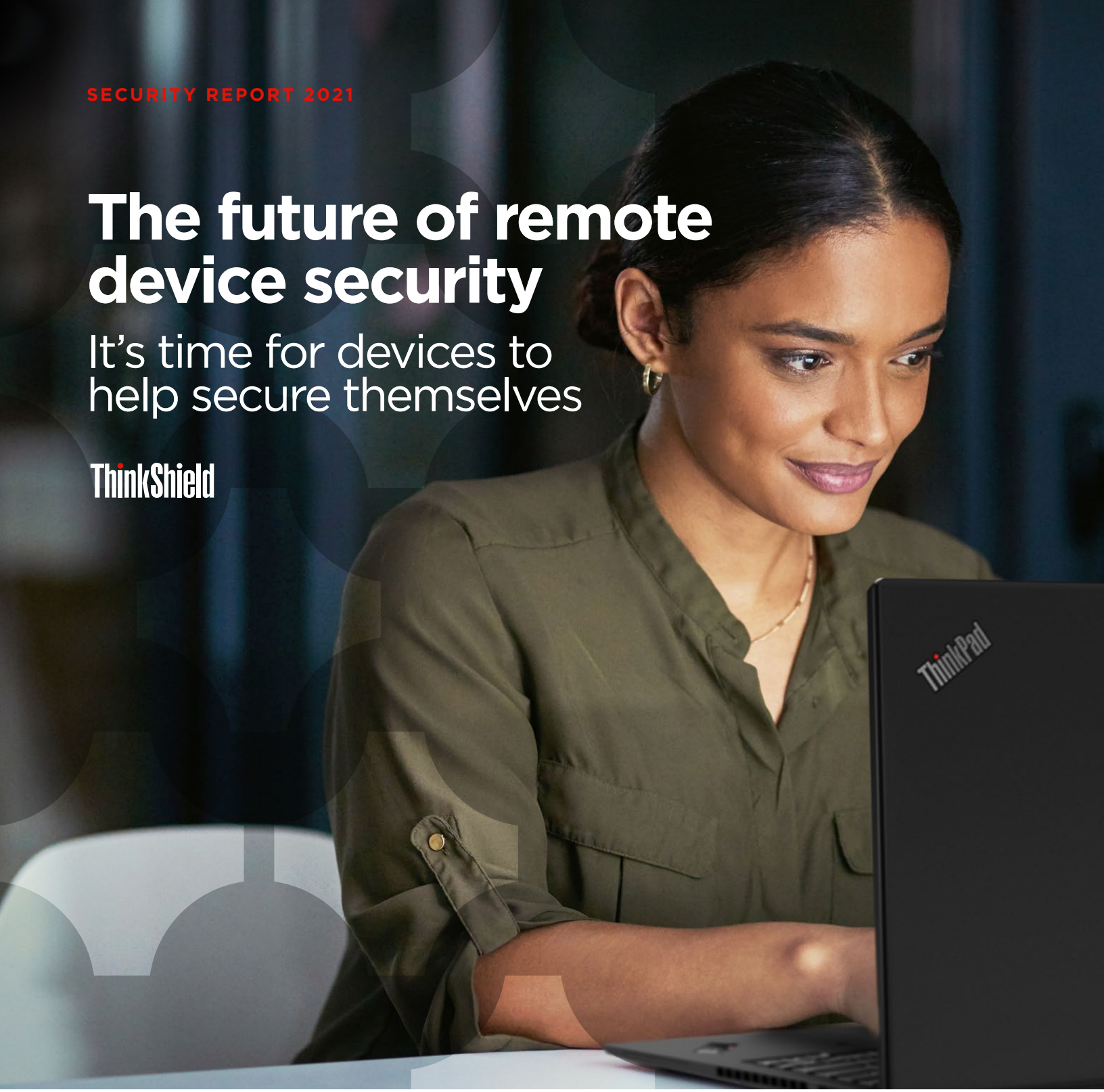
SECURITY REPORT 2021

The future of remote device security

It's time for devices to help secure themselves

ThinkShield



AMD

Smarter technology for all

Lenovo

Three years before the pandemic besieged us, CISOs were ominously warned that a laptop was stolen every 53 seconds in the U.S.[1]

Now they may wish device security was still that easy!

