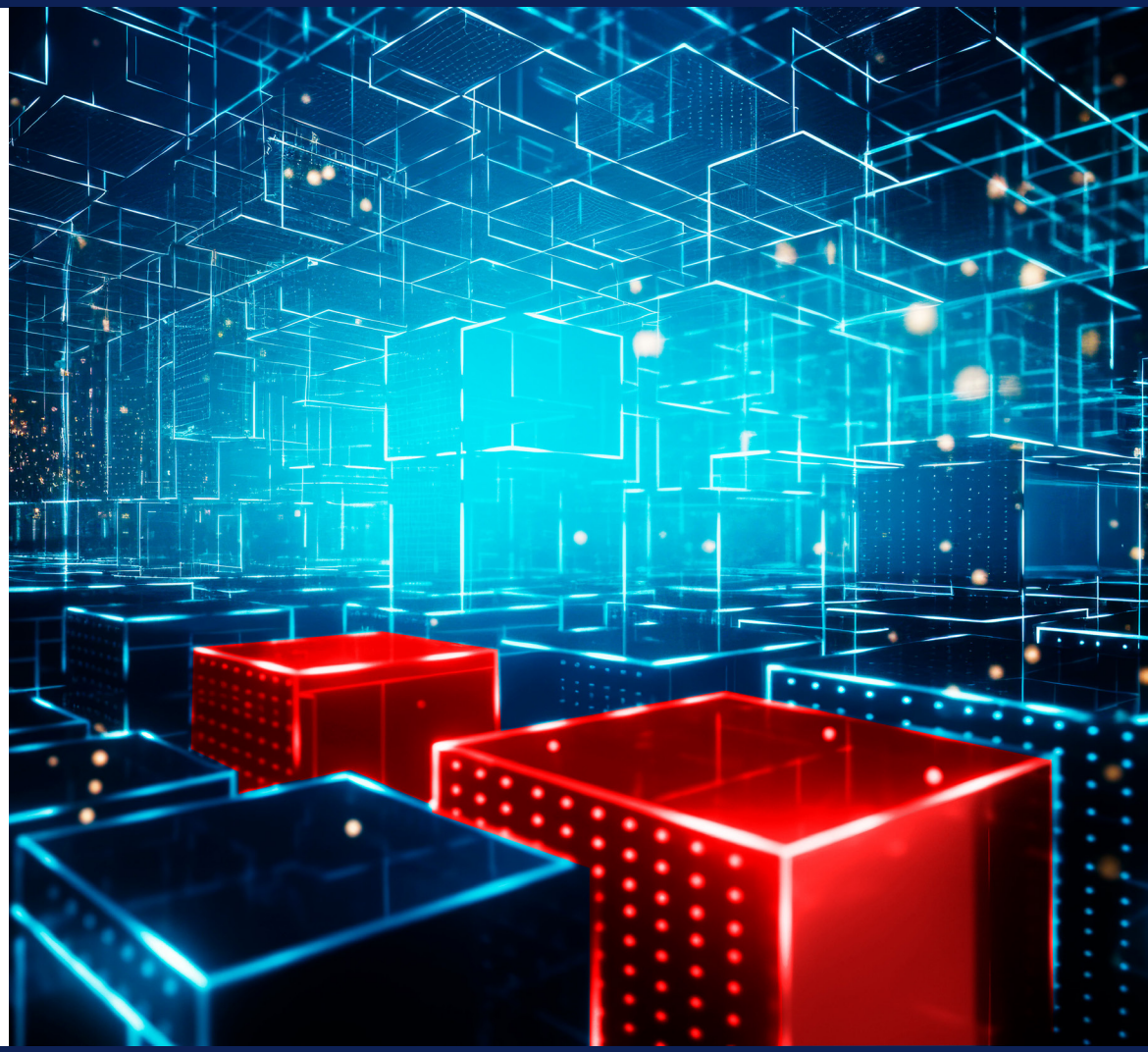
DELL Technologies

intel

Cómo proteger el uso de la IA en el punto final

Defienda las cargas de trabajo de IA en el dispositivo con dispositivos modernos y seguros y una mentalidad de adversario.



CROWDSTRIKE /ABSOLUTE®

Resumen ejecutivo

La IA en el dispositivo tiene enormes beneficios, pero también conlleva riesgos cibernéticos. En este eBook, veremos cómo preparar a su organización de forma segura para aprovechar la innovación en IA en el punto final.

