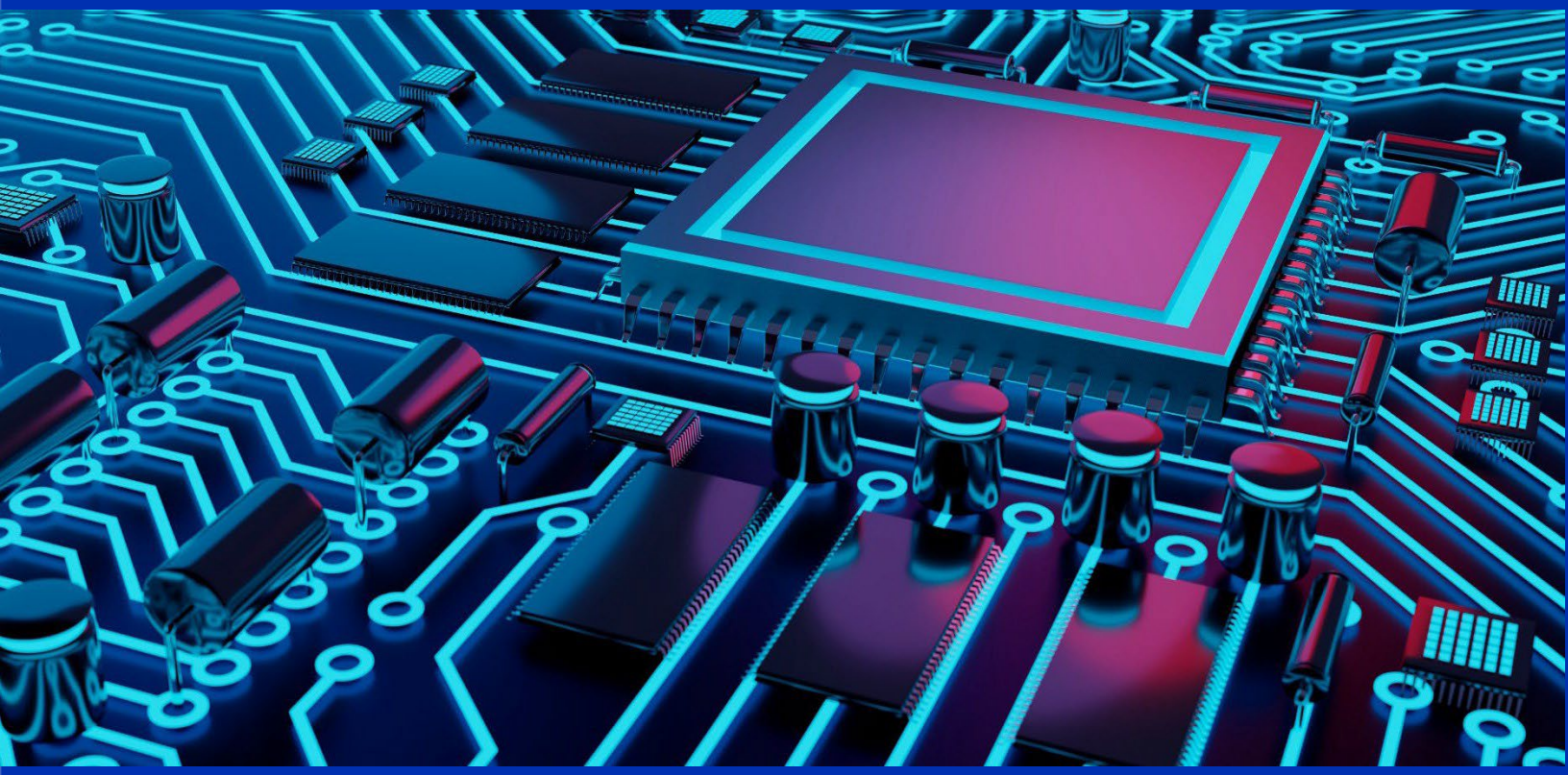
DELL Technologies intel

Lograr una seguridad ubicua por encima y por debajo del SO

Los PC comerciales con IA más seguros del mundo*, ofrecidos por Dell e Intel®. Prepare su parque informático para el futuro y manténgase un paso por delante de los ciberadversarios con múltiples capas de defensa.

Julio de 2025



Resumen ejecutivo

- Mantener la seguridad de los datos del negocio es una tarea complicada por la proliferación de terminales que funcionan fuera de la red de la organización y la evolución constante de los vectores de amenaza.
- La IA ha llegado a los dispositivos, ampliando tanto la innovación como la superficie de ataque. Con cientos de modelos y funciones de IA en circulación, los datos confidenciales están ahora más expuestos ante aplicaciones como la IA generativa.
- Dell e Intel se comprometen a proteger las redes de los clientes comerciales mediante múltiples capas de defensa.
- Dell combina la seguridad integrada en hardware y firmware con las protecciones basadas en silicio de Intel, para defender los niveles más profundos del dispositivo frente a ataques estructurales.
- Reforzamos estas defensas "por debajo del SO" con software inteligente proveniente de nuestro ecosistema de socios para ofrecer protección avanzada contra amenazas.
- Además de este enfoque, Dell e Intel han invertido en prácticas y políticas para ayudar a proteger de manera continua las plataformas una vez que salen al mercado y son susceptibles de ser atacadas por agentes maliciosos.

Temas tratados en este informe

Pilares de la seguridad

Ciclo de vida de desarrollo seguro Dell e Intel diseñan sus productos con la seguridad como elemento principal y los prueban rigurosamente antes de su lanzamiento.

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.

Marco de defensa integral

Seguridad integrada: los rigurosos controles de la cadena de suministro y la opción de validación adicional contribuyen a que los clientes estén protegidos desde el primer arranque.

Seguridad integrada:

- Las capacidades de seguridad basadas en hardware y firmware ayudan a proteger los dispositivos frente a amenazas dirigidas a sus capas fundamentales, como el BIOS.
- Las protecciones basadas en silicio proporcionan una capa esencial que respalda la fiabilidad y la confianza de la gama AI PC.

Seguridad integrada: la seguridad basada en software ofrece protección avanzada para puntos finales, redes y entornos de cloud, lo que resulta crucial para la seguridad moderna de los dispositivos.

Asistencia continua: Dell e Intel trabajan para garantizar que sus productos permanezcan seguros, solucionar vulnerabilidades y actualizar la seguridad a nivel de silicio en el SO.

