DELL Technologies

Microsoft

Documento técnico

Obtenga una protección de seguridad avanzada con las funcionalidades combinadas de Windows Server 2022 y los servidores Dell EMC™ PowerEdge™ de última generación

Refuerce las cargas de trabajo esenciales para el negocio con un entorno de hardware, firmware y sistema operativo más seguro

Se espera que la ciberdelincuencia mundial suponga un coste total de 6 billones de dólares en 2021, y que esta cifra aumente hasta los 10,5 billones de dólares en 2025, según Cybersecurity Ventures.[1] Solo los ataques de ransomware se han multiplicado por 61 en seis años hasta alcanzar los 20 000 millones de dólares en 2021, y actualmente se produce un ataque cada 11 segundos.[1] Una encuesta de IDC de 2021 determinó que más de un tercio de las organizaciones encuestadas en todo el mundo habían sufrido un ataque o una vulneración de ransomware en los últimos 12 meses (y, a menudo, más de un incidente).[2] Aunque IBM estima que el coste de una sola vulneración de datos asciende actualmente a 4,24 millones de dólares,[3] el coste real puede ser mucho mayor: en algunos casos, los hospitales de Estados Unidos han tenido que derivar a los pacientes de urgencias a otros hospitales y rechazar ambulancias por ataques de ransomware.[4]

Los ataques de firmware pueden ser una amenaza particularmente perniciosa para las organizaciones. Esto se debe a que un ataque vectorizado en el firmware puede implantar malware que se ejecute antes que el sistema operativo (SO) y, por tanto, antes que el software de seguridad. Sin embargo, menos de la mitad de las organizaciones han tomado medidas para reforzar sus sistemas contra los ataques de firmware, a pesar de que dichos ataques se han vuelto cinco veces más frecuentes en los últimos cinco años.[5] Al fin y al cabo, las cargas de trabajo serán tan seguras como lo sean todos los componentes de la pila en la que se ejecuten.

Para hacer frente a este crecimiento exponencial de la frecuencia, la variedad y el coste de las amenazas de malware, hoy en día la seguridad debe ser multicapa. Esto se debe a que el malware puede comprometer los sistemas en el nivel de hardware y firmware o durante el arranque, y la seguridad definida por software no llega a todas estas áreas. Para contrarrestar esta vulnerabilidad, la seguridad de los servidores modernos no es una estrategia con un único frente. Debe integrarse en toda la pila de la infraestructura. La combinación de los servidores Dell EMC™ PowerEdge™ de última generación y Windows Server 2022 simplifica para los administradores la importante tarea de alinear el hardware, el firmware y el sistema operativo para proteger adecuadamente las cargas de trabajo críticas para el negocio.

Los beneficios combinados de los servidores con núcleo protegido de Windows Server 2022 y los servidores PowerEdge de última generación

El servidor con núcleo protegido es una nueva característica de Windows Server 2022 que utiliza funcionalidades de hardware, firmware y SO para proporcionar protección contra las amenazas actuales y futuras. La combinación del software de servidor con núcleo protegido de Windows Server 2022 que se ejecuta en el hardware de un servidor PowerEdge de última generación ofrece tres beneficios importantes para organizaciones como la suya:

- Protección avanzada
- Defensa preventiva
- Seguridad simplificada

Protección avanzada

Según los datos de inteligencia sobre amenazas de Microsoft, los PC con núcleo protegido proporcionan más del doble de protección contra infecciones que los PC normales. Microsoft está implementando esta misma tecnología en el ámbito de los servidores con los servidores con núcleo protegido de Windows Server 2022.[5] Las protecciones que ofrece un servidor con núcleo protegido tienen como objetivo crear en dicho servidor una plataforma segura para las cargas de trabajo y los datos críticos. En concreto, los servidores con núcleo protegido utilizan la compatibilidad del procesador con la tecnología de raíz de confianza dinámica para mediciones (DRTM) para colocar el firmware en un entorno aislado basado en el hardware. Este aislamiento ayuda a limitar el impacto de las vulnerabilidades en millones de líneas de código de firmware con grandes privilegios.