Índice

La superficie de ataque de la IA en el dispositivo

Qué se puede atacar

Todas las tecnologías emergentes conllevan riesgos de ciberseguridad por un motivo: es un nuevo territorio. Estamos lidiando con lo desconocido. Lo hemos visto con cloud computing, blockchain y muchas otras tecnologías. Lo mismo ocurre con la IA en el dispositivo. La clave para mitigar este riesgo, como siempre, es arrojar luz sobre lo desconocido.

Antes de hablar sobre la seguridad que necesitamos para minimizar la superficie de ataque, conviene hablar sobre lo que estamos protegiendo y por qué. Piense en esto como un sistema de tuberías en un edificio comercial que alberga varias empresas. Estas tuberías transportan agua, gas, etc. por todo el edificio para distintos casos de uso. Si la materia que fluye a través de las tuberías está contaminada o si se interrumpe, no puede cumplir su función. Si las tuberías que transportan la materia están dañadas o corrompidas, tampoco podrán cumplir su función. Tanto las tuberías como su contenido deben estar en buen estado de funcionamiento para satisfacer las necesidades de sus respectivos casos de uso.▶

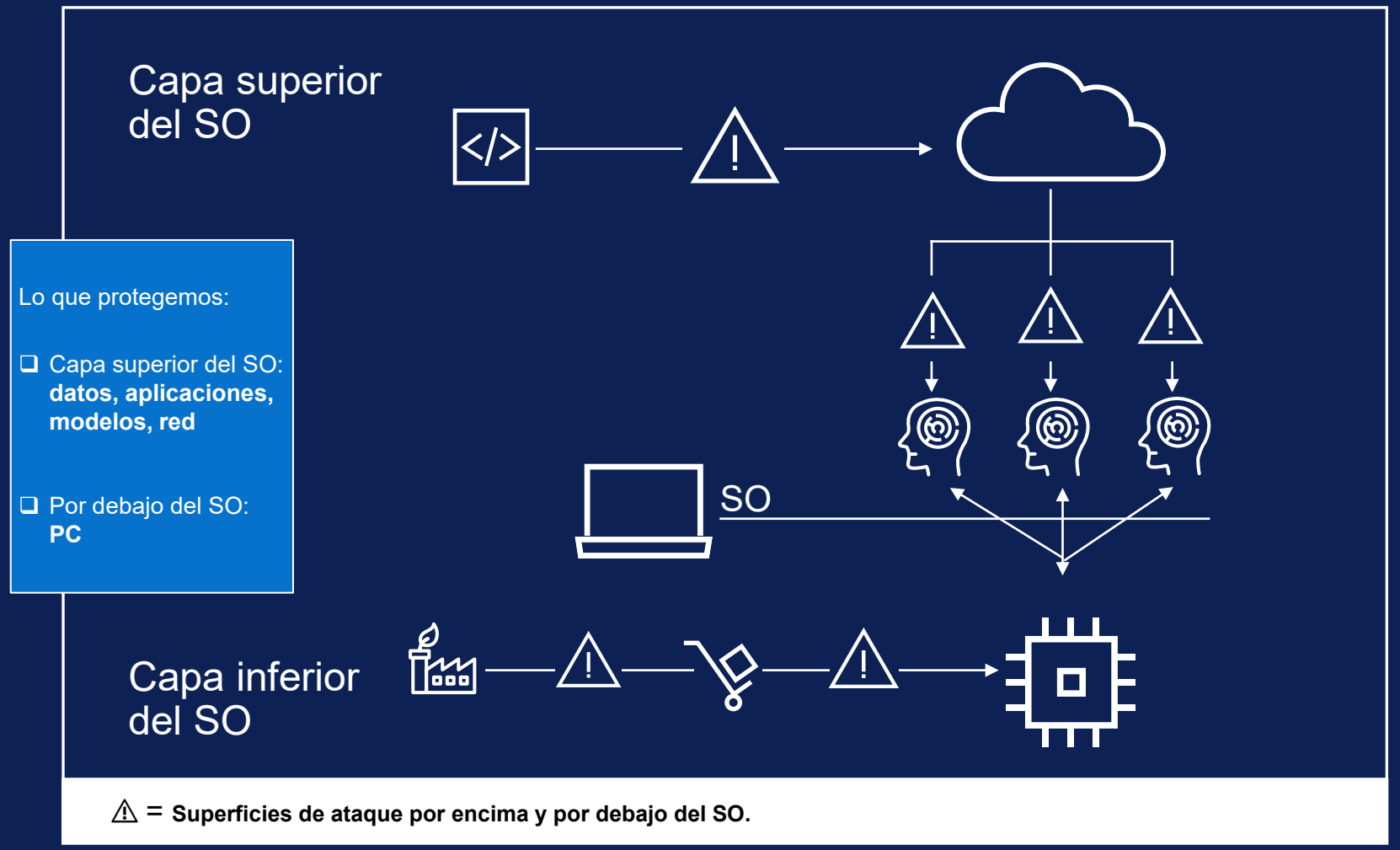
La superficie de ataque de la IA en el dispositivo (cont.)

