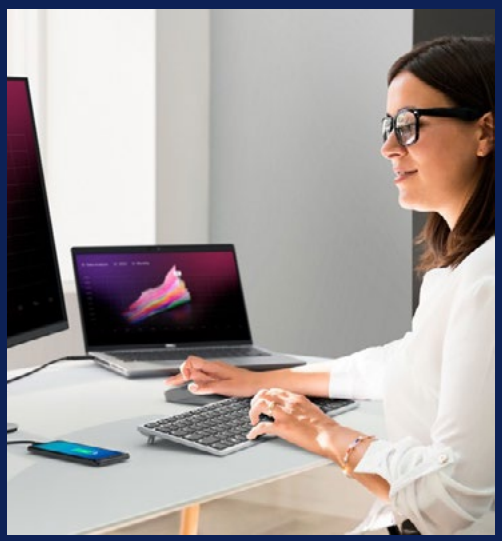
DELL Technologies

No renuncie a nada

Cómo proteger a los trabajadores que utilizan la IA generativa con Dell Technologies, Microsoft e Intel.



Windows 11

intel

Resumen ejecutivo

La transición al trabajo híbrido ha incrementado la complejidad y ha introducido nuevos vectores de ataque; además, los puntos finales, las redes y las clouds han pasado a ser superficies de ataque en expansión. Por otra parte, la carrera hacia la adopción de la IA generativa se hace más complicada con nuevos aspectos relativos a la seguridad, las filtraciones de datos e IP y los ataques contextuales a gran velocidad.

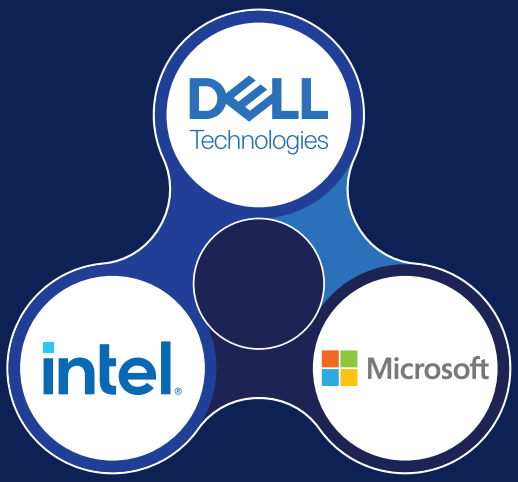
Además, ahora los atacantes emplean técnicas sofisticadas que se dirigen a diferentes capas de la pila informática y se mezclan con los procesos válidos del sistema. Algunos métodos permiten incluso a los atacantes obtener un acceso privilegiado y desactivar las protecciones de software sin ser detectados en ningún momento.

Todos a una…

Un proveedor por sí solo no puede abordar todas estas complejidades; por este motivo, Dell, Intel y Microsoft colaboran de forma estratégica para aliviar la carga a las organizaciones.

Nuestro enfoque holístico de la seguridad integra funciones "por debajo del SO" basadas en hardware que ayudan a defenderse de los ataques con seguridad basada en chip de Intel que protege los niveles más profundos de un dispositivo.

Posteriormente, nos aseguramos de que Windows 11, los dispositivos y el software modernos de Dell funcionen en conjunto para reducir la superficie de ataque, proteger la integridad del sistema y blindar a los usuarios y los datos importantes.



Mejor juntos. Mejor para usted.

La seguridad exclusiva que integra e incorpora Dell Technologies incluye toda la innovación en protección de nuestros socios Intel y Microsoft, para que pueda proteger a sus empleados híbridos frente a las amenazas a la seguridad en constante evolución.

Solo el 33 % de los responsables de la toma de decisiones de TI emplea una estrategia de seguridad integral con medidas de protección basadas tanto en hardware como en software.

Fuente: Dell Innovation Index, 2023

Temas tratados en este informe

Pilares de la seguridad

Ciclo de vida del desarrollo seguro

Dell Technologies, Intel y Microsoft colaboran estrechamente para integrar la seguridad desde el chip hasta la cloud. Un ejemplo de esto son los dispositivos de confianza de Dell, los PC más seguros que existen en el sector.*

Seguridad de la cadena de suministro

Se han incorporado medidas de protección en toda la cadena de suministro para garantizar la seguridad de los dispositivos después de salir de la fábrica.

* Según análisis internos de Dell, septiembre de 2022. No todas las funciones están disponibles en todos los PC. Algunas funciones requieren compras adicionales.

Infraestructura de defensa integral: implantamos el modelo de seguridad de confianza cero

Seguridad con tecnología de IA

Aproveche la IA para automatizar los procesos para la protección de los usuarios que ofrece soluciones de seguridad revolucionarias listas para usar.

Seguridad por debajo del SO

Las funciones de seguridad basadas en hardware protegen los dispositivos frente a las amenazas que atacan a sus capas básicas.

Seguridad por encima del SO

Las tecnologías de seguridad basadas en software y las medidas de protección integradas en el chip resultan cruciales para conseguir una seguridad integral de los dispositivos.

Seguridad de Windows 11

Funciones de protección listas para usar con capas de software y hardware estrechamente integrados en sistemas operativos, aplicaciones, identidades y la cloud.

Asistencia permanente

Dell, Intel y Microsoft garantizan una seguridad permanente en sus productos con medidas de corrección de las vulnerabilidades y actualizaciones de la seguridad integrada en el chip dentro del SO.

El punto final más expuesto de su red empresarial es lo que marca su nivel de seguridad

Da la impresión de que, cada pocos meses, surge otra empresa de renombre global que sufre una vulneración de la seguridad importante, con la consiguiente crítica por parte del público, algo que daña gravemente su reputación. Esto basta para que los empresarios y profesionales de la seguridad piensen en que pueden correr la misma suerte, ya sea por una vulnerabilidad que ha pasado desapercibida o introducida en sus dispositivos o bien un punto débil desconocido y explotable en su software. Seguramente confíe en su equipo de TI para la protección de las redes y el establecimiento de prácticas seguras de datos, pero ¿cómo puede estar seguro de que van a responder todos los puntos finales y las aplicaciones que utiliza en su empresa si no puede supervisar su fabricación o desarrollo?

Dell, Microsoft e Intel saben que la única forma de proteger de forma fiable los dispositivos y las redes empresariales es mediante una armonización de las tecnologías de seguridad de hardware y software. Aunque nuestros equipos han trabajado juntos para hacer una cota de malla de funciones de seguridad de software y hardware estrechamente integradas, es posible que otros proveedores no hayan dado este paso.

Un método habitual pero imperfecto para abordar la integridad de los dispositivos consiste en tratar de crear una falsa sensación de seguridad a través de soluciones exclusivamente para software sin tener en cuenta las vulnerabilidades subyacentes en el hardware. Es importante que los responsables empresariales vean las limitaciones de esta estrategia. Si se utiliza exclusivamente software para la protección de las empresas, queda expuesto a ataques el hardware donde se ejecuta este software. Básicamente, si el hardware no es seguro, las aplicaciones y tecnologías de seguridad que se ejecutan en él tampoco pueden serlo.

Otros proveedores intentan “vallar el jardín” para proteger los dispositivos, por lo que establecen limitaciones en aplicaciones y servicios que restringen la flexibilidad de los usuarios. Aunque esto puede tener sentido en el contexto del consumidor, se sacrifica la libertad a la hora de poder aprovechar completamente los dispositivos, un problema que se agrava aún más en el contexto comercial. Este método también puede llevar a los atacantes a apuntar cada vez más a estos sistemas para dañarlos y dejar al descubierto vulnerabilidades en configuraciones comunes.