Como complemento al aislamiento del firmware de Windows Server 2022, la seguridad basada en virtualización (VBS) aísla las partes esenciales del sistema operativo (como el kernel) del resto del sistema. Esto ayuda a garantizar que los servidores se dediquen a la ejecución de cargas de trabajo críticas y a proteger las aplicaciones y los datos relacionados contra ataques y filtraciones.

Para reforzar aún más el firmware de los servidores PowerEdge frente a ataques, Dell Technologies ayuda a proteger la cadena de suministro de los servidores PowerEdge para garantizar que nadie haya manipulado el servidor mientras estaba en tránsito desde la fábrica hasta las instalaciones del cliente (ver más detalles en Seguridad adicional a través de la integridad de la cadena de suministro de Dell Technologies más adelante).

Defensa preventiva

Esta funcionalidad de núcleo protegido ayuda a defenderse proactivamente y a interrumpir muchas de las rutas que podrían utilizar los atacantes para explotar los sistemas. La integridad del código protegida por hipervisor (HVCI) de VBS aísla la función de toma de decisiones de integridad de código (CI) del resto del sistema operativo Windows, lo que contribuye a garantizar que la única forma en que la memoria del kernel puede convertirse en ejecutable es a través de una verificación de CI. VBS también permite el uso de Windows Defender Credential Guard, en el que las credenciales y los secretos de usuario se almacenan en un contenedor virtual al que el sistema operativo no puede acceder directamente.

Trusted Platform Module 2.0 (TPM 2.0) viene de serie con los servidores con núcleo protegido y ofrece un almacén protegido para claves y datos confidenciales, como las mediciones de los componentes cargados durante el arranque. Esto ayuda a mejorar la seguridad, ya que permite comprobar que el firmware que se ejecuta durante el arranque está firmado válidamente por el autor esperado y no ha sido manipulado. Esta raíz de confianza de hardware también aumenta la protección proporcionada por funcionalidades como el cifrado de unidad BitLocker, que utiliza TPM 2.0 y facilita la creación de flujos de trabajo basados en confirmaciones que se pueden incorporar a las estrategias de seguridad de confianza cero. En conjunto, estas defensas permiten a sus equipos de TI y procedimientos operativos de seguridad distribuir mejor su tiempo entre las muchas áreas de seguridad que necesitan su atención.

Los servidores PowerEdge de última generación son compatibles con el arranque seguro de la interfaz de firmware extensible unificada (UEFI) estándar del sector. El arranque seguro de UEFI comprueba las firmas criptográficas de los controladores UEFI y otros códigos cargados antes de ejecutar el sistema operativo para ayudar a garantizar que el malware no haya manipulado el firmware. Además, los servidores PowerEdge son compatibles con TPM 2.0 para mejorar la seguridad del firmware y del sistema operativo.

Seguridad simplificada

Cuando adquiere un servidor PowerEdge con núcleo protegido, puede estar seguro de que Dell Technologies le ha proporcionado un conjunto de hardware, firmware y controladores que hace honor a su nombre. Microsoft colabora estrechamente con Dell Technologies para simplificar la activación de la seguridad en los servidores PowerEdge.

La nueva funcionalidad de Windows Admin Center facilita a los administradores la configuración de las características de seguridad del SO de los servidores con núcleo protegido de Windows Server 2022. La nueva funcionalidad de seguridad de Windows Admin Center permite a los administradores habilitar la seguridad avanzada con un solo clic. Windows Admin Center presenta el estado de todas las características de seguridad necesarias para los servidores con núcleo protegido de Windows Server 2022, y permite a los administradores activar características según sea necesario desde una única ubicación.

