Lenovo
Education

intel vPRO PLATFORM
BUILT FOR BUSINESS

Windows 10

Lenovo recommends
Windows 10 Pro for Business.

INFORME DE SEGURIDAD 2021

El futuro de la gestión remota de dispositivos en educación superior

ThinkShield

Es hora de que los dispositivos ayuden a protegerse a sí mismos

En tanto los colegios y universidades de todo el país trabajan para reabrir las aulas, la mayoría de las instituciones también esperan apoyar a los campus sin fronteras para la educación en el campus y en línea.[1]

Este cambio a los entornos de aprendizaje híbridos representa un conjunto de retos completamente nuevo para los líderes de TI encargados de proteger los dispositivos y los datos.

Para hacer frente a los desafíos, los avances críticos en los niveles de **silicio, firmware** y **software** están dando paso a una nueva línea de base en la seguridad de los dispositivos. Diseñadas para el futuro de la educación superior, las funciones tecnológicas más recientes y avanzadas, como las disponibles en la inigualable plataforma para la empresa y el aula Intel vPro®, están optimizadas para trabajar juntas. Protegen los dispositivos frente a las amenazas más sofisticadas con un sistema de defensa unificado de varios niveles, perfectamente integrado entre CPU, OEM y SO.

Smarter technology for all

Lenovo

Protección a nivel de silicio

Debido a que el 63% de las instituciones experimentó una brecha de seguridad a nivel de hardware o a nivel de silicio en los últimos 12 meses,[2] la seguridad de los procesadores constituye la primera capa de protección en un dispositivo sencillo con seguridad integrada.

Las CPU Security-First están diseñadas para validar el código durante el proceso de arranque, protegiendo la integridad del sistema operativo Windows y asegurando un enlace fluido del silicio al BIOS al sistema operativo. Busca procesadores que admitan el proceso de arranque seguro mediante raíz de confianza.

Las funciones avanzadas permiten una administración de endpoints fiable basada en hardware, bloquear el BIOS frente a actualizaciones de firmware maliciosas y proporcionar copias de seguridad a nivel de hardware para garantizar la integridad del dispositivo y del sistema operativo.

La plataforma Intel vPro® proporciona soporte a nivel de silicio de Intel para capas de seguridad en dispositivos Lenovo Think®.

intel vPRO PLATFORM

BUILT FOR BUSINESS

Windows 10

Lenovo recommends Windows 10 Pro for Business.

Smarter technology for all

Lenovo

Seguridad OEM

Los ataques de firmware han aumentado un 750% desde 2016,[3] pero los avances en la seguridad de los OEM y la plataforma Intel vPro® los están eludiendo con características que no sólo detectan y bloquean las amenazas, sino que incluso pueden reparar los dispositivos de forma autónoma.

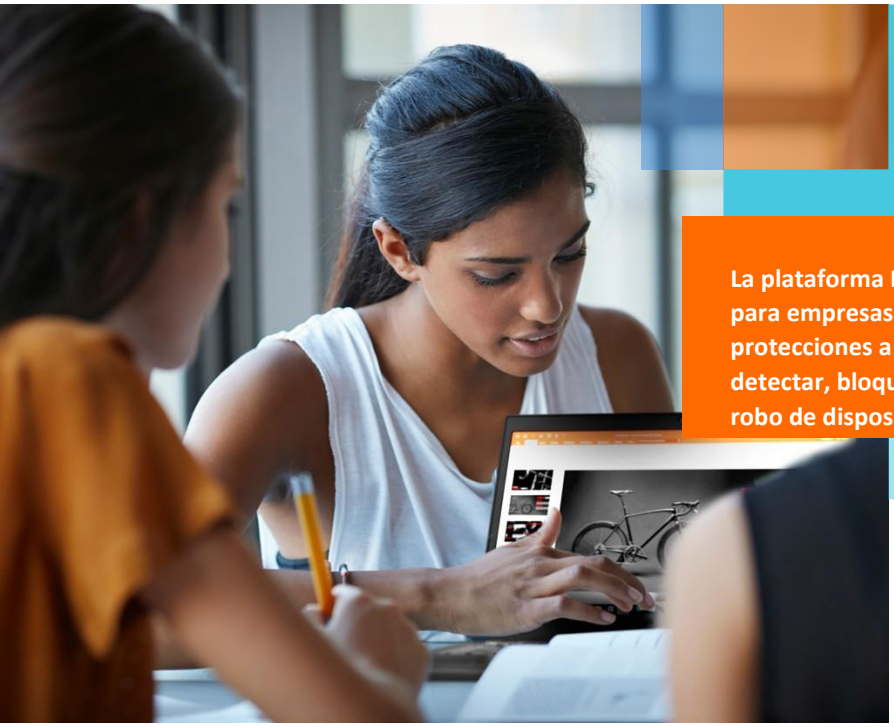
El BIOS de autorreparación restaura automáticamente los dispositivos endpoint al estado anterior correcto. Ayuda a mitigar los ataques dirigidos al BIOS y frena el "bricking" si se interrumpe o falla una actualización del BIOS.