En pocas palabras, lo que funciona para los dispositivos de consumo directo suele fallar cuando se aplica a entornos comerciales, que son un objetivo más atractivo para los atacantes.

Por eso Dell, Microsoft e Intel adoptan un enfoque diferente e integral de la seguridad.

El punto final más expuesto de su red empresarial es lo que marca su nivel de seguridad

Dell, Microsoft e Intel ofrecen seguridad integrada basada en hardware

La complejidad y consideraciones que conlleva la protección de los dispositivos y las redes son un quebradero de cabeza. Por ello hemos asumido la labor de ofrecer a nuestros clientes dispositivos diseñados atendiendo a la seguridad para que puedan centrarse en lo que realmente importa: hacer que la empresa prospere.

Dell, Microsoft e Intel llevan varias décadas colaborando en el ámbito de la ingeniería y siempre se han dedicado a administrar la seguridad de los datos de nuestros clientes, especialmente en el mercado de Business-to-Business (B2B). Gracias a su colaboración con Microsoft e Intel, Dell ha consolidado su reputación como proveedor de referencia de dispositivos de empleados para empresas de todos los tamaños y en todos los mercados.

¿Qué tiene un dispositivo comercial de Dell? Bastante más que una colección aleatoria de funciones y características: juntos creamos tecnologías, herramientas y políticas para la totalidad todo del ciclo de vida de los PC comerciales, con el fin de ayudar a establecer medidas de seguridad integral para nuestros clientes y sus empresas.

Seguro por diseño

Microsoft, Intel y Dell van por delante de las amenazas actuales en el diseño de los sistemas del mañana para minimizar la superficie de ataque y garantizar la seguridad de los dispositivos comerciales.

Protección durante el tránsito

Contamos con tecnologías y políticas para proteger la integridad de los dispositivos antes de que lleguen a sus manos, ya que mantenemos la seguridad durante el suministro de componentes, el montaje y la entrega.

Defensa frente a las amenazas en constante evolución

Utilizamos seguridad basada en hardware a través de las tecnologías de los dispositivos de confianza Dell y las funciones de Intel® Hardware Shield para reforzar la defensa de los dispositivos mediante una infraestructura de prevención, detección y respuesta. Además, Dell, Microsoft e Intel cuentan con equipos de seguridad dedicados a sondear productos para localizar nuevas vulnerabilidades, antes de que lo hagan los atacantes, y desplegar parches con rapidez para ayudarle tanto a usted como a sus empleados a protegerse.

En este documento técnico, exploraremos cómo Dell, Microsoft e Intel han colaborado para crear plataformas de PC comerciales con seguridad incorporada en los niveles más profundos con el fin de proteger los dispositivos a lo largo de su ciclo de vida, hasta la próxima actualización y bastante después.

La protección de las plataformas comienza en la pizarra blanca

Planificación, evaluación y análisis

Antes empezar a diseñar sus últimas plataformas y conjuntos de chips, los expertos de Dell, Microsoft e Intel, respectivamente, definen estrictos parámetros para determinar lo que se necesita en una plataforma segura para satisfacer las necesidades de seguridad del futuro y cumplir la normativa de seguridad necesaria. Este proceso comienza con un debate para determinar los posibles riesgos futuros de seguridad y privacidad, así como las medidas necesarias para abordarlos. Esta evaluación se utiliza para definir los objetivos de seguridad que emplearemos para evaluar nuestras arquitecturas.

Con esta información, los equipos de seguridad de Dell, Microsoft e Intel desarrollan modelos de amenazas adoptando una mentalidad de adversario y analizando las posibles vulnerabilidades de seguridad y puntos débiles que se deben mitigar. Este ejercicio ha demostrado ofrecer mejoras significativas para detectar y mitigar posibles vulnerabilidades en el diseño del BIOS, el firmware y el hardware.

Diseño centrado en la seguridad

Una vez que se han efectuado las evaluaciones de las amenazas y se han creado modelos para definir la superficie de las amenazas y dónde se deben centrar las pruebas, los ingenieros comienzan a desarrollar el código del producto. Los objetivos de seguridad definidos en la etapa anterior ofrecen orientación durante esta fase de desarrollo y sirven como criterios para determinar si el producto está va por el buen camino para satisfacer las necesidades de los clientes.

La protección de las plataformas comienza en la pizarra blanca

Verificación y pruebas

Una vez perfeccionado el código hasta que cumpla los objetivos de seguridad trazados al inicio del ciclo de vida de desarrollo, el producto pasa a un riguroso proceso de pruebas.

Por lo general, estas pruebas comienzan con revisiones de código seguro y análisis de código estático, un proceso automatizado que se sirve de herramientas especiales para buscar y reparar defectos. Algunos productos con código más complicado pasan, posteriormente, a un proceso de revisión manual, donde los expertos en seguridad revisan el código de producto línea por línea para encontrar errores que pudieron haber pasado desapercibidos y garantizar el desarrollo se efectuó de forma segura.

Por último, se indica a los equipos de hackers expertos que efectúen pruebas de penetración y otras actividades de Red Team para encontrar posibles vulnerabilidades que se hayan pasado por alto en las fases anteriores. Estos hallazgos se mitigan de nuevo en función del riesgo, de forma que cualquier exposición adicional identificada quede documentada y corregida.

Lanzamiento y seguimiento posterior

Una vez que se el producto se ha probado y verificado cumple o supera los objetivos de seguridad definidos al principio, estará listo para su lanzamiento al mercado. Sin embargo, estas fases representan solo un segmento del ciclo de vida del desarrollo seguro. Para Dell e Intel, la seguridad de nuestras plataformas requiere un trabajo constante. Nuestros equipos se dedican a detectar las vulnerabilidades antes de que las puedan explotar los atacantes y, después, desarrollan y distribuyen actualizaciones de seguridad para corregirlas.

Un ejemplo de nuestro compromiso para implantar una seguridad integral es todo el trabajo dedicado a conseguir una cadena de suministro segura entre el montaje y la entrega de los dispositivos, uno de los vectores de ataque de más rápido crecimiento para los atacantes maliciosos. En la siguiente sección, profundizaremos en cómo Dell e Intel mitigan los riesgos en sus cadenas de suministro para garantizar que los dispositivos que reciben los usuarios a domicilio sean seguros desde que se arrancan por primera vez.

Proteger la cadena de suministro es esencial para la seguridad de los dispositivos

Entre que un componente o dispositivo sale de fábrica y llega a su destino, pueden ocurrir muchas cosas. Cada paso de la cadena de suministro es un nuevo vector que deja a sus empleados, empresa y clientes a merced de posibles ataques. Dell e Intel han desarrollado herramientas, tecnologías y procesos para ayudar a garantizar la seguridad de sus productos antes de que lleguen a las empresas de los clientes, y permitir la autoverificación de la autenticidad de los dispositivos antes de entregarlos a los empleados.

Obtención

Dell emplea un riguroso proceso de análisis de los socios para garantizar la calidad y la seguridad de los dispositivos y sus componentes. Estos socios también se someten a auditorías rutinarias para garantizar que cumplen el amplio conjunto de normas de seguridad de la cadena de suministro de Dell.

Fabricación

Además de cumplir los estándares de seguridad de la cadena de suministro de Dell, los fabricantes de dispositivos Dell también prueban con frecuencia las piezas durante la fabricación para garantizar que no se infiltran productos falsificados en la cadena de suministro. Para mitigar aún más este riesgo, se colocan etiquetas con un número único de identificación de pieza (PPID) en componentes específicos de alto riesgo, que contienen información sobre el proveedor, el número de pieza, el país de origen y la fecha de fabricación, para que Dell pueda identificar, autenticar, rastrear y finalmente validar estos componentes con el fin de garantizar que el cliente reciba exactamente lo que se hubo enviado.