An estimated 36.7 million Americans are expected to be working remotely by 2025 — an 87% increase from pre-pandemic levels.[2] No longer office-based, employees are now disbursed with their company-owned devices to all corners of the world. They're also using personal devices to access company data.

20%

Remote workers have caused a security breach in 20% of organizations.

As a result of these two distinct device vulnerabilities, laptop security rapidly emerged as a 2021 IT crisis:

- More than half of global organizations say they are struggling to protect the influx of company-owned and personal devices employees use in a remote environment.[2]
- Remote workers have caused a security breach in 20% of organizations.[3]
- Remote work has increased the average cost of a data breach by $137,000.[4]

53 seconds was the watermark — back when employees still largely worked within the confines of the office. Now that IT leaders have less onsite control of devices, the future of IT security depends upon technology that enables devices to help manage themselves.

This report examines critical advances at the **silicon**, **firmware**, and **software** levels that usher in a new baseline in device security. Designed for the 2021 workforce, the newest and most advanced technology features are optimized to work together, protecting devices against the most sophisticated threats with a unified, multilayered system of defense — woven seamlessly from CPU to OEM to OS.

Lenovo

OEM security

Collaboration and optimization at the manufacturing level ensure a smooth, safe handshake between the CPU and the firmware. Firmware attacks have increased 750% since 2016,[5] but advances in OEM security are fending them off with features that not only detect and block threats but can even repair devices autonomously.

1

Manufacturing integrity

Hardware manipulation is difficult to accomplish, but the payoff is significant — making it an appealing frontier for hackers.[6] Once hardware is successfully breached, the modification is extremely difficult to detect and repair, which gives the hacker long-term access.

Secure Supply Chain

Lenovo's Secure Supply Chain process locks down the entire manufacturing supply chain, rigorously vetting all suppliers, components, and processes. Every step of the manufacturing process is controlled, audited, and tamper-proof, so CISOs can be assured their employees are starting with secure devices.

2

Resilient firmware

In the event of attack or corruption, not only can resilient BIOS autonomously detect and stop a security threat — it can even repair the damage.

Lenovo self-healing BIOS

Lenovo's 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.

ThinkShield Engine
A custom chip embedded within Lenovo Think® devices performs security functions that are completely isolated from the software.

NIST Special Publication 800-193 requires resilience features for the Flash Descriptor in SPI flash memory. ThinkShield Engine EC (embedded controller) provides root of trust for the Flash Descriptor. ThinkShield Engine is required for supporting the resilience features of platform firmware in the pre-OS environment.

PROTECTION:
Mechanisms for ensuring that platform firmware remains in a state of integrity and is protected from corruption, such as the process for ensuring the authenticity and integrity of firmware updates.

DETECTION:
Mechanisms for detecting when platform firmware has been corrupted.

RECOVERY:
Mechanisms for restoring platform firmware to a state of integrity in any event that firmware code corruption is detected, or when firmware is forced to recover through an authorized mechanism.

CHAIN OF TRUST IN SECURE BOOT

3

Device integrity

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

Tamper switch

The Lenovo tamper switch notifies IT admins when the back cover of a device is opened. If the tamper switch is activated and triggered, then connection to the Lenovo AC adapter and entry of a supervisor password are subsequently required.

Smart USB protection

Devices with Lenovo smart USB protection are configured to respond only to keyboards and pointing devices, blocking unknown storage devices and prohibiting the unauthorized transfer of data.