Los nuevos avances también separan la seguridad a nivel de firmware de la capa de software, aislando completamente las funciones de seguridad críticas de posibles intrusiones.

Las funciones de seguridad basadas en dispositivos forman un conjunto de blindaje, protegiendo los puntos de acceso en caso de pérdida o robo de un dispositivo.

Entre ellos se incluyen:

- Un interruptor de sabotaje que notifica a los administradores de TI cuando se abre la cubierta posterior de un dispositivo
- Protección smart USB para bloquear los dispositivos de almacenamiento desconocidos y prohibir la transferencia de datos no autorizada
- Lectores de huellas digitales y cámaras de infrarrojos para facilitar la autenticación biométrica



La plataforma Intel vPro® ofrece una plataforma de PC validada para empresas y educación superior que se integra con las protecciones a nivel de hardware y firmware de Lenovo para detectar, bloquear y autorreparar frente a amenazas de malware o robo de dispositivos.

intel vPRO PLATFORM

Windows10

BUILT FOR BUSINESS

Lenovo recommends Windows 10 Pro for Business.

Smarter technology for all

Lenovo

Seguridad a nivel software

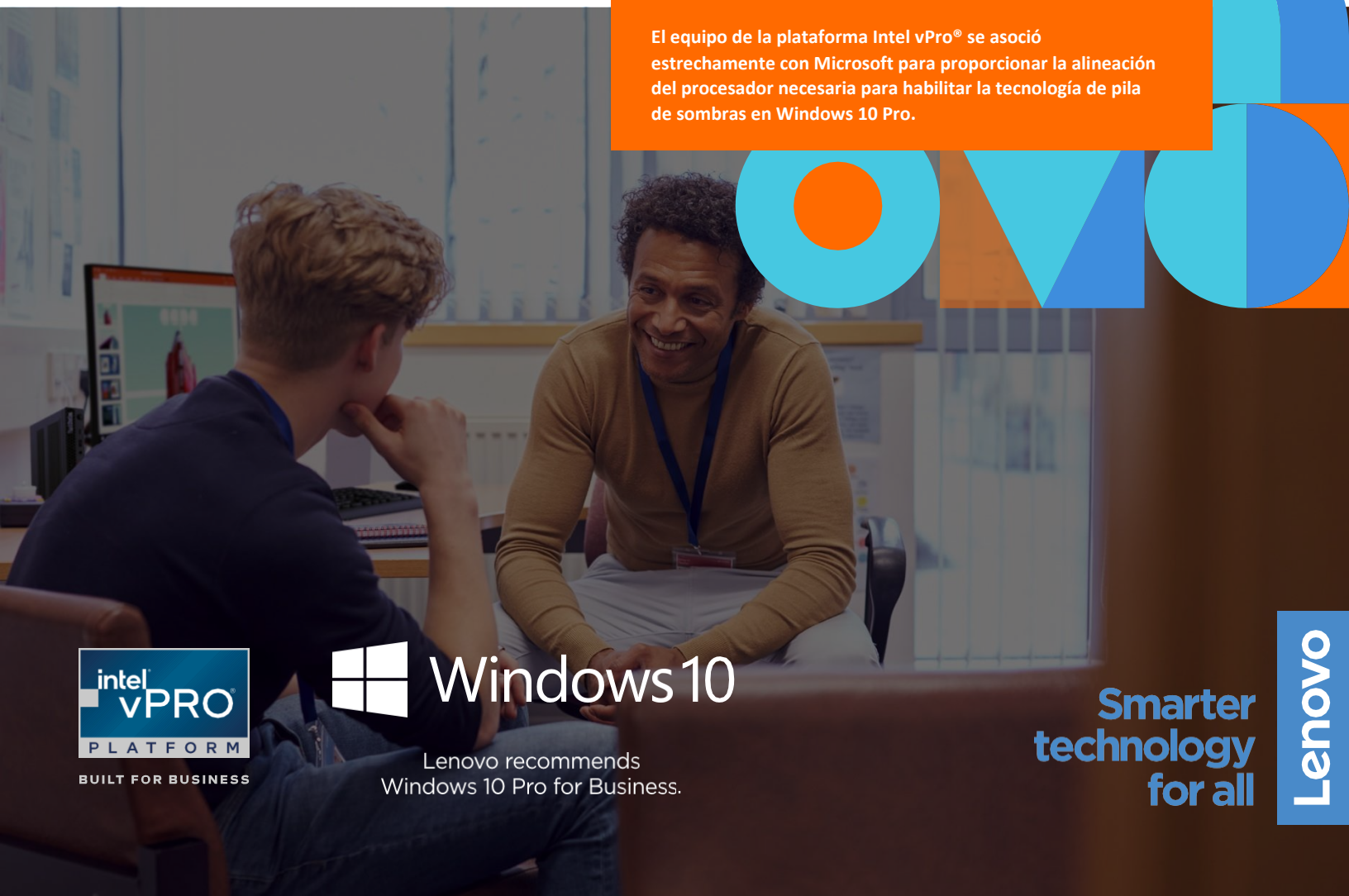
La defensa de la capa de software vulnerable requiere una integración y alineación profundas con la seguridad de silicio y OEM.