Entrega

Los envíos de Dell están protegidos por capas de seguridad física, desde precintos antimanipulación y mecanismos de bloqueo de las puertas hasta diversos dispositivos de seguimiento diseñados para detectar si los dispositivos Dell transportados se han manipulado durante el tránsito.

Los propios dispositivos Dell también cuentan con tecnologías de detección de manipulaciones. Las soluciones de cadena de suministro segura de Dell Technologies se ocupan de los controles de integridad y seguridad de la cadena de suministro, como los precintos antimanipulación y los borrados de disco duro de nivel NIST para favorecer su reputación empresarial desde el principio.

Proteger la cadena de suministro es esencial para la seguridad de los dispositivos

Verificar

Los dispositivos comerciales Dell se envían con certificados de plataforma firmada criptográficamente que captura atributos de instantánea de plataformas durante la fabricación, montaje, pruebas e integración. Estos atributos de plataforma se vinculan posteriormente de forma criptográfica con un dispositivo en particular a través de Trusted Platform Module (TPM) como raíz de confianza del hardware.

Dell ha implementado certificados de plataforma Trusted Computing Group en la solución Dell Secured Component Verification (SCV) para PC comerciales con procesadores Intel. SCV entrega a TI certificados de inventario firmados criptográficamente para dispositivos Dell compatibles. Con herramientas de auto-verificación seguras, SCV ayuda a garantizar la integridad del hardware durante el transporte hasta los entornos informáticos y permite a los clientes verificar que los PC comerciales y los componentes clave de Dell llegan exactamente como se han pedido y fabricado.

De manera similar, Intel lleva muchos años facilitando a los proveedores transparencia y seguimiento básico de la cadena de suministro digital. Intel® Transparent Supply Chain (Intel® TSC) entrega certificados de plataforma TCG y distribuye datos de componentes para admitir plataformas basadas en Intel mediante una API de cloud disponible a la que puede acceder el equipo de TI a través del portal web de Intel® TSC. Aunque Dell e Intel optaron por implementar soluciones independientes, los certificados de la plataforma TCG son un ingrediente común entre Intel® TSC y Dell SCV. Este rasgo común hace que exista compatibilidad e interoperabilidad, lo que permite a los compradores empresariales y gubernamentales implementar certificados de plataforma TCG para mejorar la garantía de seguridad de la cadena de suministro digital para dispositivos basados en Intel.

Infraestructura de defensa integral: implantamos el modelo de seguridad de confianza cero

Las organizaciones que quieren evolucionar en ciberseguridad establecen un roadmap viable que apunte formas para reducir la superficie de ataque, detecte las ciberamenazas y responda ante ellas, e implemente procesos de recuperación frente a ciberataques; todo ello, con funciones basadas en seguridad de confianza cero.

Para abordar unas ciberamenazas cada vez más sofisticadas, Dell utiliza las funciones de seguridad integradas en nuestras soluciones y las de nuestros socios, incluso Microsoft e Intel, para que los clientes consigan una seguridad de confianza cero que se adapte a sus objetivos empresariales.

77 %

no ha estudiado o creado una arquitectura de confianza cero*

* Dell Technologies, Innovation Index, 2023: https://www.dell.com/en-us/dt/perspectives/innovation-index.htm

Simplifique drásticamente la adopción del modelo de confianza cero entre sus empleados con una arquitectura totalmente integrada

Dell, Microsoft e Intel colaboran para ofrecer un entorno de trabajo híbrido seguro y eficiente que permita a los clientes adoptar los tres aspectos fundamentales del modelo de confianza cero:

1. Verificación explícita

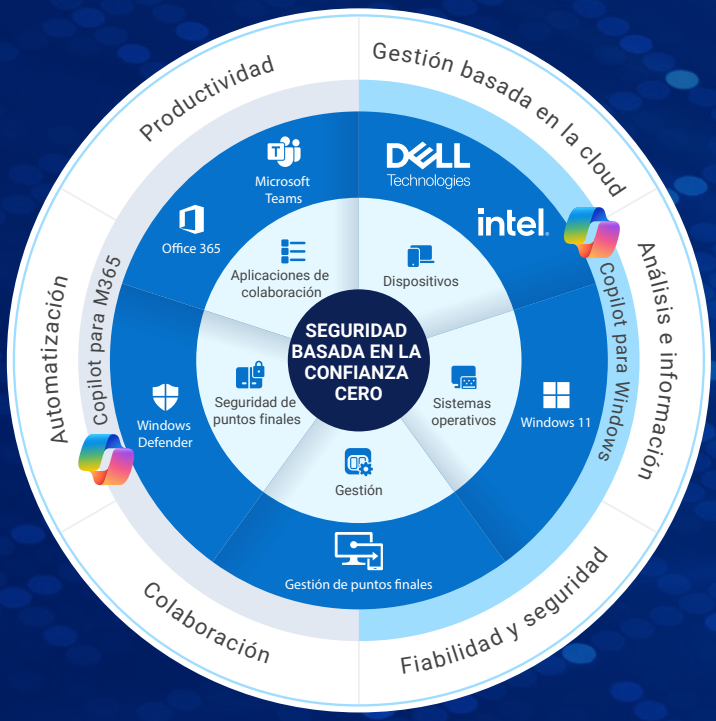
La autenticación y la autorización deben incluir todos los puntos de datos disponibles, como la identidad del usuario, su ubicación, el estado del dispositivo, los servicios o las cargas de servicio, clasificaciones de datos y anomalías.

2. Acceso de privilegios mínimos

Limite el acceso de los usuarios mediante métodos "justo a tiempo" y de "acceso justo" (JIT/JEA), políticas adaptables basadas en el riesgo y protección de datos para garantizar la seguridad de los datos y la productividad.

3. Mentalidad "Assume breach"

Trabaje intentando minimizar el radio de impacto y el acceso por segmentos. Verifique el cifrado integral y utilice análisis para obtener visibilidad, mejorar la detección de amenazas y reforzar las defensas.



Nuestras soluciones conjuntas ayudan a las organizaciones a implementar el modelo de seguridad de confianza cero, ya que verifican cada intento de acceso y aplican estrictas políticas de seguridad basadas en la identidad, el estado del dispositivo, la ubicación y el grado de riesgo, lo cual reduce el riesgo de que se produzcan accesos no autorizados y mitiga el impacto de las vulneraciones de la seguridad.

Se logra mediante la integración de:

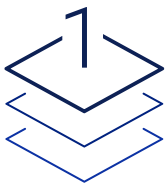
La seguridad del BIOS y el firmware, la seguridad del hardware, la garantía de la cadena de suministro, el software de gestión de amenazas (EDR, XDR, VDR) y el software de protección de red y datos en la cloud de los PC comerciales Dell, combinados con Intel® Hardware Shield, exclusivamente en la plataforma Intel vPro®.

Completo conjunto de herramientas y tecnologías de Microsoft para la administración de los accesos y las identidades, la seguridad de los puntos finales, la seguridad de la red, la protección de datos, la inteligencia frente a amenazas, el análisis de seguridad, la aplicación de políticas y la supervisión y la respuesta continuadas. Esto incluye Azure Active Directory, Microsoft Defender para punto de conexión, Azure Firewall, Azure Information Protection, Microsoft Threat Intelligence, Azure Sentinel, Microsoft Endpoint Manager y el centro de seguridad de Microsoft.