Tendencias clave en seguridad

1. En su artículo Endpoint Security Market Insights de marzo de 2025, Forrester Research, Inc. explica que "los puntos finales [...] se encuentran entre los principales objetivos de ataques externos para empresas que han experimentado una vulneración en los últimos 12 meses".

2. Según el Informe global de amenazas de CrowdStrike 2025, los ataques de malware sin archivos representan actualmente el 79 % de los ataques, lo que implica que los ataques en memoria son más difíciles de detectar.

3. Según un informe de investigación de Enterprise Strategy Group de mayo de 2023, más del 75 % de las organizaciones afirman haber sufrido al menos un ciberataque provocado por un punto final desconocido, no gestionado o mal gestionado.

Introducción

Su red es tan segura como su punto final más vulnerable

La seguridad comienza mucho antes de lo que imagina. Da la impresión de que, cada pocos meses, otra marca de renombre global sufre una vulneración de la seguridad importante y el escarnio público resultante daña gravemente su reputación. Un daño suficiente para que los propietarios de las empresas y los profesionales de la seguridad estén justamente preocupados de correr la misma suerte, ya sea a través de una vulnerabilidad pasada por alto incorporada en sus dispositivos, o un punto débil desconocido y explotable en su software. Es posible que pueda confiar en su equipo de TI para proteger sus redes e implementar prácticas seguras de datos, pero ¿cómo puede confiar en todos los terminales y las aplicaciones en los que confía para hacer negocios cuando no ha supervisado ningún aspecto de su fabricación o desarrollo?

No basta con una seguridad basada únicamente en software. 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 líderes empresariales comprendan las limitaciones de esta estrategia: al confiar solo en el software para proteger sus empresas, dejan a merced de posibles ataques el hardware en el que se ejecuta el 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 directos al consumidor a menudo falla cuando se aplica en un entorno comercial que representa un objetivo más atractivo para los atacantes. Por eso Dell e Intel adoptan un enfoque diferente e integral de la seguridad. Dell e Intel saben que la única forma de proteger de forma fiable los dispositivos y las redes comerciales es mediante una armonización de las tecnologías de seguridad de hardware y software trabajando de forma concertada. 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.

Seguridad basada en hardware para PC comerciales con IA

Todos los PC serán AI PC. Según el analista del mercado tecnológico Canalys, los PC con IA dominarán todo el mercado de PC en los próximos seis años. Esto significa que los PC sin capacidades de IA integradas dejarán de venderse en 2030. En resumen, si quiere preparar su empresa para el futuro, debe empezar ahora. La buena noticia es que Dell e Intel están ayudando a los clientes a adaptarse al cambiante panorama de TI y seguridad con PC comerciales con IA que incorporan las funciones de seguridad, velocidad y eficiencia esenciales para hacer frente a las amenazas modernas.

Pero no es una tarea sencilla. La complejidad y consideraciones que conlleva la protección de los dispositivos y las redes son un quebradero de cabeza, y las tecnologías emergentes de IA han hecho que este terreno sea aún más difícil de gestionar. Por eso nos hemos asignado la misión de proporcionar a nuestros clientes dispositivos diseñados teniendo en cuenta la seguridad para permitirles centrarse en lo que realmente importa: hacer que sus negocios funcionen. La relación de coingeniería entre Dell e Intel abarca varias décadas y siempre se ha centrado en mantener la seguridad de los datos de nuestros clientes, especialmente en el mercado de Business-to-Business (B2B). A través de su colaboración con Intel, Dell ha consolidado su reputación como proveedor de referencia de dispositivos destinados a empleados para empresas de todos los tamaños y en todos los mercados. ¿Qué incluye un dispositivo comercial con IA de Dell? Es mucho más que una colección aleatoria de funciones y características: Intel y Dell entretejen sus tecnologías, herramientas y políticas a lo largo de todo el ciclo de vida de los PC comerciales para ayudar a proporcionar seguridad integral para nuestros clientes y sus negocios.

Seguro por diseño

Intel y Dell miran más allá de las amenazas actuales al diseñar 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

Empleamos seguridad basada en hardware a través de Dell Trusted Devices y las capacidades de seguridad de Intel vPro® para reforzar los dispositivos frente a los principales casos de uso en ciberseguridad: prevención, detección, respuesta, recuperación y corrección. Además, Dell e Intel cuentan con equipos de seguridad dedicados a probar sus productos con el fin de localizar nuevas vulnerabilidades antes de que lo hagan los atacantes, y desplegar parches con rapidez para ayudarle a usted y a su equipo a protegerse.

En este documento técnico, exploraremos cómo Dell e Intel han colaborado para producir plataformas de PC con IA comerciales, con la seguridad incorporada desde los niveles más profundos para ayudar a proteger los dispositivos durante todo el ciclo de vida, durante su próxima actualización y más allá.

Ciberseguridad e IA generativa: un arma de doble filo

Así como los ciberdefensores utilizan la IA generativa con fines legítimos, los ciberatacantes la emplean para impulsar sus propios objetivos malintencionados, lanzando ataques más sofisticados, más rápido y a mayor escala.

Aunque los casos de uso de la IA generativa aún están en una fase inicial y se expanden a diario, es importante tener en cuenta algunos conceptos clave. En primer lugar, la IA generativa conlleva una serie de amenazas para las organizaciones, como:

- Problemas de integridad y privacidad de datos.
- Problemas de cumplimiento normativo.
- Infracción de la propiedad intelectual.

Además, identificamos varias formas en que la IA generativa podrá contribuir en la lucha por la seguridad, entre ellas:

- Detección de amenazas avanzadas
- Formación especializada y dirigida para empleados
- Automatización

Dell e Intel trabajan activamente para ofrecer un mejor modelado de amenazas específico para la IA generativa. Este puede incluir aspectos como la prevención de pérdida de datos, la gestión de derechos de datos, el phishing avanzado, la manipulación de modelos, la regulación y el cumplimiento normativo, todo ello con los controles adecuados aplicados.

Dell también puede ayudarle a evaluar su panorama de IA generativa en materia de seguridad, mediante programas de gestión de vulnerabilidades y pruebas de penetración que le permitan mantenerse al día con el cambiante panorama de amenazas.