Prevista para este año, la tecnología de seguridad de pila oculta bloqueará la programación orientada a retorno (ROP), que los piratas informáticos utilizan para explotar el código de software legítimo de un dispositivo. La nueva tecnología crea una pila "oculta" almacenada en el procesador para verificar la pila de llamadas en la memoria y confirmar que no se ha manipulado.

Las PC de núcleo seguro protegen contra ataques dirigidos debajo del sistema operativo, manteniendo el código malicioso fuera del BIOS y fuera de la red. Integración profunda con los procesos de arranque raíz de confianza de hardware y firmware para validar el código antes de su ejecución. El arranque se cancela si cualquier movimiento se desvía de la norma.

Se está utilizando IA y ActiveEDR para predecir, prevenir y detener los ataques de día cero. La protección con tecnología IA alerta a la red y devuelve los dispositivos a un estado limpio previo a la intrusión. Posteriormente, la red dispone de sistemas completos de análisis forense e información global. Las soluciones basadas en detección y respuesta de endpoints (EDR) son más avanzadas que el software antivirus heredado y mucho más eficaces para detectar ataques evasivos, que se dirigen al firmware del equipo y a los componentes inferiores al sistema operativo.

El equipo de la plataforma Intel vPro® se asoció estrechamente con Microsoft para proporcionar la alineación del procesador necesaria para habilitar la tecnología de pila de sombras en Windows 10 Pro.



El poder de la protección multicapa

Con un sistema unificado de defensa de varios niveles, los dispositivos ayudan a protegerse y a potenciar el futuro de la educación superior. Los líderes de TI deberían esperar que las características tecnológicas se optimicen para trabajar en conjunto, desde CPU a OEM y SO.

Mediante el uso de IA estática y conductual, SentinelOne toma decisiones autónomas y ejecuta respuestas automáticas e instantáneas.

Evoluciona y prospera con la seguridad de ThinkShield

ThinkShield es la cartera de seguridad de Lenovo de hardware, software, servicios y procesos, soluciones totalmente personalizables para proteger a tus estudiantes, cuerpo docente y personal dentro y fuera del campus. Obtén la protección más completa con un moderno dispositivo Windows 10 Pro con la plataforma Intel vPro®.

Más información en www.lenovo.com/Education.

intel vPRO PLATFORM

Windows 10

BUILT FOR BUSINESS

Lenovo recommends Windows 10 Pro for Business.

Smarter technology for all

Lenovo

Fuentes

1 Kathe Pelletier, et al., "2021 EDUCAUSE Horizon Report, Teaching and Learning Edition"
2 Josh Fruhlinger, "Top cybersecurity facts, figures and statistics," CSO report, csoonline.com, marzo de 2020
3 "Five questions to evaluate and improve your firmware security posture," Eclypsium ***Assessing Enterprise Firmware Security Risk*** blog, eclypsium.com, enero de 2020

intel vPRO PLATFORM
BUILT FOR BUSINESS

Windows 10

Lenovo recommends
Windows 10 Pro for Business.

Smarter technology for all

Lenovo