Seguridad con tecnología de IA

Seguridad basada en IA revolucionaria ya lista para usar.

Dell, Intel y Microsoft utilizan la IA para automatizar los procesos de protección de los usuarios que ofrecen soluciones de seguridad revolucionarias listas para usar. Estas innovadoras medidas se han diseñado para evitar y detectar los ataques actuales, que son más sofisticados, e incluyen seguridad basada en hardware, cifrado avanzado y protección frente a malware; todo ello, con la tecnología de los procesadores Intel® Core™ Ultra en Intel vPro® y los sistemas operativos Windows 11 Pro, integrados a la perfección en los dispositivos modernos de Dell. Gracias a esta colaboración se ha conseguido reducir notablemente la superficie de ataque implementando capas de defensas básicamente en tres áreas clave:



1. Por debajo del SO:

- Dell e Intel han colaborado estrechamente para desarrollar Dell SafeBIOS, un mecanismo de defensa sólido frente a los ataques al BIOS y al firmware, que incorpora verificación fuera del host para garantizar la integridad del BIOS mediante firmware en Intel vPro®.
- La versión más reciente de la plataforma Intel vPro® reduce la superficie de ataque física hasta en un 70 % (en comparación con dispositivos de hace cuatro años).*
- Dispositivos Dell con Intel vPro® que cuentan con la certificación de nivel 3 de PC Windows 11 con núcleo protegido, así como un conjunto de protecciones estrechamente integradas.
- Por ejemplo, el informe de seguridad de sistemas Intel ofrece protección para SO respecto al proceso de arranque seguro, para garantizar la integridad desde el principio.
- Estas medidas de protección son inherentes y funcionan a la perfección sin necesidad de ningún tipo de configuración previa.

2. Protección de las aplicaciones y los datos:

- Se han implementado funciones avanzadas para salvaguardar las credenciales de los usuarios, entre las que se incluyen las credenciales que facilita Windows Hello a través de las tecnologías de virtualización de Intel.
- El cifrado íntegro de la memoria con varias claves hace posible cifrar la memoria de las máquinas virtuales de Windows 11, de forma que se puedan aislar los procesos y los datos asociados con eficacia.
- Estas medidas de protección se configuran previamente para utilizarlas de forma inmediata o se pueden ajustar cómodamente a través del centro de seguridad de Windows.

3. Detección de amenazas avanzadas:

- Intel® Threat Detection Technology (TDT) sobresale por ser la única solución de detección de amenazas por IA y basada en chip capaz de impedir ataques de programas de secuestro y el criptominado.
- Dado que los programas de secuestro dependen enormemente de los recursos de la CPU para cifrar el contenido empresarial esencial, Intel TDT utiliza la detección de amenazas basada en IA para analizar la telemetría de la CPU en busca de indicadores de ataque, de forma que identifica rápidamente los procesos maliciosos para que el software de seguridad, como Microsoft Defender, pase a la acción con la cuarentena o la eliminación.

*13th Gen Intel® Core™ Processor Attack Study Report

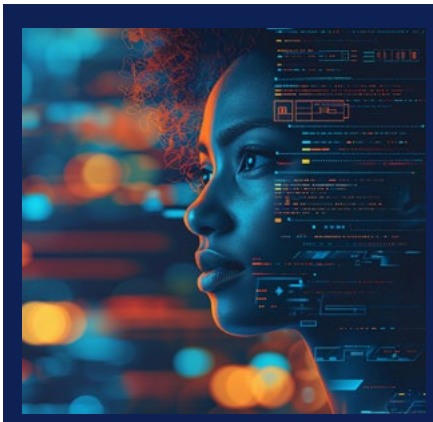
Seguridad con tecnología de IA

Nuestra colaboración también abarca la oferta de análisis acelerados de memoria para una detección anticipada de malware sin archivos, lo que ofrece una capa adicional de seguridad para rechazar ataques de malware. Gracias a la colaboración con Microsoft Defender e Intel Threat Detection Technology, optimizamos los procesos de análisis que consumen muchos recursos de computación al descargarlos de la GPU para que esta quede libre y pueda ofrecer productividad de forma ininterrumpida. En caso de ataques potenciales, la GPU se comunica de forma proactiva con Microsoft Defender, para establecer un método análisis más completo.

Esta función es una **ventaja para las organizaciones** por los siguientes **tres motivos:**

Reducción del volumen de ataques sin archivos, que se han convertido en el método predominante de entrada de varias ciberamenazas.

Detección anticipada de los programas de secuestro y tras amenazas maliciosos en la fase inicial de acceso a la memoria



Preservación de una experiencia del usuario de alto rendimiento, al tiempo que se efectúan análisis de seguridad.

Al utilizar los análisis de memoria acelerados, las organizaciones podrán reforzar su defensa frente a las ciberamenazas en constante evolución, a la vez que garantizan una eficiencia operativa y una productividad del usuario óptimas.

Básicamente, la colaboración entre Dell, Microsoft e Intel ofrece completas soluciones de seguridad que engloban la protección basada en hardware, los procesos de arranque seguro, la seguridad de las aplicaciones y los datos, y las funciones de detección de amenazas avanzadas; todo ello, meticulosamente entretejido para abordar las ciberamenazas en constante evolución que existen actualmente.

Tecnologías de seguridad integradas que ayudan a prevenir y detectar amenazas y responder ante ellas

Seguridad integral hace referencia a un método que además de utilizar el modelo heredado de programas de protección de software, mantiene el ritmo de las nuevas categorías de amenazas a la seguridad digital, la protección y la privacidad. Al combinar este tipo de seguridad con hardware, la tecnología de seguridad "por debajo del SO" ayuda a proteger todas las capas de la pila informática, ya que se ejecuta para prevenir y detectar ataques a las estructuras fundamentales, incluidas las variantes de amenazas que se producen con mayor frecuencia en la totalidad de la cadena de suministro. La relación de desarrollo conjunto en ingeniería entre Dell, Microsoft e Intel se ha centrado en respaldar esta superficie de ataque con un intrincado tejido de tecnologías tanto en los componentes como en la plataforma. Además de otras herramientas y tecnologías de Dell e Intel, Intel® Hardware Shield y la infraestructura SafeBIOS de Dell ofrece a los usuarios de dispositivos comerciales Dell protección integrada basada en hardware.

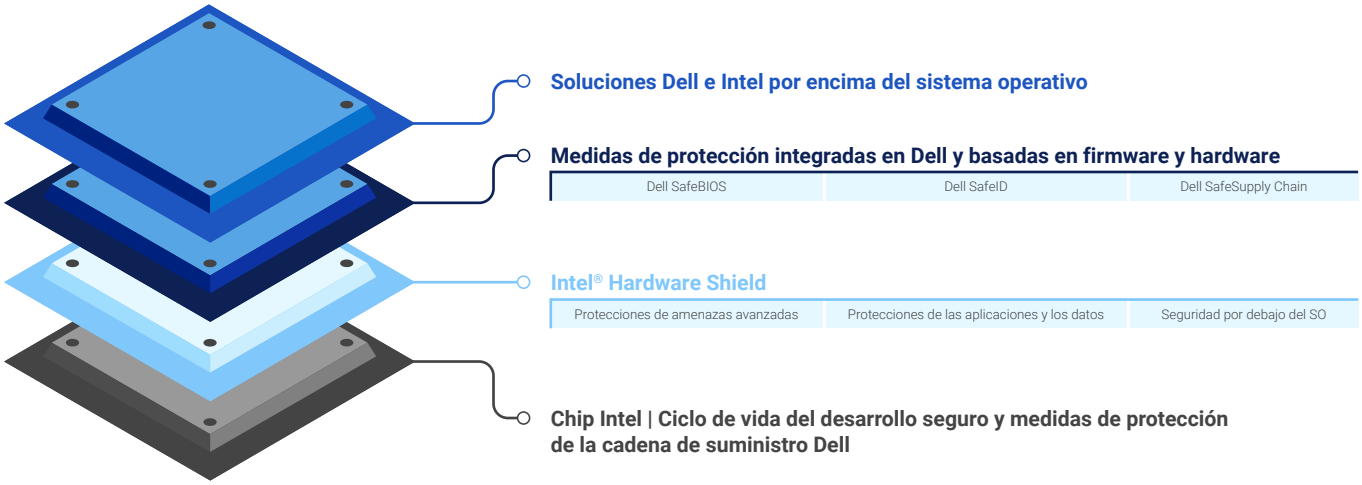


Figura 1: Intel® Hardware Shield y las medidas de protección basadas en hardware Dell son capas de seguridad que ayudan a defenderse frente a ataques en la base