Qué se puede atacar (cont.)

Volviendo a la IA en el punto final:

- Las tuberías son su infraestructura: sus PC, sus redes corporativas. Cómo y dónde trabaja.
- El contenido que fluye por las tuberías son los datos, las aplicaciones y los modelos que impulsan distintos casos de uso de IA. Los activos y recursos que necesita para realizar su trabajo.

Y lo ha adivinado: los ciberadversarios dirigen sus ataques a ambos. Pueden robar propiedad intelectual para obtener un rescate o envenenar datos o modelos para afectar a las operaciones. En cualquier caso, las consecuencias pueden ser graves y provocar daños financieros y reputacionales o revisiones normativas.►



Riesgos de seguridad en el punto final

Tácticas que utilizan los atacantes para obtener acceso

Ahora, hablaremos sobre los métodos que los atacantes pueden utilizar para acceder a ambos objetivos.

Riesgo del dispositivo. Como vemos en Endpoint Security Market Insights, Forrester Research, Inc., marzo de 2025, los PC se encuentran entre los principales objetivos de las ciberamenazas modernas. Este tipo de ataque puede ocurrir mucho antes de que comience el trabajo de IA en el dispositivo, por ejemplo, un **ataque a la cadena de suministro de hardware o software**. Hay decenas, si no cientos, de puntos durante la cadena de suministros en los que un agente malicioso puede manipular componentes (por ejemplo, circuitos o firmware) para introducir debilidades que se puedan aprovechar más adelante. Imagine el desastre inminente si una empresa de inversión recibiera un nuevo envío de PC con componentes falsificados.

Riesgo de identidad. Las vulneraciones relacionadas con credenciales robadas o comprometidas son uno de los vectores de ataque de más rápido crecimiento. No es de extrañar. Los atacantes que utilizan credenciales válidas pueden iniciar sesión en un PC, moverse libremente dentro de la red corporativa y permanecer sin ser detectados durante largos periodos de tiempo. Según el último informe Cost of a Data Breach de IBM, se tardó en identificar y contener estas vulneraciones una media de 292 días, el vector de ataque más prolongado de todos los que se hayan estudiado. Ese nivel de acceso es demasiado valioso para que los atacantes lo ignoren. De hecho, las investigaciones de Zscaler muestran que los agentes maliciosos están perfeccionando el robo de credenciales para mejorar y escalar sus ataques de phishing mediante el uso de IA generativa. Este acceso no autorizado aplicado a datos confidenciales de entrenamiento o inferencia, o directamente a modelos, se clasifica como un **ataque a la cadena de suministro del modelo**.

Amenaza interna. Investigaciones recientes muestran que, en comparación con otros vectores de ataque, los **ataques maliciosos internos** ocasionaron los mayores costes, con una media de 4,99 millones de dólares. Tenga en cuenta que los ataques internos pueden ocurrir en toda la cadena de suministro de hardware, la cadena de suministro de software y la cadena de suministro de modelos.►

Tiempo medio que un usuario final tarda en caer en un correo electrónico de **phishing**: <60 segundos*

Tiempo medio de 292 días para detectar y contener **riesgos de credenciales****

Los ataques internos maliciosos cuestan una media de 4,99 millones de dólares**

**Fuente: DBIR, Verizon, 2024*
***Fuente: Cost of a Data Breach, IBM, 2024*

Contramedidas que deben aplicarse

Qué mitiga el riesgo

Ninguno de estos objetivos de ataque es completamente nuevo. Tampoco lo son los objetivos finales de los atacantes. Como siempre, queremos centrarnos en mantener su parque informático seguro y resiliente. **Aplicar varias capas de contramedidas** puede ayudar a reducir la superficie de ataque y a detectar inmediatamente cualquier comportamiento sospechoso.