Silicon-level protections

Resilient hardware-based security depends on the confluence of a few critical features. Because 63% of companies experienced a hardware- or silicon-level security breach within the last 12 months,[7] the following features are designed to form the first protective layers in a modern secured device.

1

Security-first architecture

Security-first processor architecture forms the foundation of resilience. Security patches can impact performance from 20% to 60%,[8] so processors that require fewer patches also reduce downtime and improve overall cost of ownership. But be aware that some CPUs themselves are released as patched upgrades from older architecture.

AMD Modern Security Architecture

With the Ryzen™ PRO processor line, AMD redesigned its architecture from a security-first perspective, engineering it to lock out known threats and prevent future threats. The architecture is built to validate silicon-level instructions so that attack vectors are exposed before they can be executed. As a result, the vast majority of speculative execution attacks haven't impacted AMD's processors.[9]

63%

of companies experienced a hardware- or silicon-level security breach within the last 12 months.

Lenovo

2

Processor security

Secure processors act as a hardware root of trust. They authenticate the confidentiality and integrity of any formula that loads on the device, validating it before it can be executed into the system. This must happen at three levels: first-party silicon formulas, then OEM BIOS formulas, and finally the third-party OS formulas. If errors or modifications are detected, they are automatically denied access before they can infiltrate and cause damage.

AMD Secure Processor

AMD's silicon includes a dedicated security processor, embedded in the architecture, that acts as the hardware root of trust. It enables secure boot-up from the BIOS level into the Trusted Execution Environment. Trusted applications can leverage industry-standard APIs to take advantage of the Trusted Execution Environment.

3

Memory encryption

Full memory encryption is critical to protect lost or stolen laptops. When in physical possession of a device, a hacker can access encryption keys stored in system memory to easily unscramble the software-encrypted data in the hard drive.

Despite a recent rise in attacks aimed at system memory,[10] end users often decline or disable the technology because of its history of slowing down computer performance. The solution to this problem is hardware-based security, which is more efficient than software-based encryption. It has minimal impact on overall system performance — even when the device is in standby mode.

AMD Memory Guard

AMD Memory Guard generates 128-bit AES encryption keys to protect the data that's stored in the system memory. Random-key encryption of all DRAM contents helps protect against physical cold boot and DRAM interface snooping.

Security is accomplished with dedicated hardware in the on-die memory controllers that keeps the memory and processor separate from each other. The AES keys that encrypt the memory are stored in the CPU in a location the system memory does not have access to. Further, new AES encryption keys are generated with every reboot, which provides additional security assurance.

Software-level security

Defending the vulnerable software layer requires deep integration and alignment with both silicon and OEM security. Here's how multilayer optimization secures devices in and above the operating system.

1

Shadow stack technology

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. Microsoft's 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.

CPU manufacturers are partnering closely with Microsoft to provide the processor alignment required to enable the technology, such as AMD Shadow Stack.

2

Secured-core PC

Microsoft's Secured-core PC guards 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 leverages root-of-trust boot processes to validate code before execution. Boot-up is aborted if any movements deviate from the norm.

AMD enables Secured-core PC with its Dynamic Root of Trust Measurement (DRTM) Service Block, which is made up of ADM's SKINIT CPU instructions, the AMD Secure Processor, and the AMD Secure Loader.

The service block measures and authenticates the firmware and bootloader, gathers system configuration requirements for the OS, then validates those system configurations against its security requirements.

Further, AMD's Memory Guard is enabled by default on Secured-core PCs, which provides extra protection for encryption keys in the event of physical attack.

Lenovo can configure Secured-core PC at the factory. This not only ensures fleet consistency, but also allows devices to be shipped directly to remote employees.

Lenovo

3

AI-powered endpoint protection

Malware can infect a system using nothing but the binaries already on the system itself, and other types of malware — such as ransomware — can encrypt an organization's files, causing significant business disruptions. This means that both old and new attacks are in play. Combating this requires endpoint controls that are mature enough for advanced prevention, detection, and response capabilities.