Intel® Hardware Shield

Intel Hardware Shield se incluye en todos los dispositivos comerciales de Dell que se ejecutan en la plataforma Intel vPro® y ofrece funciones de seguridad mejoradas por hardware que ayudan a proteger todas las capas de la pila informática.

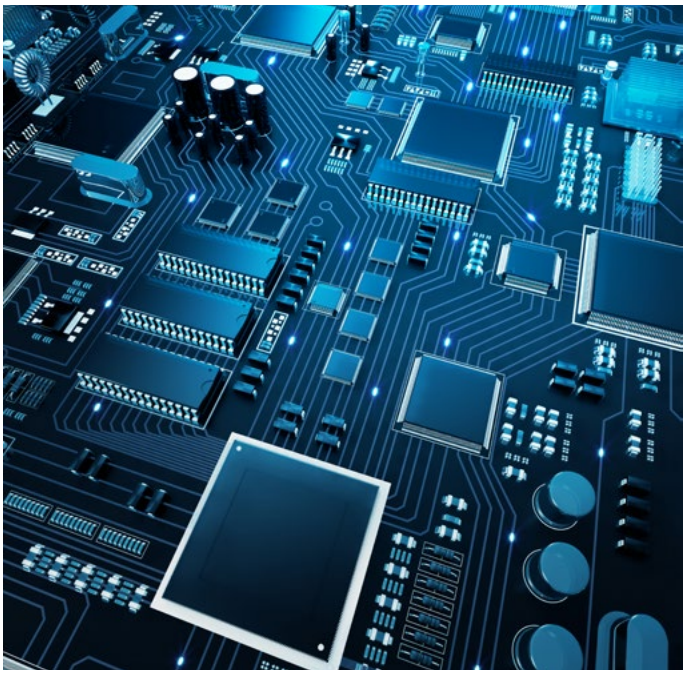
Intel Hardware Shield incluye protección contra amenazas avanzada, protección de los datos y las aplicaciones, y seguridad por debajo del SO, que consta de más de veinte innovadoras tecnologías de seguridad. Dell ha sacado partido a casi todas estas funciones para desarrollar soluciones de seguridad que se basen en sus funciones fundamentales para proporcionar a los clientes uno de los dispositivos comerciales más seguros del mercado. Estas soluciones incluyen la infraestructura Dell SafeBIOS, Dell SafeID y Dell SafeSupply Chain, que en conjunto ayudan a ofrecer un nivel aún mayor de garantía de protección frente a las amenazas actuales y las futuras.

Tecnologías de seguridad integradas que ayudan a prevenir y detectar amenazas y responder ante ellas

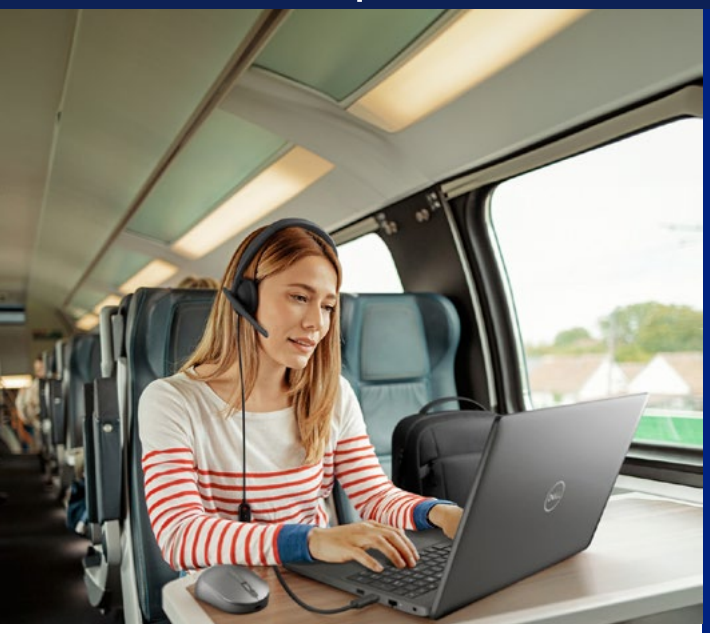
Infraestructura Dell SafeBIOS, Dell SafeID y Dell SafeSupply Chain

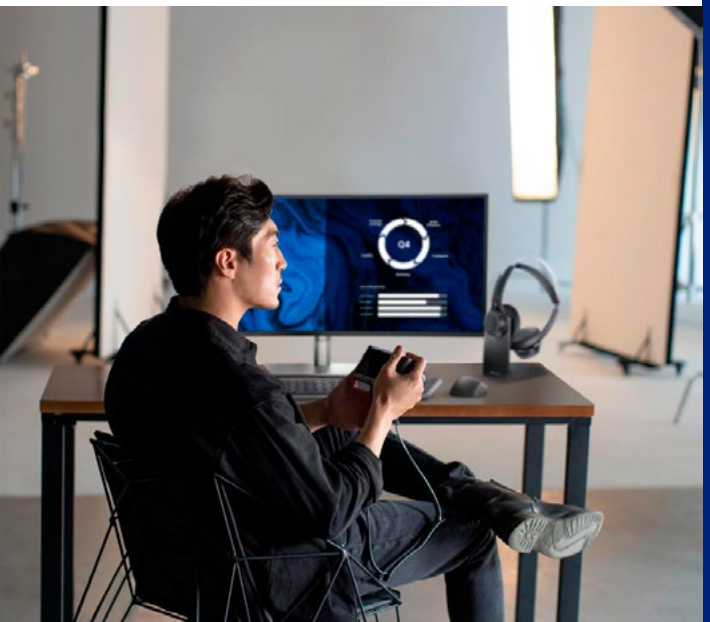
La protección del BIOS es fundamental para la seguridad de los dispositivos. Si un atacante consigue dañar el BIOS de un dispositivo, podría hacerse con el control de todo el dispositivo, ya que el BIOS tiene una posición única y privilegiada en la arquitectura de los dispositivos. Para proteger esta capa, que es crítica, los dispositivos comerciales Dell se distribuyen con SafeBIOS, un conjunto de herramientas que ayuda a evitar los ataques al BIOS, identificar si se ha vulnerado el BIOS y responder mediante alertas al departamento de TI en caso de encontrar irregularidades.