Una **mentalidad de confianza cero** mitigará el riesgo en todo su parque informático. Los principios de no confiar nunca, comprobar siempre y supervisar continuamente le ayudan a mantenerse un paso por delante de los atacantes. Es imposible bloquear el 100 % de los ataques. Para tener un estado de seguridad sólido, necesita **visibilidad y control** en todo su ecosistema de TI.

Con ese marco en mente, reevalúe su infraestructura, especialmente los sistemas y procesos que interactúan con la inteligencia artificial. ¿Qué contramedidas minimizan el riesgo de comprometer los dispositivos, la identidad y las amenazas internas?►

Los principios básicos de confianza cero le ayudan a defenderse contra el riesgo y a reducir el radio de expansión de la ciberactividad.

- Asume el peor de los casos
- Sin confianza implícita
- Autenticación continua

Contramedidas que deben aplicarse (cont.)

Qué mitiga el riesgo (cont.)

Hay dos categorías generales de contramedidas.

La seguridad "por debajo del SO" protege los dispositivos de IA en los que trabaja. Podemos dividirla en dos partes:

- Defienda su parque informático con dispositivos **diseñados de forma segura**. Esto significa utilizar PC con IA que sean seguros desde el diseño, es decir, que se hayan desarrollado con principios de diseño seguros y en una cadena de suministro segura.
- Defienda su parque informático con dispositivos con **seguridad integrada**. Los PC con IA seguros incluyen capas de protección integrada que proporcionan visibilidad (hasta los niveles del BIOS y silicio) desde el primer momento.

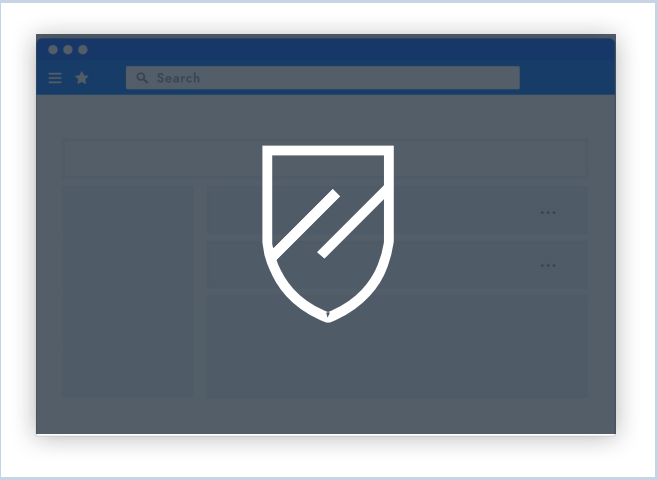
La seguridad "por encima del SO" protege el acceso a los modelos de IA. Defienda los datos y los modelos *con* los que trabaja y las redes corporativas *en* las que trabaja con **seguridad de software**. Es esencial proteger las operaciones de seguridad de aprendizaje automático y supervisar el tráfico de red de las cargas de trabajo de IA implementadas.►

Seguridad por debajo del SO

PC con IA seguros

Seguridad de hardware y firmware, seguridad en la cadena de suministro, núcleo de chips

Seguridad por encima del SO



Seguridad de software

Capa adicional de seguridad para puntos finales, redes y entornos de cloud

Servicios de seguridad y conocimientos disponibles para integrar todos estos elementos.

Aplicación de procedimientos recomendados a todo el parque informático

Cómo los PC Dell con IA aportan seguridad básica a su parque informático

Aquí es donde Dell Trusted Workspace puede ayudar. Nuestros tecnólogos diseñan y conciben la seguridad de nuestros PC comerciales con IA con una profunda comprensión de la mentalidad de adversario.