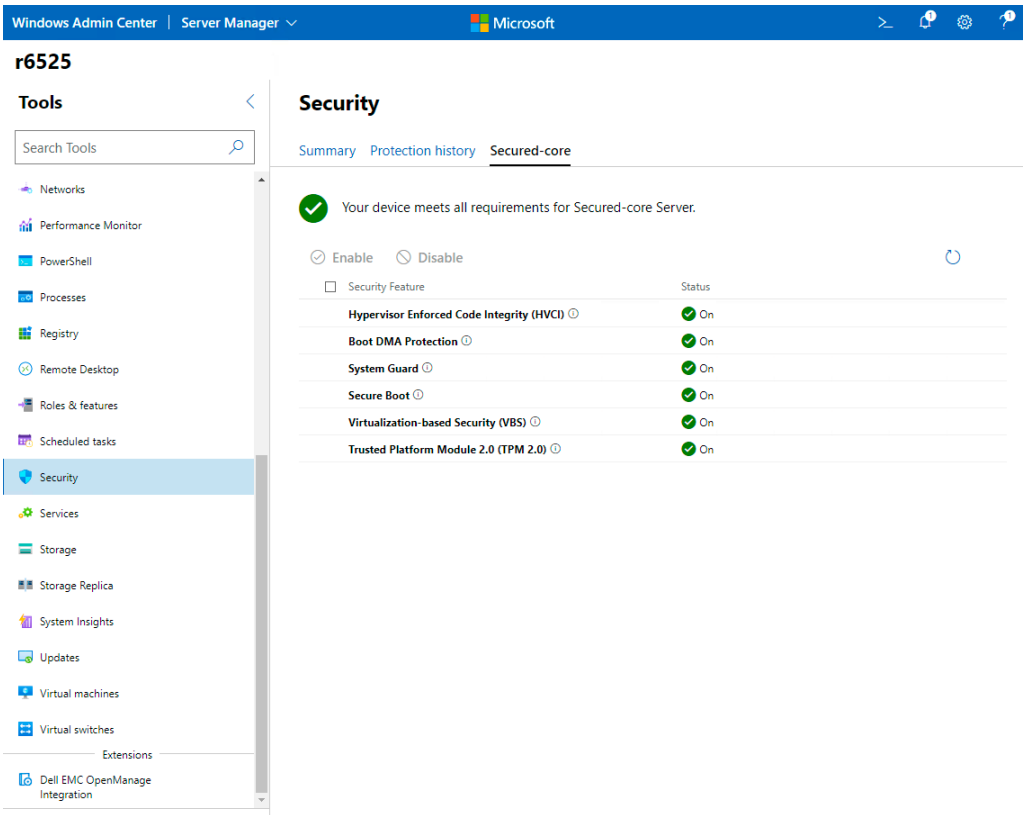


Figura 1. Pantalla de confirmación de núcleo protegido en Windows Admin Center

Dell EMC™ OpenManage™ Integration with Windows Admin Center es una extensión de Windows Admin Center que simplifica aún más la gestión de los servidores con núcleo protegido. Esta extensión de Windows Admin Center simplifica las tareas de seguridad (entre otras) de los administradores de TI gracias a la gestión remota de los servidores PowerEdge. En el contexto de los servidores con núcleo protegido de Windows Server 2022, la extensión OpenManage Integration with Windows Admin Center le permite consultar el inventario de servidores PowerEdge desde Windows Admin Center, y le ofrece una visión unificada del estado, el hardware y la información del inventario de firmware de los componentes del servidor PowerEdge.