Determinados dispositivos comerciales Dell también incluyen Dell SafeID, que protege las credenciales de los usuarios finales en un chip de seguridad dedicado para mantenerlas ocultas de malware, que busca y roba las credenciales de acceso, una violación que podría poner en peligro toda una red empresarial. Para aumentar la seguridad de los productos, Dell ofrece funciones opcionales en forma de complemento como Secured Component Verification y embalajes con precinto a prueba de manipulación a través de Dell SafeSupply Chain.



Las soluciones de Dell e Intel por encima del OS ayudan mantener los puntos finales protegidos





A pesar del aumento de las amenazas de ataque por debajo del SO, la protección por encima del OS es ahora más importante que nunca antes. Con el aumento exponencial de usuarios finales que trabajan de forma remota y móvil, necesita soluciones inteligentes que eviten y detecten amenazas y respondan ante ellas dondequiera que ocurran. La cartera de seguridad de punto final Dell Trusted Workspace incluye software opcional como Dell SafeGuard and Response, junto con Dell SafeData con el fin de dotar a los líderes empresariales de las herramientas necesarias para proteger sus puntos finales. Las funciones de seguridad, estrechamente integradas en el chip, como Intel® Control-Flow Enforcement Technology, protegen frente a ataques dirigidos al SO, mientras que otras funciones de Intel Hardware Shield protegen por debajo del SO, ofrecen seguridad a las aplicaciones y los datos, y brindan protección contra amenazas avanzadas.

Posteriormente, añadimos la capa de seguridad de software de Microsoft, que se ejecuta desde la base de la seguridad hasta la cloud. En Windows 11, el hardware y el software se combinan para proteger los datos confidenciales desde el centro del PC hasta la cloud. La protección integral ayuda a salvaguardar la seguridad en toda la organización, independiente de donde trabajen los empleados. En la página siguiente, se muestran las capas de protección de Windows 11.

Las soluciones de Dell, Microsoft e Intel por encima del OS ayudan a mantener seguros los puntos finales

Posteriormente, Intel integra las protecciones de hardware adicionales en cada capa de la visión de seguridad de Microsoft. Después, estas protecciones se incorporan en las soluciones de cliente de Dell.

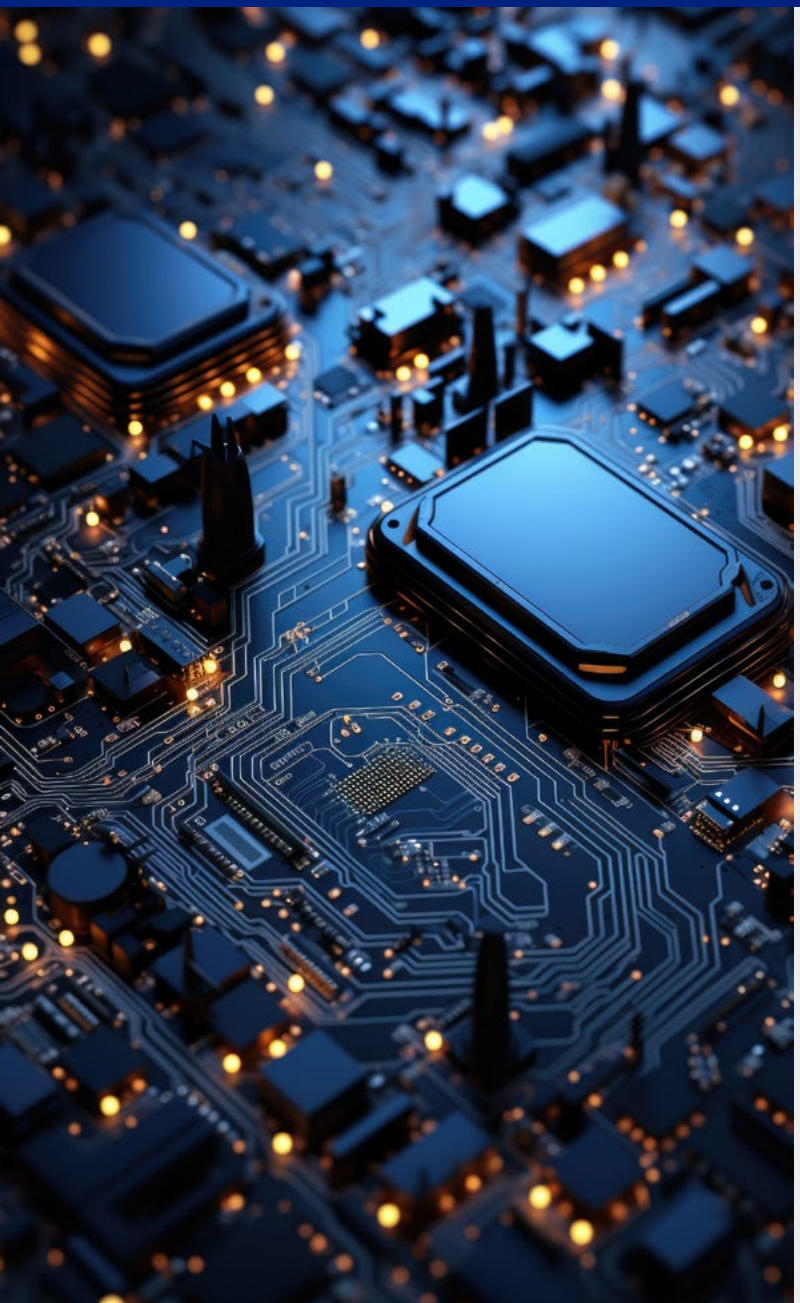
Nos asociamos para ofrecer una protección eficaz que no necesita configuración.

La seguridad exclusiva que integra e incorpora Dell Technologies incluye toda la innovación en protección de nuestros socios Intel y Microsoft, para que pueda proteger a sus empleados híbridos frente a las amenazas a la seguridad en constante evolución.

Seguridad de Windows 11

Protección integral con una gestión moderna.

Windows 11 es el sistema operativo de Windows más seguro que nunca ha existido, ya que las funciones de seguridad vienen configuradas y listas para usar. El hardware y el software funcionan en combinación para proteger los datos confidenciales desde el centro del PC hasta la cloud, con capas de protección en cada nivel de hardware, sistema operativo, aplicaciones, identidades y la cloud; todo ello, con una mejora en la productividad, la seguridad y la resiliencia allí donde estén los trabajadores.