Pilares de la seguridad

Ciclo de vida de desarrollo seguro

La protección de nuestras plataformas comienza en la pizarra blanca

Planificación, evaluación y análisis

Antes de diseñar sus últimas plataformas y conjuntos de chips, respectivamente, los expertos de Dell e Intel establecen parámetros estrictos para determinar lo que necesita incluir una plataforma segura para satisfacer las necesidades de seguridad del futuro y cumplir con las normativas de seguridad necesarias. Este proceso comienza con una mesa redonda para determinar los riesgos futuros de seguridad y privacidad, así como las actividades 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 e Intel desarrollan modelos de amenazas enfrentándose a esta arquitectura conceptual con una mentalidad de adversario y analizando posibles vulnerabilidades de seguridad y puntos débiles que deben mitigarse. 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 va por el buen camino para satisfacer las necesidades de los clientes.

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 utiliza herramientas especiales para buscar y reparar defectos. Algunos productos con código más complicado requieren un proceso de revisión manual, donde los expertos en seguridad revisan el código de producto línea por línea para encontrar errores desconocidos y garantizar que el desarrollo se efectuó de forma segura. Por último, se encarga a equipos de hackers expertos que acometan pruebas de penetración y otras actividades de equipo rojo 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 identificada adicional quede documentada y corregida.

Lanzamiento y seguimiento posterior

Una vez probado y verificado que el producto cumple o supera rigurosamente los objetivos de seguridad definidos al principio, está 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 del compromiso de Dell e Intel con la seguridad integral es su inversión en una cadena de suministro segura entre el montaje y la entrega de un dispositivo, uno de los vectores de ataque de más rápido crecimiento para agentes maliciosos. En la sección siguiente, profundizaremos en cómo Dell e Intel moderan los riesgos en sus cadenas de suministro para ayudar a garantizar que el dispositivo que usted recibe a la puerta de su empresa esté seguro desde el primer arranque.

Seguridad de la cadena de suministro

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

Entre el momento en que un componente o dispositivo sale de fábrica y aquel en que llega a su destino, pueden suceder muchas cosas. Cada fase de la cadena de suministro representa un nuevo vector que deja a sus empleados, su negocio y sus 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 implementarlos entre el personal.

Source
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 rutinariamente a auditorías para garantizar el cumplimiento normativo del conjunto completo de estándares de seguridad de la cadena de suministro de Dell.

Haga de
Además de cumplir los estándares de seguridad de la cadena de suministros de Dell, los fabricantes de dispositivos Dell también prueban con frecuencia 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 para garantizar que el cliente reciba exactamente lo que se haya enviado.

Entregar
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 alojados en el interior se han manipulado durante el transporte.

Los propios dispositivos Dell también cuentan con tecnologías de detección de manipulaciones. Las soluciones Dell SafeSupply Chain abarcan los controles de integridad y seguridad en la cadena de suministro, como precintos antimanipulación y borrados de disco duro con estándares NIST, para garantizar un inicio limpio y seguro de cara a su imagen corporativa.

Verificar
Los dispositivos comerciales con IA de Dell se envían con certificados de plataforma firmados criptográficamente, que capturan instantáneas de los atributos de la plataforma durante la fabricación, el montaje, las pruebas y la integración. A continuación, estos atributos de plataforma se vinculan criptográficamente al dispositivo específico mediante Trusted Platform Module (TPM) como fuente de confianza en el hardware.

Obtenga más información sobre el esfuerzo conjunto de Dell e Intel para proteger la cadena de suministro. Vea la entrevista ***con SiliconANGLE***

Dell ha implementado certificados de plataforma Trusted Computing Group (TCG) en la solución Dell Secured Component Verification (SCV) para PC comerciales con IA y procesadores Intel. El certificado está disponible tanto en el dispositivo para las organizaciones federales como en la cloud para clientes comerciales. SCV entrega a TI certificados de inventario firmados criptográficamente para dispositivos Dell compatibles. Con herramientas de autoverificación seguras, el SCV único de Dell* ayuda a garantizar la integridad del hardware durante el transporte hasta los entornos informáticos y permite a los clientes verificar que los PC comerciales con IA y los componentes clave de Dell llegan exactamente como se han pedido y fabricado.

Marco de defensa integral

Seguridad por debajo del SO

Las tecnologías de seguridad integradas ayudan a prevenir, detectar, responder y recuperarse ante amenazas

La seguridad integral implica ir más allá del modelo heredado de software que protege el software para mantenerse al día con las nuevas categorías de amenazas contra la seguridad y la privacidad digitales. 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 ingeniería conjunta entre Dell e Intel se ha centrado en cubrir esta superficie de ataque con un tapiz intrincado de tecnologías a nivel tanto de componente como de plataforma.