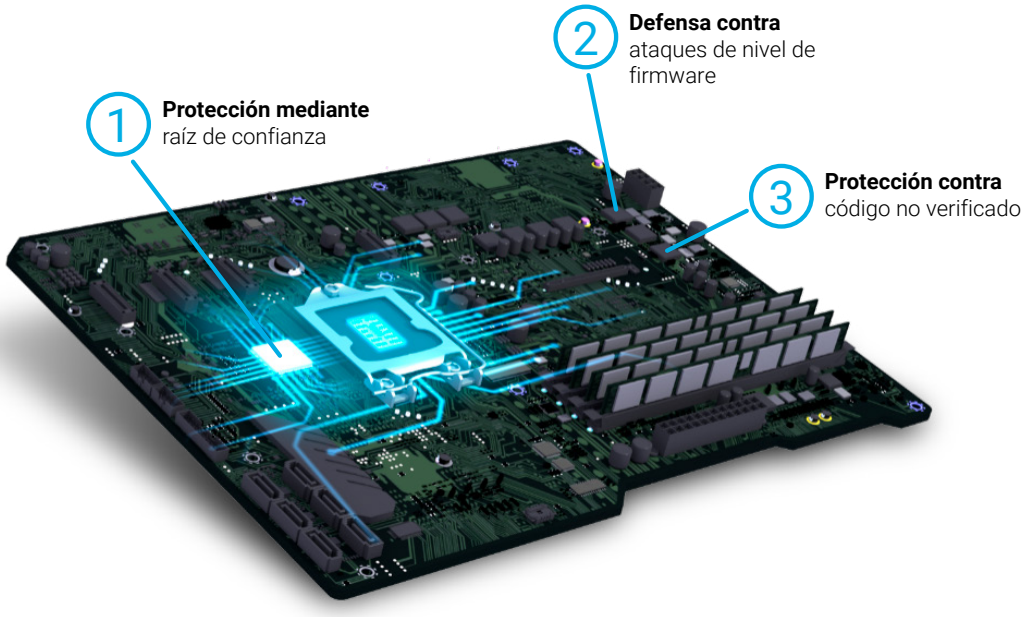
Compatibilidad de los servidores PowerEdge con los servidores con núcleo protegido de Windows Server 2022

Dado que las defensas de los servidores con núcleo protegido son multicapa, la asistencia de su OEM de hardware es crucial. Dell Technologies prueba y certifica los servidores PowerEdge para garantizar que el hardware y el firmware cumplan con los requisitos de las características de seguridad de Windows Server 2022. Además, el hardware y el firmware de los servidores PowerEdge están configurados para habilitar el servidor con núcleo protegido de Windows Server 2022. En la Tabla 1 se detalla cómo el hardware de los servidores PowerEdge da soporte a las características de Windows Server 2022.

Tabla 1. Correlación de las características de seguridad de Windows Server 2022 y las principales características de soporte de los servidores Dell EMC™ PowerEdge™ de última generación

	Windows Server 2022	Servidores Dell EMC™ PowerEdge™ de última generación
Protección avanzada	Los sistemas con núcleo protegido colocan el firmware en un entorno aislado basado en hardware, lo que ayuda a limitar el impacto de las vulnerabilidades basadas en firmware. VBS aísla las partes esenciales del sistema operativo del malware avanzado.	Dell Technologies ayuda a proteger la cadena de suministro de los servidores PowerEdge para garantizar que nadie haya manipulado el firmware ni lo haya puesto en peligro durante el tránsito desde la fábrica hasta las instalaciones del cliente.
Defensa preventiva	Las características de VBS, como HVCI y Windows Defender Credential Guard, evitan clases enteras de vulnerabilidades y protegen mejor los activos confidenciales, como las credenciales. TPM 2.0 proporciona una raíz de confianza de hardware que se utiliza como base segura.	Los servidores PowerEdge admiten el arranque seguro de UEFI, estándar del sector, para comprobar las firmas criptográficas de los controladores UEFI y otros códigos cargados antes de ejecutar el sistema operativo. Los servidores PowerEdge son compatibles con TPM 2.0.
Seguridad simplificada	Windows Admin Center proporciona un acceso sencillo para configurar servidores con núcleo protegido.	Microsoft colabora con Dell Technologies para simplificar la activación de la seguridad en los servidores PowerEdge. La integración de Windows Admin Center con Dell EMC™ OpenManage™ simplifica aún más la gestión de los servidores con núcleo protegido.