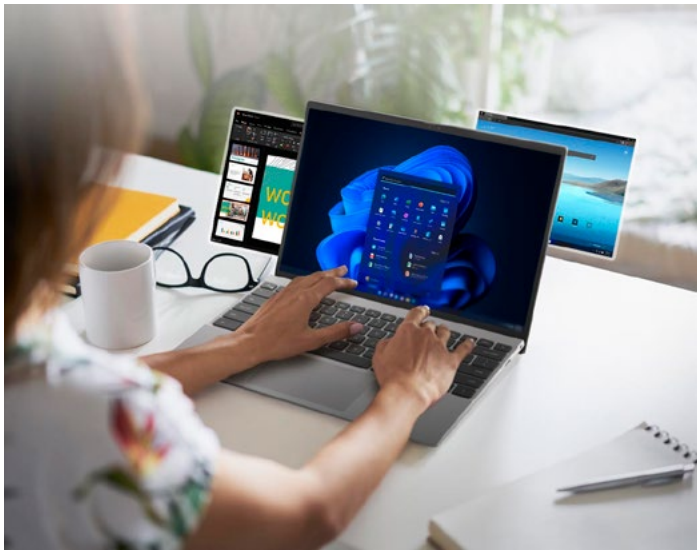


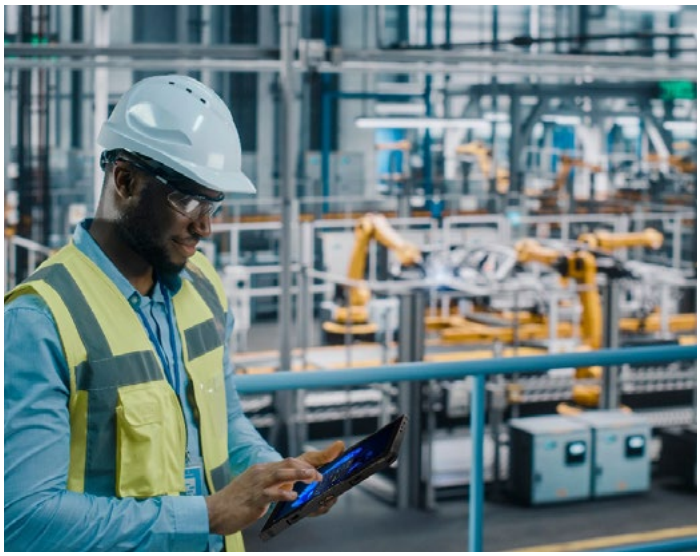
Hardware (chip)

Raíz de confianza en el hardware
Una raíz de confianza de hardware ayuda a proteger y mantener la integridad del sistema cuando arranca, carga firmware y, posteriormente, inicia el sistema operativo; de este modo, se consiguen importantes objetivos de seguridad del sistema.

Trusted Platform Module (TPM)
La tecnología de Trusted Platform Module (TPM) está diseñada para ofrecer funciones de seguridad basadas en hardware. TPM aporta ventajas de seguridad y privacidad para el hardware del sistema, los propietarios de la plataforma y los usuarios. Windows Hello, BitLocker, System Guard (antes denominado Windows Defender System Guard) y otras funciones de Windows se basan en TPM para funcionalidades como la generación de claves, el almacenamiento seguro, el cifrado, las medidas de integridad de arranque y las certificaciones.

Seguridad de Windows 11





Sistema operativo

Seguridad del sistema

Trusted Boot (Secure Boot y Measured Boot) Windows 11 requiere que todos los PC utilicen la función Secure Boot de Unified Extensible Firmware Interface (UEFI). Cuando se inicia un dispositivo con Windows 11, Secure Boot y Trusted Boot funcionan en combinación para evitar que se cargue malware y componentes dañados.

Cifrado y protección de datos

El **cifrado de unidad BitLocker** es una función de protección de datos que se integra con el sistema operativo y se ocupa de las amenazas de robo de datos o la exposición de datos que se crea tras el robo, pérdida o baja inadecuada de los equipos.

Secured-core PC

Microsoft ha trabajado con Dell para ofrecer una categoría especial de dispositivos denominados Secured-core PC (SCPC). Los dispositivos se envían con medidas de protección adicionales habilitadas en la capa de firmware o en el núcleo del dispositivo en cuya base está Windows.

Seguridad de la red

Para reducir la superficie de ataque de una organización, la protección de red en Windows evita que los usuarios puedan acceder a direcciones IP peligrosas y a dominios que podrían alojar ataques por suplantación de identidad, puntos débiles y otro contenido malicioso. A través del uso de servicios basados en la reputación, la protección de red bloquea el acceso a dominios y direcciones IP potencialmente dañinos y de baja reputación.

Protección frente a amenazas y virus

Microsoft Defender SmartScreen Microsoft Defender SmartScreen protege frente a ataques por suplantación de identidad, y sitios web y aplicaciones de malware, así como de la descarga de archivos potencialmente maliciosos.

Seguridad de Windows 11

Aplicación

Smart App Control
Smart App Control evita que los usuarios ejecuten aplicaciones maliciosas en los dispositivos Windows, ya que bloquea aplicaciones que no son de confianza o están sin firmar. Smart App Control ofrece más protección que otras soluciones integradas del explorador al añadir otra capa de seguridad directamente entretejida en el núcleo del sistema operativo en el nivel de los procesos.

Aislamiento de aplicaciones
El aislamiento de aplicaciones Win32 es una nueva característica de seguridad de la versión preliminar pública que está diseñada para ser el estándar de aislamiento predeterminado en clientes Windows. Está integrado en AppContainer y ofrece diversas características de seguridad adicionales para ayudar a la plataforma de Windows a defenderse frente a ataques que aprovechan las vulnerabilidades en aplicaciones o bibliotecas de terceros.

Identidad

Implementación del inicio de sesión sin contraseña
Windows Hello permite el inicio de sesión sin contraseña mediante la verificación PIN o biométrica y ofrece asistencia integrada para la norma del sector referente a inicios sin contraseña FIDO2. Windows Hello para Empresas amplía las funciones de Windows Hello para poder integrarse con las cuentas de Active Directory y el Id. de Microsoft Entra. Ofrece acceso de inicio de sesión único para los recursos profesionales o académicos como OneDrive para la Empresa, el correo electrónico profesional y otras aplicaciones empresariales.

Protección de credenciales avanzada
Además de la adopción del inicio de sesión sin contraseña, las organizaciones pueden reforzar la seguridad para las credenciales de los usuarios y los dominios en Windows 11 con Credential Guard y Remote Credential Guard.

Transparencia y controles de la privacidad
Gracias a los iconos prominentes en la bandeja del sistema, los usuarios pueden ver cuándo se están utilizando recursos y aplicaciones como los micrófonos y la ubicación. Se presenta una descripción de la aplicación y su actividad en un sencillo mensaje de globo que aparece cuando pasa el cursor sobre un icono. Las aplicaciones también pueden utilizar API de Windows con el fin de respaldar la funcionalidad de silencio rápido.

Seguridad de Windows 11

Cloud

Id. de Microsoft Entra

El Id. de Microsoft Entra (anteriormente denominado Azure Active Directory) es una completa solución de administración de las identidades basada en la cloud que ayuda a habilitar el acceso seguro a las aplicaciones, redes y otros recursos; además, protege frente a amenazas.

Microsoft Intune

Microsoft Intune es una solución muy completa de administración de puntos finales que ayuda a proteger, implementar y administrar usuarios, aplicaciones y dispositivos. Intune combina tecnologías como Microsoft Configuration Manager y Windows Autopilot para hacer más sencillo el aprovisionamiento, la gestión de la configuración y las actualizaciones de software en toda la organización.

Microsoft Azure Attestation Service

La generación remota de certificados ayuda a garantizar que los dispositivos cumplen las directivas y funcionan en un entorno de confianza antes de poder acceder a los recursos. Microsoft Intune se integra con el servicio de certificación de Microsoft Azure para revisar el estado del dispositivo Windows en su integridad y conectar esta información con el acceso condicional del Id. de Microsoft Entra.

Dell, Microsoft e Intel invierten en la seguridad continuada tras el lanzamiento de la plataforma

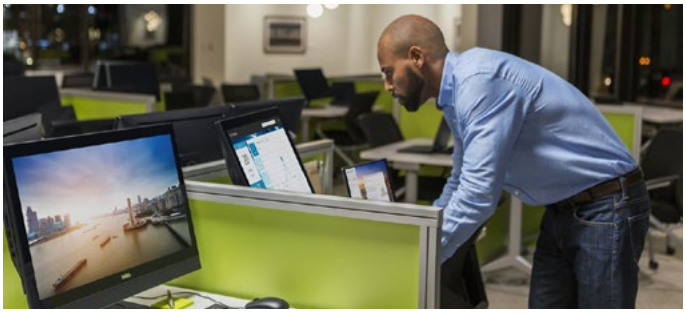
46 400 millones de USD

es nuestra inversión combinada en I+D en 2023*

* Macrotrends.net, gasto en I+D en 2023: Dell Technologies 2880 millones de USD, Intel 16 046 millones de USD, Microsoft 27 524 millones de USD

Dell e Intel han realizado inversiones significativas y continuadas para ayudar a garantizar la seguridad en todo el ciclo de vida de un producto. Una vez que un dispositivo o plataforma ha salido al mercado, los equipos de Dell e Intel siguen probando activamente sus productos en busca de vulnerabilidades. En el caso de Intel, este proceso incluye colaborar con investigadores y universidades para detectar los posibles puntos débiles antes de que lo hagan los agentes maliciosos; aplicar parches rápidamente a las vulnerabilidades que se encuentren; y, posteriormente, notificarlas tras reparar la brecha de seguridad.