Advanced, autonomous endpoint protection provided by SentinelOne uses AI and ActiveEDR to predict, prevent, and stop zero-day attacks.

AI-powered protection alerts the network and rolls devices back to a clean, known good pre-breach state. Using both static and behavioral AI, SentinelOne makes autonomous decisions and executes automatic, instant responses. 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 that target the computer firmware and below-OS components.

4

Secure authentication

Out-of-the-box authentication and adaptive user management help protect devices from unauthorized access.

Integration between Windows 10 and Lenovo device security enables eight modes of secure authentication — including biometrics via IR camera and fingerprint reader. Lenovo's match-on-chip and match-on-network fingerprint readers are the most secure in the industry.

EIGHT MODES OF AUTHENTICATION

1. **Network security**
2. **NFC tap to login**
3. **GPS security**
4. **Smart card**
5. **Facial recognition**
6. **Password and PINs**
7. **Bluetooth**
8. **Match on chip fingerprint reader**

Lenovo

The power of multilayered protection

Despite the security risks associated with remote work, the trend 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.[11]
- Remote workers are 35%–40% more productive than their in-office counterparts.[12]
- More than half of US employees who transitioned to remote work during the pandemic want to continue working remotely even after it's safe to return to the office.[13]

With a unified, multilayered system of defense, devices help protect themselves and empower the 2021 workforce. IT leaders should expect technology features to be optimized to work together, from CPU to OEM to OS.

94%

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.

ThinkShield + AMD PRO security

All Lenovo devices featuring AMD Ryzen™ PRO processors 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.

Sources

1 "The mobile device conundrum: Employee flexibility and security at odds," CIO Dive, March 2017. Accessed at https://www.ciodive.com/news/the-mobile-device-conundrum-employee-flexibility-and-security-at-odds/437427/

2 "Future of Secure Remote Work" report, Cisco. Accessed February 2021 at https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html

3 "Enduring from home: COVID-19's impact on business security," Malwarebytes. Accessed February 2021 at https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf

4 "2020 Cost of a Data Breach" report, IBM. Accessed February 2021 at https://www.ibm.com/security/data-breach

5 "Five questions to evaluate and improve your firmware security posture," Eclysium, January 2020. Accessed at https://eclypsium.com/2020/01/20/assessing-enterprise-firmware-security-risk/

6 "Guarding against supply chain attacks — Part 2: Hardware risks," Microsoft, February 3, 2020. Accessed at https://www.microsoft.com/security/blog/2020/02/03/guarding-against-supply-chain-attacks-part-2-hardware-risks/

7 "Top cybersecurity facts, figures and statistics," CSO, March 2020. Accessed at https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

8 AMD statistic

9 "Intel vs. AMD Processor Security: Who Makes the Safest CPUs?" Tom's Hardware Review, November 2019. Accessed at https://www.tomshardware.com/features/intel-amd-most-secure-processors

10 "Newly discovered computer attack can steal data from memory chips," Algorithm, June 2019. Accessed at https://algorithm.data61.csiro.au/newly-discovered-computer-attack-can-steal-data-from-memory-chips/

11 "90% of employers say working remotely hasn't hurt productivity," CNN Business, August 2020. Accessed at: https://www.cnn.com/2020/08/27/success/work-from-home-employer-plans-for-more-flexible-policies/index.html

12 "Advantages of Agile Work Strategies for Companies," Global Workplace Analytics. Accessed February 2021 at https://globalworkplaceanalytics.com/resources/costs-benefits

13 "How Coronavirus with Change the 'Next Normal' Workplace," Gallup, May 2020. Accessed at https://www.gallup.com/workplace/309620/coronavirus-change-next-normal-workplace.aspx

Contact your Lenovo Account Representative or local Business Partner

Visit www.lenovo.com/ThinkShield

Follow us on Twitter @Lenovo

AMD

Smarter technology for all

Lenovo