Anatomía de la seguridad avanzada y multicapa



1 Protección a través de raíz de confianza

Al asociarse con OEM líderes como Dell Technologies y proveedores de chips como Intel y AMD, los servidores con núcleo protegido utilizan la raíz de confianza de hardware estándar del sector, junto con las funcionalidades de seguridad integradas en las CPU de hoy en día.

Los servidores con núcleo protegido utilizan TPM 2.0 y una CPU moderna con DRTM para arrancar los servidores de forma más segura y minimizar las vulnerabilidades del firmware.

2 Defensa contra ataques de nivel de firmware

Los servidores con núcleo protegido utilizan la seguridad basada en hardware de la CPU moderna para iniciar el sistema en un estado de confianza , y evitan que el malware avanzado manipule el sistema y ataque en el nivel de firmware.

Inicio seguro de protección del sistema utiliza la CPU para validar que el dispositivo arranque de forma más segura, lo que contribuye a evitar ataques avanzados contra el firmware.

3 Protección contra código no verificado

El código que se ejecuta dentro de una base informática de confianza se ejecuta con integridad y no está sujeto a vulnerabilidades ni ataques.

Habilitado con HVCI, un servidor con núcleo protegido solo inicia ejecutables firmados por entidades reconocidas y aprobadas. El hipervisor establece y aplica permisos para evitar que el malware intente modificar la memoria y hacerla ejecutable.

Compatibilidad con los servidores PowerEdge de última generación para una conectividad segura en Windows Server 2022

Los servidores PowerEdge de última generación son compatibles con el cifrado AES-256 de Server Message Block (SMB) para cargas de trabajo que necesiten especial protección. Esta compatibilidad implica que los servidores PowerEdge que ejecutan Windows Server 2022 pueden proporcionar un cifrado integral de los datos de las cargas de trabajo para reforzar la seguridad. El cifrado AES de 256 bits que se usa para SMB en Windows Server 2022 también es lo suficientemente sólido como para resistir incluso ataques de fuerza bruta por parte de ordenadores cuánticos si se utilizan contraseñas lo suficientemente seguras.

Los servidores PowerEdge y Windows Server 2022 amplían aún más el cifrado de SMB integral desde servidores individuales hasta las comunicaciones internas de clústeres con cifrado AES-256 para el tráfico de datos de SMB este-oeste. Estos controles adicionales de cifrado de SMB refuerzan aún más las cargas de trabajo y cierran las posibles vías de ataque.

Por último, Windows Server 2022 utiliza las nuevas instrucciones del estándar de cifrado avanzado de Intel® (Intel® AES-NI) incluido en los procesadores escalables Intel® Xeon® de 3.ª generación y el cifrado AES vectorizado para 256 bits (vAES256) incluido en los procesadores AMD EPYC™ Zen 3. Los conjuntos de instrucciones de estos procesadores avanzados aumentan el rendimiento para el cifrado AES-256 en servidores PowerEdge. Al hacer uso de estas tecnologías de seguridad avanzadas, Dell Technologies y Microsoft le garantizan que no tendrá que elegir entre seguridad sólida y capacidad de respuesta para las cargas de trabajo críticas para el negocio.

Seguridad adicional a través de la integridad de la cadena de suministro de Dell Technologies

La integridad de la cadena de suministro de Dell Technologies protege los componentes del hardware y el firmware de cualquier riesgo durante la fabricación y el envío. En el ámbito de la integridad del hardware, Dell Technologies trabaja para garantizar que no se manipulen los productos ni se inserten componentes falsificados antes de enviarlos a los clientes. Los controles de los que dispone Dell Technologies abarcan la selección de proveedores, el abastecimiento, los procesos de producción y la gobernanza mediante auditorías y pruebas. Las inspecciones de materiales durante la producción ayudan a identificar los componentes marcados de forma incorrecta, que no cumplen los parámetros de rendimiento normales o que contienen un identificador electrónico incorrecto.