Como parte de estas iniciativas, Intel financia un programa de recompensas por detección de errores que es uno de los mejores del sector y que representa el 86 % de las vulnerabilidades encontradas externamente en 2021. Las CVE (vulnerabilidades y exposiciones comunes) que se detecten a través de este programa y por investigadores internos o externos se registran en una base de datos pública. Como líder monitorización e informes de vulnerabilidades tras el lanzamiento, Intel ha registrado y corregido más vulnerabilidades potenciales que la mayoría de la competencia, y se sitúa por delante de otros fabricantes de chips que no alcanzan nuestro nivel de compromiso con la transparencia y la seguridad de los dispositivos.

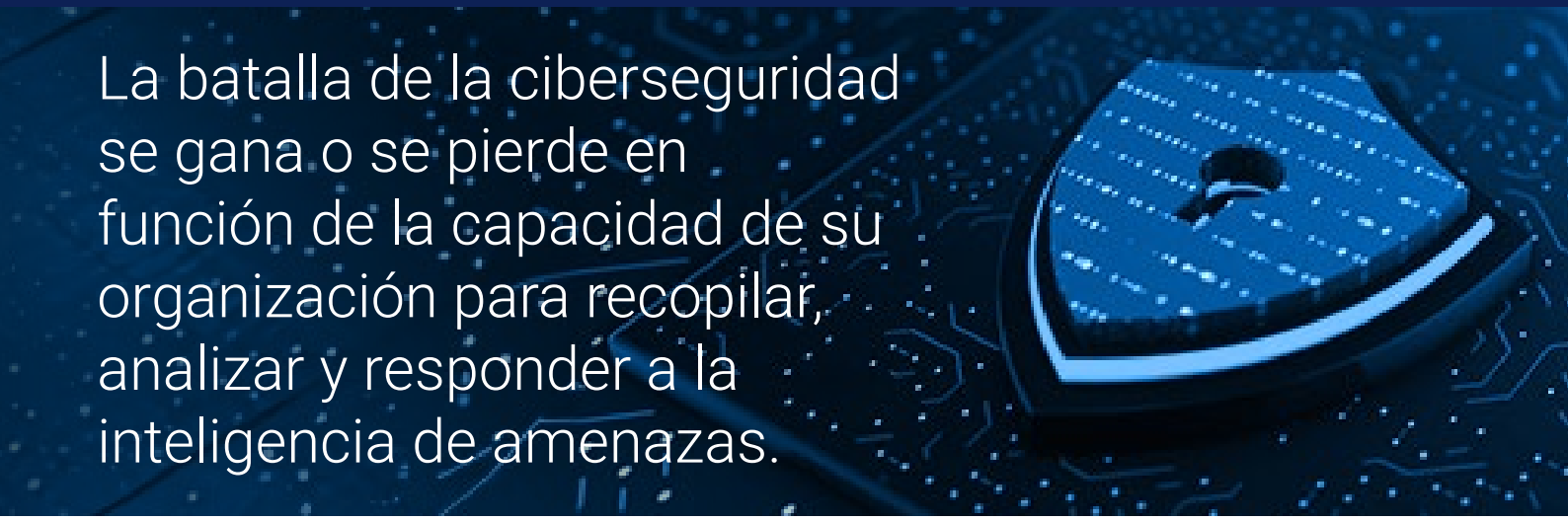


Para hacer frente a las CVE detectadas gracias a sus completos programas, Intel envía periódicamente actualizaciones de plataforma a todos los sistemas que se ejecutan en sus productos. Esta implementación es un proceso extenso que requiere la validación del ecosistema de socios de Intel, incluidos CSP, ISV, OEM/ODM y SI.

La coordinación de la divulgación y la respuesta a vulnerabilidades de los productos identificados las gestiona Dell y los equipos dedicados de respuesta ante incidentes de seguridad de los productos de Intel. Juntos, trabajan para ayudar a garantizar que las CVE se gestionen de forma rápida y segura, mitigando eficazmente los riesgos que puedan plantear.

Dell, Microsoft e Intel han efectuado estas inversiones para ofrecer una asistencia continuada a nuestros clientes y facilitar el trabajo a sus equipos informáticos. Hemos contratado investigadores, arquitectos de seguridad y analistas forenses de ciberseguridad para ayudar a proteger su empresa con el fin de permitir a sus equipos centrarse en equipar a los empleados para que hagan su trabajo lo mejor posible.

Dell, Microsoft e Intel tienen el compromiso de ayudarle a proteger su empresa en crecimiento



La batalla de la ciberseguridad se gana o se pierde en función de la capacidad de su organización para recopilar, analizar y responder a la inteligencia de amenazas.

Los atacantes de hoy en día son innovadores. En vista de que la mayoría de las soluciones de seguridad se dedican exclusivamente a proteger el software, están analizando las capas por debajo del SO y la cadena de suministro como nuevos vectores que ponen en peligro la seguridad y aprovechan los puntos débiles de empresas como la suya.

Para ir por delante de estos agentes maliciosos y garantizar la protección de las empresas, los líderes actuales deben pensar que las tecnologías de seguridad a nivel de hardware, estrechamente integradas en el chip, son cruciales a la hora de implementar dispositivos comerciales para sus empleados.

Dell e Intel llevan décadas colaborando en el ámbito de los dispositivos comerciales y se han ganado la confianza de los clientes con varios de los dispositivos comerciales más seguros del sector. Nuestros conocimientos y desarrollo en ingeniería conjuntos nos permiten ir por delante de los hackers gracias a la investigación, diligencia e innovación continuadas. Como líderes del panorama de los dispositivos comerciales durante décadas, podemos identificar y detener más amenazas, y actuamos constantemente sobre un enorme conjunto de datos y telemetría para ayudar a habilitar y mejorar continuamente la seguridad de los dispositivos comerciales de nuestros clientes conjuntos. Nuestros líderes de pensamiento se reúnen regularmente para hablar sobre los aspectos de la seguridad integral actual, cómo se perfilará en el futuro y las inversiones necesarias para garantizar que nuestros productos permanezcan a la vanguardia de la ciberseguridad comercial.

Con una seguridad de la cadena de suministro de primer nivel, las protecciones basadas en hardware, el software para la protección frente a amenazas avanzadas y la asistencia continuada, Dell e Intel están preparadas para ofrecerle tanto a usted como a su empresa dispositivos comerciales que además de cumplir su cometido, están diseñados para ayudar a conservar los datos de su negocio fuera de la web oscura. Hable con su representante de ventas de Dell hoy mismo para obtener más información sobre nuestros programas de dispositivos comerciales y saber cómo podemos ayudarle a alcanzar sus objetivos de negocio.

Haga clic aquí para

No renunciar a nada

DELL Technologies

Windows 11

intel.