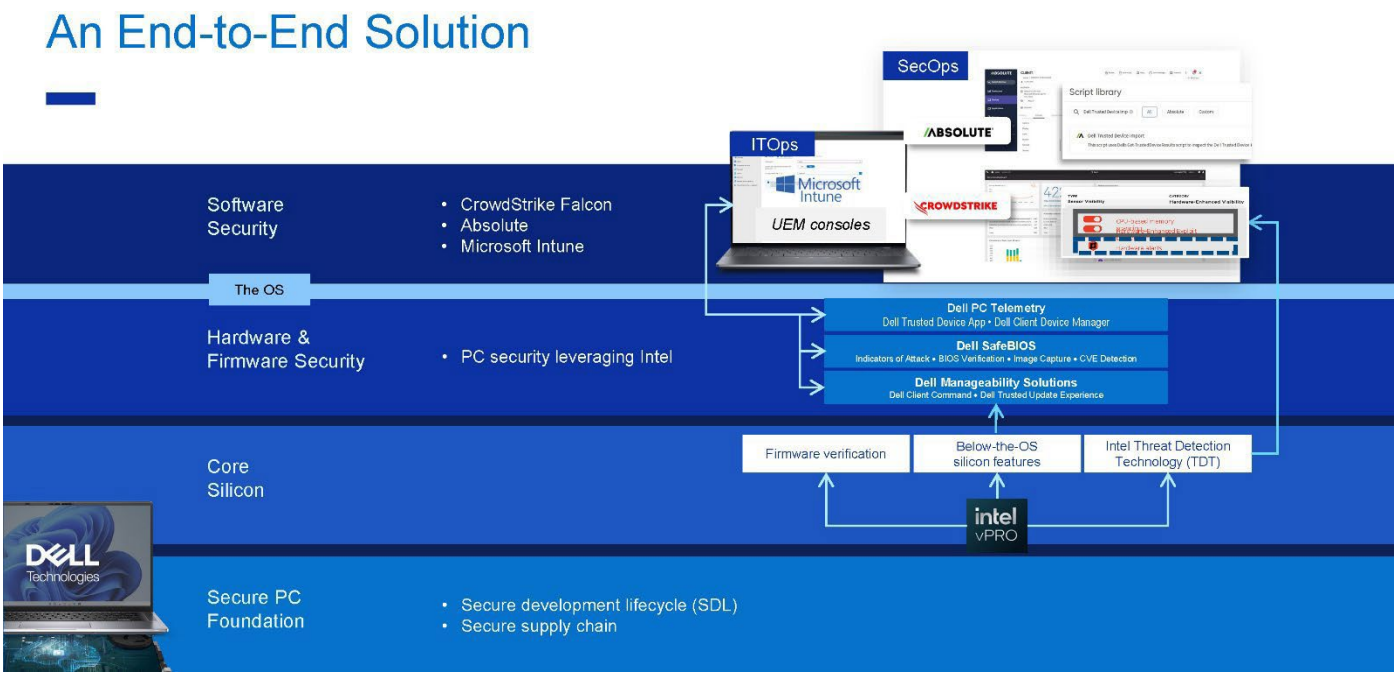


Figura 1: En la actualidad, una seguridad eficaz requiere múltiples capas de contramedidas frente a ataques. Dell e Intel colaboran con socios de software para ofrecer una defensa en profundidad.

Hemos abordado la cadena de suministro y los cimientos seguros de la gama AI PC que ofrecen Dell e Intel. Ahora, veamos las capas intermedias.

Seguridad Intel vPro®

Intel vPro Security 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. Este conjunto de tecnologías de seguridad contribuye a proteger frente a amenazas modernas en todas las capas: hardware, BIOS/firmware, hipervisor, máquinas virtuales, sistemas operativos y aplicaciones.

Seguridad integrada de hardware y firmware de Dell

La protección del sistema básico de entrada y salida (BIOS) es crucial 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 crítica, los dispositivos comerciales con IA de Dell incluyen SafeBIOS, un conjunto de medidas de seguridad por capas a nivel del firmware. Las capacidades que sustentan SafeBIOS refuerzan la protección, la detección y la recuperación a nivel de BIOS.

Figura 2: Según Principled Technologies, Dell e Intel ofrecen los PC comerciales con IA más seguros del mundo.*

También es importante tener en cuenta que la seguridad efectiva incluye visibilidad sobre el estado de seguridad actual. Dell hace visibles estos eventos a nivel inferior al sistema operativo mediante SafeBIOS, para que administradores y usuarios finales puedan visualizarlos y tomar decisiones a través de la aplicación Dell Trusted Device (aplicación DTD). La aplicación DTD detecta si el BIOS se ha visto comprometido al comparar la imagen activa del BIOS con la copia de referencia almacenada en el entorno de Dell: una verificación del BIOS fuera del host que nos diferencia en el mercado. Además, la verificación del firmware del motor de gestión (ME) de Intel, disponible exclusivamente en PC comerciales de Dell, protege frente al acceso no autorizado y la manipulación del firmware altamente privilegiado.

Esta telemetría exclusiva de los PC de Dell, disponible a través de Dell Client Device Manager (DCDM) en entornos de TI gestionados o mediante la consola de la aplicación DTD en entornos no gestionados, es el ingrediente clave en la ecuación de seguridad. Esta telemetría permite integrarse con consolas de terceros como CrowdStrike y Absolute (para seguridad), y Microsoft Intune (para gestión) (véase la Figura 1). De hecho, Dell es el único fabricante de PC que ofrece integración y visibilidad de amenazas a nivel de firmware a través de consolas de seguridad de terceros*

Dell también mitiga el riesgo creciente de suplantación de identidad y de acceso no autorizado a cargas de trabajo confidenciales. Algunos dispositivos comerciales de Dell incluyen Dell SafeID con ControlVault 3+, un exclusivo chip de seguridad certificado FIPS 140-3 de nivel 3*, que almacena las credenciales de los usuarios finales y las aísla del sistema operativo, lo que reduce considerablemente su vulnerabilidad frente a ataques.

La seguridad por debajo del SO es solo una parte del enfoque integral que Dell adopta para proteger los dispositivos.

Para reforzar la protección de los dispositivos comerciales con IA de Dell, Dell e Intel también han invertido considerablemente en verificar y seleccionar un ecosistema de soluciones de seguridad de software líderes en el sector. Estas capacidades protegen los dispositivos frente a amenazas avanzadas procedentes de atacantes sofisticados, al ofrecer un nivel de seguridad adicional en la capa de datos y de aplicaciones.

Una vez más, Dell e Intel pueden potenciar las tecnologías de software mediante la telemetría de PC por debajo del SO para mejorar la detección y respuesta ante amenazas.

Seguridad por encima del SO

La seguridad integrada en el software proporciona protección avanzada frente a amenazas.

El potencial beneficio de una única brecha exitosa basta para que los ciberatacantes, altamente motivados, realicen decenas de intentos durante toda la vida útil de un dispositivo. Si se multiplica por todo el parque informático de una organización, es un serio motivo de preocupación. ¿Se imagina que un ataque logra eludir las defensas? A estas alturas, está claro que ninguna solución puede bloquear el 100 % de los ataques. Esto incluye los puntos finales de su parque informático, así como las redes y los entornos de cloud en los que operan. Las soluciones de software inteligentes ayudan a prevenir, detectar, responder y recuperarse frente a amenazas, sin importar dónde se produzcan. Por eso, la cartera de seguridad para puntos finales de Dell Trusted Workspace incluye software líder en el sector para simplificar las adquisiciones y ofrecer a los líderes empresariales todo lo necesario para proteger sus dispositivos. Las prestaciones incluyen:

- Prevención, detección, respuesta y corrección en entornos de puntos finales, redes y cloud, con tecnologías basadas en IA y aprendizaje automático
- Geolocalización de puntos finales, geoperimetraje, borrado remoto de datos y autorreparación para aplicaciones críticas, tanto dentro como fuera de la red
- Soluciones Security Service Edge para un enfoque de seguridad y acceso a la cloud centrado en los datos, que protege tanto la información como a los usuarios en cualquier lugar

Las capacidades de seguridad de Intel, integradas en la parte más interna del chip, como la tecnología Intel Control-flow Enforcement, protegen contra ataques dirigidos al SO, mientras que otras capacidades de seguridad de Intel vPro® protegen por debajo del SO, aportan seguridad a las aplicaciones y los datos, y brindan protección contra amenazas avanzadas.