En aras de la integridad del software, Dell Technologies quiere asegurarse de que no se introduzca malware ni en el firmware ni en los controladores de dispositivos antes de enviar un producto a sus clientes, además de evitar cualquier tipo de vulnerabilidad en el código. Dell Technologies mantiene la certificación ISO 9001 para todas sus fábricas a nivel mundial. El estricto cumplimiento de estos procesos y controles ayuda a minimizar el riesgo de que se integren componentes falsificados entre los productos de Dell Technologies™ y de que se introduzca malware en el firmware o en los controladores de dispositivos. Además, Dell Technologies implementa estas medidas como parte del proceso del ciclo de vida del desarrollo de software (SDLC).

Dell Technologies también trabaja para garantizar la seguridad física de las instalaciones de fabricación y las cadenas de transporte. Dell Technologies exige que determinadas instalaciones en las que se fabrican productos de Dell Technologies cumplan los requisitos de seguridad de las instalaciones especificados por la Asociación para la Protección de Activos Transportados (TAPA), lo que incluye el uso de cámaras de circuito cerrado supervisadas en áreas clave, controles de acceso y vigilancia continua de entradas y salidas. Dell Technologies también ha implementado medidas de protección contra robos y manipulaciones durante el transporte como parte de un programa de logística líder en su sector. Por último, la verificación de componentes seguros (SCV) de Dell Technologies para servidores PowerEdge permite a los clientes de Dell Technologies verificar que el servidor PowerEdge que ha recibido coincide con el fabricado en origen.

Proteja sus cargas de trabajo críticas con una mejor base de seguridad gracias a Windows Server 2022 y los servidores Dell EMC PowerEdge de última generación

Las cargas de trabajo son tan seguras como la base sobre la que se ejecutan. Las amenazas del malware y las filtraciones de datos no dejarán de crecer en el futuro, sobre todo a medida que los actores maliciosos sigan explorando vías de ataque inmunes a la seguridad tradicional basada en software. Los ataques de firmware se dirigen específicamente a los servidores durante el proceso de arranque, antes incluso de que la seguridad basada en software haya comenzado a proteger los sistemas. La protección de servidores moderna requiere seguridad de múltiples frentes que abarque el hardware, el firmware y el sistema operativo.

Puede que actualizar a Windows Server 2022 tenga ahora más sentido que nunca. El servidor con núcleo protegido incluido con Windows Server 2022 ayuda a las empresas a hacer frente a las amenazas, tanto para el firmware como para el sistema operativo. Si se combinan con las protecciones de integridad del hardware y del software de Dell Technologies, los servidores Dell EMC PowerEdge de última generación que ejecutan Windows Server 2022 pueden ofrecer una seguridad de última generación para toda la pila de hardware, firmware y SO. Además, las características de conectividad segura de Windows Server 2022, que son compatibles con los servidores PowerEdge de última generación, amplían esta seguridad más allá de los servidores individuales y permite abarcar clústeres enteros dentro de su centro de datos. Asimismo, el soporte para Windows Server 2012 finaliza en octubre de 2023, lo que implica que es hora de empezar a planificar la actualización.[6]

Para obtener más información sobre cómo Windows Server 2022 y los servidores Dell EMC PowerEdge de última generación pueden ayudarle a proteger sus cargas de trabajo y datos críticos, visite www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025". Noviembre de 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
[2] IDC. "IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach". Agosto de 2021.
[3] IBM. "How much does a data breach cost?" 2021. www.ibm.com/security/data-breach.
[4] Dan Goodin. "Hospitals hamstrung by ransomware are turning away patients". *Ars Technica*. Agosto de 2021. https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.
[5] Microsoft. "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats". Marzo de 2021. www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/.
[6] A la redacción de este documento. Para obtener la información más reciente sobre el fin de soporte para Windows Server 2012, visite la página del ciclo de vida de Windows Server 2012: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Modernícese con Windows Server 2022.
El sistema operativo preparado para la cloud que potencia las inversiones en las instalaciones con capacidades híbridas.