Por debajo del sistema operativo, el diseño seguro, los sólidos controles de la cadena de suministro y la garantía opcional de la cadena de suministro ayudan a garantizar que los PC estén seguros desde el primer arranque. La seguridad integrada del hardware y el firmware mantiene el PC protegido mientras se utiliza, por ejemplo, detecciones de manipulación a nivel del BIOS exclusivas de Dell* (Dell SafeBIOS) y seguridad de credenciales sin contraseña (Dell SafeID) para protegerlo frente a accesos no autorizados. Además, las tecnologías de silicio de Intel® ayudan a proporcionar una base para proteger diversos aspectos de la IA tal como la utilizan los clientes de PC con IA. Por ejemplo, Intel ayuda a proteger los datos de IA en reposo en el cliente con aceleración para el cifrado de modelos en el disco.►

Aplicación de procedimientos recomendados a todo el parque informático (cont.)

Cómo los PC con IA Dell ayudan a aportar seguridad básica a su parque informático (cont.)

Para complementar esta seguridad por debajo del sistema operativo, la tecnología Persistence de nuestro socio Absolute se puede integrar en la fábrica para obtener aún más visibilidad y control durante todo el ciclo de vida del PC, lo que permite, por ejemplo, la geolocalización de los dispositivos en tránsito y la autorreparación de aplicaciones críticas en el peor de los casos.

De hecho, Dell ha seleccionado un ecosistema de soluciones de socios de software, como CrowdStrike Falcon XDR y Absolute Secure Access, que activan los principios de confianza cero para proteger la cadena de suministro de su modelo frente al acceso no autorizado por **encima del SO**. Con estas soluciones, puede crear y aplicar políticas con controles de acceso granulares (por ejemplo, control de acceso basado en funciones o RBAC) para mitigar el riesgo de que personal interno malintencionado acceda o manipule sus modelos de IA.►

Aplicación de procedimientos recomendados a todo el parque informático (cont.)

Cómo los PC con IA Dell ayudan a aportar seguridad básica a su parque informático (cont.)

En conjunto, esto constituye la ***seguridad para la IA***. Estas capacidades defienden las cargas de trabajo de IA en el dispositivo contra los ciberataques, lo que le permite centrarse en la innovación y en el crecimiento del negocio. ►

Detenga los ataques avanzados a puntos finales con defensas coordinadas de hardware y software

Dell trabaja con Intel y CrowdStrike para integrar las capas por debajo y por encima del sistema operativo mediante seguridad asistida por hardware. *Más información >*

Conclusiones clave y próximos pasos

Proteja la IA en el punto final con Dell

Las empresas están entusiasmadas con la IA, pero la preparación para adoptarla aún es limitada, según una encuesta reciente de CISO realizada por Absolute. Un análisis de millones de dispositivos reveló que la población de PC no puede absorber las nuevas capacidades de IA en general. **Dell puede ayudarle a reunir todo lo necesario.**

Desarrolle e implemente modelos de IA sobre una base segura y moderna. El soporte para Windows 10 finaliza en octubre de 2025. Los PC ya no recibirán actualizaciones de seguridad, actualizaciones de funciones ni soporte para Windows 10. Es posible que los dispositivos más antiguos no cumplan los requisitos de Windows 11 y no incorporen las mejoras integradas más recientes en rendimiento, seguridad e IA. Actualice a **Dell Pro** o **Dell Pro Max con procesadores Intel® Core™ Ultra con Intel vPro®** para aprovechar los beneficios de seguridad y defender las cargas de trabajo de IA con los **PC comerciales con IA más seguros del mundo.*** ►

El soporte para Windows 10 finaliza en octubre.

Actualice a los PC con IA Dell más recientes basados en Intel para aprovechar los beneficios de seguridad y las mejoras de IA:

Compre Dell Pro ● Dell Pro Max

*Los PC comerciales con IA más seguros del mundo**

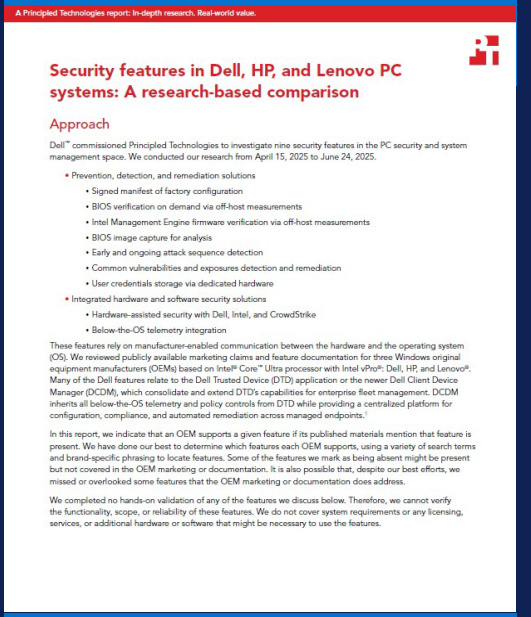
Explore software y servicios de valor agregado para mejorar su estado de seguridad:

Software e integraciones

Servicios

Liderazgo en el sector

Principled Technologies revela que la seguridad de los PC comerciales con IA de Dell e Intel supera a la de sus homólogos


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Leer el estudio

Descargos de responsabilidad

*Basado en un análisis independiente realizado por Principled Technologies al comparar PC comerciales con IA de Dell con procesadores Intel frente a HP y Lenovo, julio de 2025. Respaldado por un análisis interno de Dell sobre el mercado mundial de PC, octubre de 2024. Aplicable a PC con procesadores Intel. No todas las funciones están disponibles en todos los PC. Algunas funciones requieren compras adicionales.

Más información:

Contáctenos: Global.Security.Sales@Dell.com

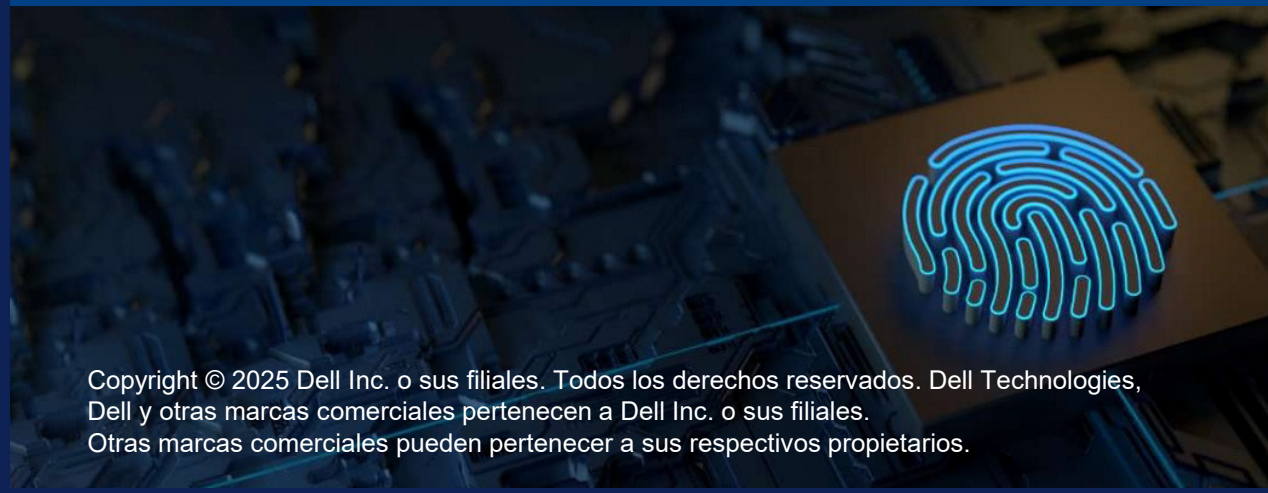
Visítenos: Dell.com/Endpoint-Security

Síganos: LinkedIn @DellTechnologies | X @DellTech

Acerca de la seguridad de puntos finales de Dell

La seguridad es un tema abrumador para organizaciones de todos los tamaños. **Contrate a un socio de tecnología y seguridad experimentado para modernizar la seguridad de puntos finales**.

Dell Trusted Workspace ayuda a proteger los puntos finales para conseguir un entorno de TI moderno y preparado para la confianza cero. Reduzca la superficie de ataque y mejore la ciberresiliencia con una cartera completa de protecciones de hardware y software exclusivas de Dell. Nuestro enfoque, ampliamente coordinado y basado en la defensa, desvía las amenazas mediante la combinación de protecciones integradas y una vigilancia constante. Los usuarios finales se mantienen productivos y el equipo de tecnología informática trabaja con confianza gracias a soluciones de seguridad creadas para el mundo basado en la cloud de hoy en día.



Copyright © 2025 Dell Inc. o sus filiales. Todos los derechos reservados. Dell Technologies, Dell y otras marcas comerciales pertenecen a Dell Inc. o sus filiales.
Otras marcas comerciales pueden pertenecer a sus respectivos propietarios.