Seguridad asistida por hardware

Seguridad integrada

Los atacantes se centran cada vez más en la pila informática de la organización, que tradicionalmente ha carecido de visibilidad y control. Estas amenazas en constante evolución están burlando las herramientas de seguridad heredadas de detección y respuesta en los puntos finales (EDR), lo que hace que la seguridad de los PC sea más crítica que nunca. Para adelantarse a las amenazas modernas y de rápida evolución, se requiere una colaboración profunda en el ecosistema que conecte adecuadamente las protecciones frente a superficies de ataque entre distintos proveedores en una solución cohesionada.

Sin embargo, ese trabajo de integración en el back-end es complejo y requiere mucho tiempo y recursos. Para resolverlo, Dell e Intel han aprovechado su profundo conocimiento de los puntos débiles del adversario y del cliente para colaborar con socios en el desarrollo de una solución integrada de hardware y software denominada "seguridad asistida por hardware". Además de ofrecer la gama AI PC segura y recurrir a los principales socios de software del sector, Dell ofrece una telemetría* de dispositivos única que enriquece todo el ecosistema de seguridad, para aportar una mayor visibilidad a nivel del BIOS a todo el parque informático. Esta capacidad de integración es crucial para cerrar la brecha de seguridad de TI a la que tantas organizaciones se enfrentan hoy en día. Con Dell, Intel y nuestro ecosistema de socios, el hardware y el software se comunican entre sí, lo que mejora la seguridad y la capacidad de gestión en todo el parque informático.

Figura 3: Las nuevas ciberamenazas sortean las defensas basadas solo en software. Reduzca la superficie de ataque de los puntos finales a través de medidas de protección asistidas por hardware.

Descubra la seguridad asistida por hardware con Dell, Intel y CrowdStrike

Dell, Intel y CrowdStrike han desarrollado de forma conjunta funciones de detección y respuesta ante amenazas que combinan la potencia de los Dell Trusted Devices, los PC comerciales con IA más seguros del mundo*, con las capacidades de silicio de Intel y la posición destacada de CrowdStrike en el informe Gartner Magic Quadrant, 2024. La solución conjunta de CrowdStrike, Dell e Intel replantea la seguridad de los puntos finales para su empresa, y va más allá de las protecciones basadas en software al incorporar seguridad asistida por hardware.

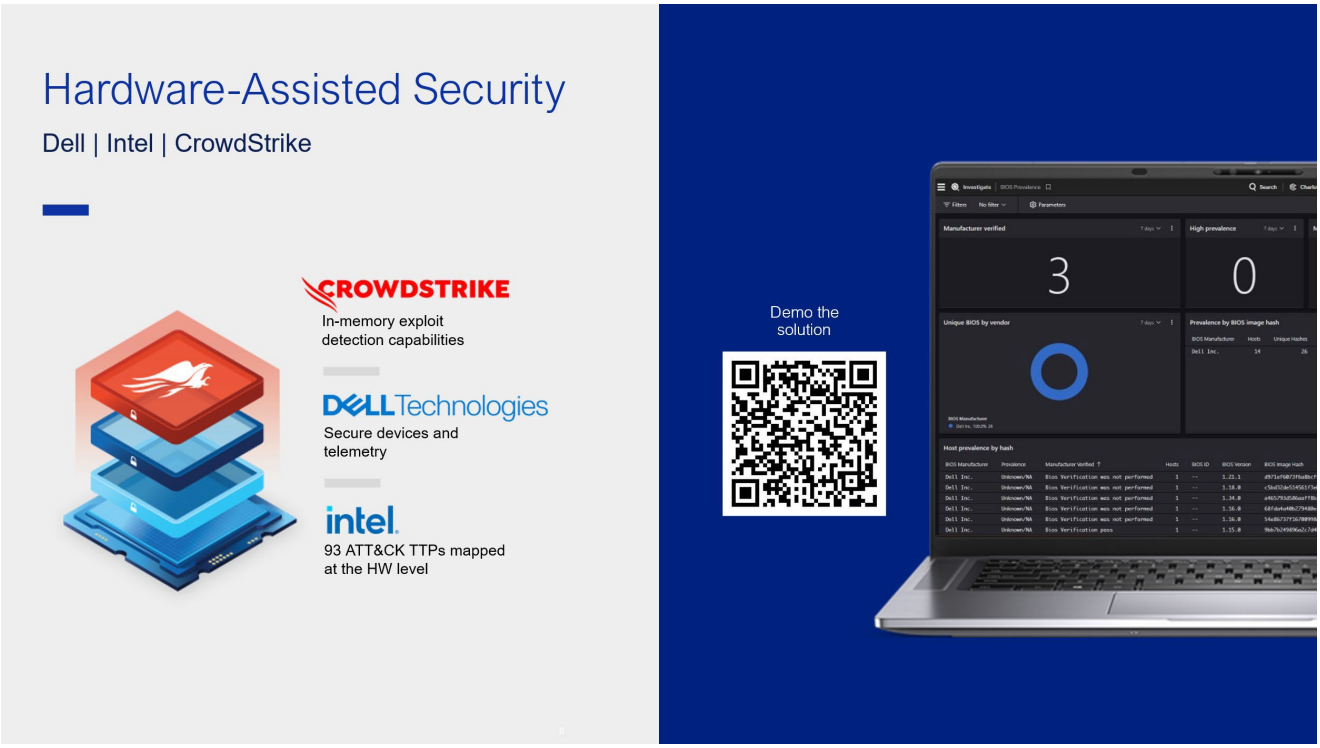


Figura 4: Seguridad multicapa en los PC comerciales con IA de Dell, integrada con CrowdStrike e Intel.

Valor añadido de la integración de Intel y CrowdStrike en los PC con IA de Dell

Avance en la seguridad de los puntos finales gracias a la aceleración por IA/GPU/NPU: las ciberamenazas son cada vez más sofisticadas, y los PC con IA están diseñados para anticiparse a ellas mediante IA integrada en el dispositivo, lo que ofrece una detección más rápida y en tiempo real, y también reduce la dependencia de los servicios de cloud. Herramientas como las de CrowdStrike pueden descargar la detección de malware en unidades de procesamiento neuronal (NPU) integradas, lo que permite identificar amenazas más rápido con un impacto mínimo en el rendimiento de la CPU. Gracias al procesamiento local de datos y a las avanzadas capacidades antiphising de los PC con IA basados en Intel, la información confidencial permanece protegida y se reduce la exposición a riesgos externos.

Algunos ejemplos del trabajo conjunto entre Intel y CrowdStrike (actualmente en fase de prueba de concepto, pero que estará disponible públicamente en los próximos meses) para reforzar la seguridad de los puntos finales mediante la aceleración por IA y NPU:

- Detección mejorada de exploits mediante hardware (HEED): utiliza la telemetría de CPU de Intel para rastrear el flujo de control de las aplicaciones y detectar ataques dirigidos a la memoria.
- Análisis acelerado de memoria (AMS): usa la tecnología Intel Threat Detection para derivar el análisis intensivo de memoria a la GPU integrada de Intel, lo que permite multiplicar por siete la capacidad de análisis.

Con estas dos funciones, Intel desempeña un papel clave al proporcionar indicadores de ataque basados en IA a los puntos finales y a la cloud de seguridad de CrowdStrike. Estas capacidades también aportan una nueva perspectiva sobre la capa de memoria, lo que permite a CrowdStrike desarrollar nuevos modelos de detección para el futuro y reforzar la seguridad con el tiempo.

Defensa de AI PC validada por el sector: los nuevos estudios de MITRE demuestran que la elección del hardware del PC desempeña un papel clave a la hora de habilitar el software de seguridad y las funciones del sistema operativo para proteger los activos de forma eficaz.

Los equipos de operaciones de seguridad (SecOps) despliegan agentes potentes en los parques informáticos de PC para inspeccionar cada proceso en busca de señales de malware. Los proveedores de software de seguridad han asignado sus capacidades a la infraestructura MITRE ATT&CK para mostrar dónde proporcionan soluciones. Los proveedores de seguridad gestionada ayudan a las empresas a clasificar las alertas diarias mediante herramientas como XDR, SIEM y asistentes de seguridad. Bastante sofisticado, sí. Pero la aplicación de la seguridad basada en hardware en los PC que ya posee frente a ataques reales había sido todo un misterio… hasta ahora.

A finales de 2024, el Center for Informed Defense* (CTID) de MITRE colaboró con más de treinta expertos de Intel, Microsoft, CrowdStrike y ATTACK IQ para identificar y clasificar la relevancia de las funciones de seguridad optimizadas por hardware frente a las tácticas y sub-técnicas del marco MITRE ATT&CK. En conjunto, el grupo analizó las funciones de seguridad de Intel vPro® en relación con 150 tácticas de amenaza, tanto acumuladas como únicas, incluyendo (sub)técnicas y (sub)procedimientos (TTP), para identificar en qué casos el hardware del PC puede ofrecer protecciones listas para usar mediante software de seguridad optimizado.

Para validar las pruebas de mapeo y emulación, MITRE utilizó un equipo Dell Pro con procesador Intel Core Ultra, que incluía el conjunto completo de protecciones de seguridad Intel vPro habilitadas sobre una pila típica de software de seguridad empresarial. Esto complementa las defensas exclusivas de Dell integradas por debajo del SO.

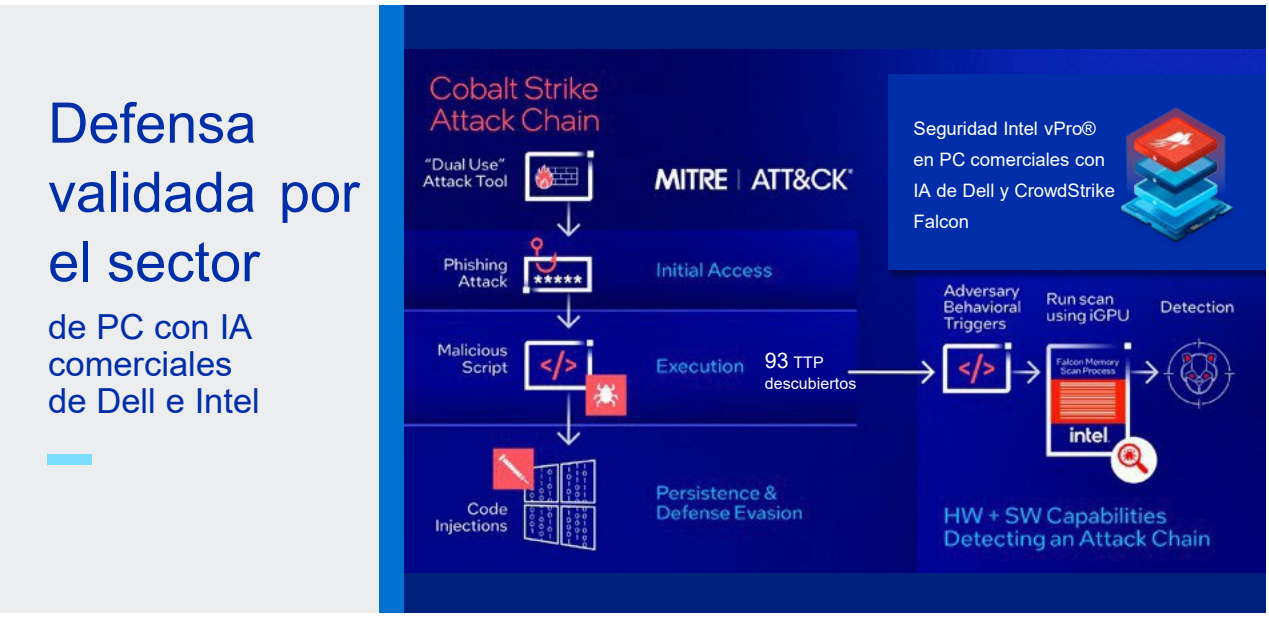


Figura 5: La seguridad asistida por hardware funciona.

En el escenario de ejemplo (cadena de ataque de Cobalt Strike), se muestra un ataque sin archivos de Cobalt Strike que afecta a la memoria, y cómo CrowdStrike Falcon contribuye a mitigarlo mediante el uso de hardware. Como se mencionó anteriormente, los ataques de malware sin archivos han cobrado fuerza entre los adversarios. Casi el 75 % de todos los tipos de ataque abusan de procesos válidos del sistema, como la ejecución en memoria, lo que les permite eludir las defensas EDR tradicionales. Este es un claro ejemplo de cómo el hardware del PC aporta la potencia de cálculo incremental necesaria para escanear la memoria sin afectar a la experiencia informática del usuario. **CrowdStrike utiliza algoritmos de escaneo acelerado de memoria de la tecnología Intel Threat Detection (Intel TDT) y aprovecha su capacidad para derivar el procesamiento al procesador gráfico integrado con tecnología de Gráficos Intel. Esto permite acelerar el rendimiento hasta 7 veces, garantizando una buena experiencia de usuario y, al mismo tiempo, ofreciendo una capacidad de escaneo más profunda, capaz de detectar más de 93 TTP.** (Nota: La capacidad de escaneo de memoria de CrowdStrike, integrada en su software, solo está disponible en PC con Intel vPro).

Conocer las medidas de seguridad basadas en software y hardware puede ayudar a las empresas a aprovechar todo el potencial de los PC con IA modernos. Los resultados demuestran que la elección del hardware del PC influye significativamente en la capacidad del software de seguridad y las funciones del sistema operativo para contrarrestar amenazas específicas y proteger los activos corporativos frente a ciberadversarios avanzados.

Las infraestructuras de seguridad por encima y por debajo del SO de Intel ofrecen un enfoque integral para proteger los dispositivos comerciales, pero, como expertos en seguridad, sabemos que ningún dispositivo está absolutamente seguro. Este es el motivo por el que somos líderes del sector en inversiones en seguridad posterior al lanzamiento para ayudar a garantizar que nuestros dispositivos permanezcan seguros años después de salir al mercado.

Asistencia permanente

Dell e Intel invierten en la seguridad continua de sus plataformas tras el lanzamiento

Dell e Intel han realizado inversiones significativas e ininterrumpidas 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 continúan sondeando activamente sus productos en busca de vulnerabilidades. En el caso de Intel, este proceso incluye trabajar con investigadores y universidades para detectar posibles explotaciones antes de que lo hagan los agentes maliciosos; aplicar parches rápidamente a las vulnerabilidades que se encuentren; y, a continuación, informar de ellas tras cerrar la brecha de seguridad.

La garantía proactiva de seguridad de productos incluye esfuerzos para detectar vulnerabilidades de forma interna, así como incentivos a la comunidad externa de investigadores en seguridad mediante programas de incentivos por la detección de errores (Bug Bounty). En 2024, la inversión de Intel en la garantía proactiva de la seguridad de los productos representó el 96 % de las vulnerabilidades detectadas y mitigadas. El 4 % restante de las vulnerabilidades tratadas por Intel no se remitieron a través del programa Intel Bug Bounty, sino que fueron reportadas por socios u otras organizaciones que no solicitan recompensas económicas. En todos los casos, Intel colaboró con los investigadores para coordinar la divulgación pública de estos problemas, de modo que las mitigaciones estuvieran disponibles para los clientes desde el mismo momento de la publicación.

Para hacer frente a las vulnerabilidades y exposiciones comunes (CVE) detectadas gracias a sus completos programas, Intel envía periódicamente actualizaciones de plataforma a todos los sistemas que se ejecutan en sus productos. Este proceso trimestral incluye actualizaciones de seguridad, funcionales y de características en el microcódigo, el firmware y el BIOS del sistema. Las actualizaciones periódicas permiten a los socios de Intel validar e integrar actualizaciones de hardware y firmware en sus plataformas siguiendo un calendario trimestral predecible, lo que facilita una divulgación pública coordinada en todo el ecosistema.

La coordinación de la divulgación y la respuesta a vulnerabilidades de productos identificadas corre a cargo de los equipos específicos de respuesta a incidentes de seguridad de productos de Dell e 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 e Intel han efectuado estas inversiones para proporcionar una asistencia continua a nuestros clientes y facilitar la tarea 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.

La inversión de Intel representa el 96 % de las vulnerabilidades atajadas en 2024

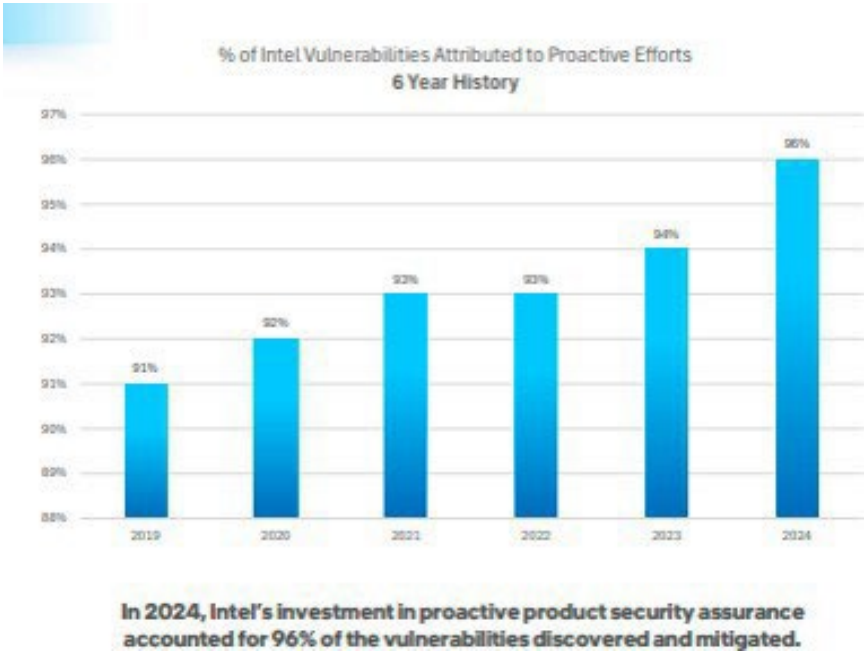
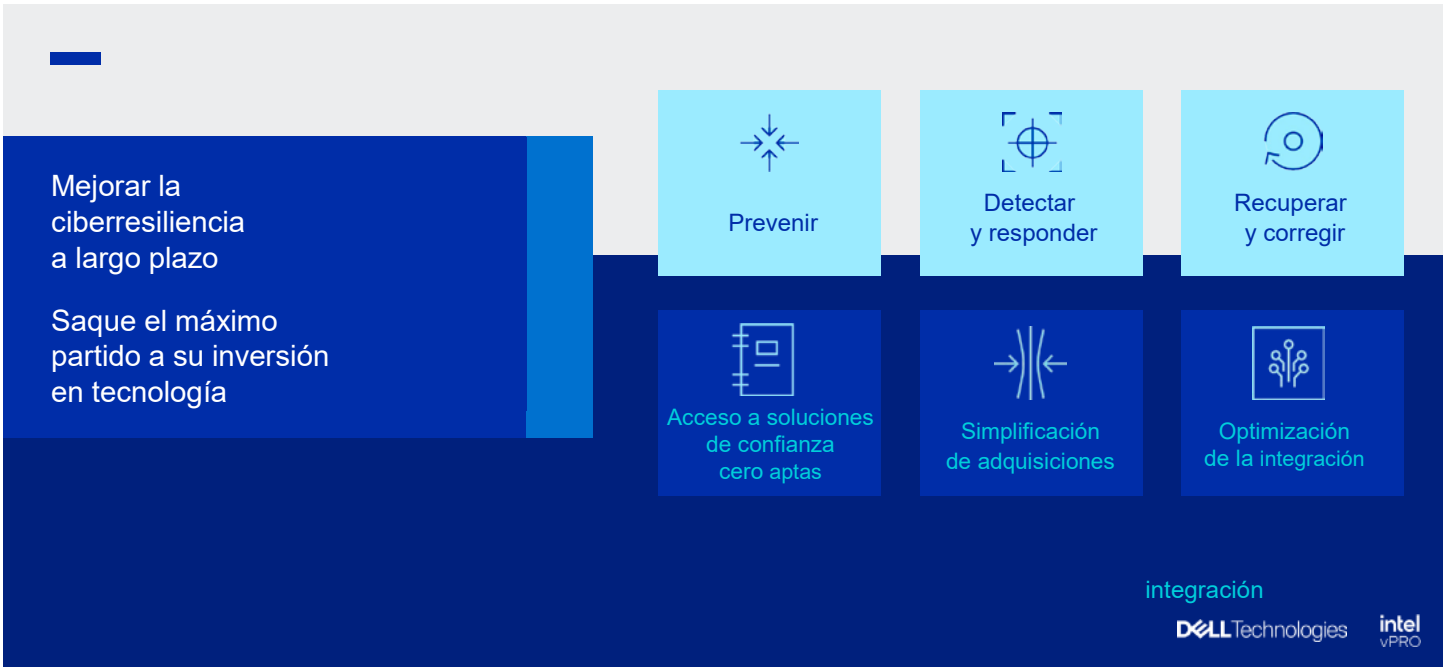


Figura 6: Porcentaje de vulnerabilidades de Intel atribuidas a esfuerzos proactivos (fuente: 2024 Intel Product Security Report)

Conclusión

Resultados de trabajar con Dell e Intel



Dell e Intel se centran en los resultados en materia de seguridad y desarrollan soluciones con un enfoque basado en la mentalidad del adversario. El objetivo final de los ciberadversarios es el dinero, que obtienen robando datos y vendiéndolos o exigiendo un rescate por ellos. Por lo tanto, aunque el método de entrada puede variar (el marco MITRE ATT&CK® identifica nueve métodos generales de acceso inicial), las cadenas de ataque cibernético siguen patrones similares: reconocimiento, acceso inicial (mediante la explotación de una vulnerabilidad [debilidad] o una exposición [error] que hayan detectado), infiltración en la red, movimiento lateral para obtener mayores privilegios, exploración y recopilación de información, y exfiltración de datos.

Podemos ayudarle a proteger cualquier carga de trabajo con productos, soluciones y servicios inteligentes diseñados con la mentalidad del adversario en mente. En lugar de intentar bloquear el 100 % de los ataques (algo imposible), dejamos el ego de lado, asumimos que un ataque es inevitable y desplegamos defensas por capas para el peor escenario posible. Priorizamos la visibilidad y la capacidad de respuesta en todo el parque informático de PC. Esto ayuda a nuestros clientes a adelantarse a los vectores de ataque emergentes.

Gracias a las soluciones de seguridad para endpoints de Dell e Intel, las organizaciones **logran resultados clave en materia de seguridad**:

- **Mejorar la ciberresiliencia a largo plazo**
- **Saque el máximo partido a su inversión en tecnología**

Conozca ambos casos de uso de ciberseguridad...:

- **Reduzca la superficie de ataque**: mitigue el riesgo de que un ataque pase desapercibido, minimice las vulnerabilidades y los puntos de entrada que se pueden explotar para comprometer el entorno.
- **Mejore la detección y respuesta ante amenazas**: identifique y aborde activamente posibles incidentes de seguridad y actividades malintencionadas mediante capas de defensa integradas que aceleran la detección y la respuesta.
- **Habilite la recuperación y la corrección**: recopile información sobre vulneración de datos para su análisis, protéjase frente a amenazas futuras y restaure los dispositivos a un estado seguro y operativo conocido tras un incidente de seguridad.

…y reduzca la carga operativa de la seguridad:

- Mantenga la confianza en los dispositivos y la identidad con **ofertas compatibles con el modelo de confianza cero**.
- **Simplifique las adquisiciones** mediante la consolidación de proveedores y el acceso al hardware, el software y los servicios en un mismo punto.
- Ahorre tiempo y recursos con una **integración optimizada**.

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. Sabemos que la mayoría de las soluciones de seguridad se centran únicamente en la capa del sistema operativo, por lo que los adversarios buscan superficies de ataque más vulnerables, como las capas inferiores al sistema operativo y la cadena de suministro. 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.

Descubra qué soluciones son más adecuadas para usted

PC comerciales con IA

PREGUNTE POR:

Seguridad de hardware y firmware • Seguridad en la cadena de suministro • Capacidad de gestión • Núcleo de chips y optimizaciones de IA

Software e integraciones

PREGUNTE POR:

Licencias disponibles para su compra con PC Dell • Licencias independientes • Integraciones de telemetría

Servicios

PREGUNTE POR:

Managed Detection & Response (MDR) • Recuperación ante incidentes

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, los servicios gestionados 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 mantener los datos de su empresa fuera de la web oscura.

*Los PC comerciales con IA más seguros: 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
sobre las soluciones Dell

Póngase en contacto
con un experto
de Dell Technologies

Ver más recursos

Participe
en la conversación

DELL Technologies

intel