DELL Technologies

intel®

Resiliencia cibernética

Combata las amenazas con una postura de seguridad profunda que comienza por los servidores Dell PowerEdge, con la tecnología de los procesadores escalables Intel® Xeon®.

Comenzar

Tabla de Contenido

Haga clic en los iconos o en los títulos de los capítulos que aparecen a continuación para ir a secciones específicas. Utilice los botones de flecha en la parte superior para navegar página por página. Use el botón de inicio en la esquina superior izquierda para volver al inicio.

Parte 1: El panorama de la seguridad cibernética

Amenazas cambiantes

Las amenazas cibernéticas y los ataques se están volviendo cada vez más nefastos y generalizados, y se prevé que esto se acelere. En 2020, Cybersecurity Ventures predijo que los costos globales del crimen cibernético crecerían el 15 % por año en los próximos cinco años, y ascenderían a los US$10 500 billones anuales para 2025, un aumento respecto de los US$300 billones en 2015[1]. A medida que se accede a los datos a través de dispositivos, en las instalaciones y en la nube, las vulneraciones de datos de alto impacto se siguen acumulando. Para mantener un entorno más seguro, las empresas deben tener un enfoque más completo.

La transformación digital fue la historia principal los primeros años del nuevo milenio y su aceleración en esta década solo se da a medida que las empresas luchan por adaptarse a los nuevos entornos empresariales, que cambian con rapidez. Debido a la mayor adopción del centro de datos definido por software (SDDC), las empresas se han vuelto más dependientes de los servidores como la base de las funciones de la empresa. Esto significa que la seguridad de los servidores debe ser fundamental para su estrategia general de defensa empresarial, ya que protege contra las amenazas incluso en la capa de firmware.

Se espera que, en todo el mundo, los ataques de ransomware cuesten **US$265 000 millones para 2031[3]**.

Desafíos de la seguridad cibernética

Las amenazas cibernéticas llegan a su empresa desde todas las direcciones. Los participantes tradicionales incluyen hacktivistas, grupos terroristas, estados-nación hostiles, organizaciones delictivas, hackers independientes y espías corporativos pero cada vez más debe tener cautela con las amenazas internas.

Las noticias actuales se enfocan en el aumento de la velocidad, la sofisticación, la eficacia y el impacto financiero de los ataques cibernéticos. Por ejemplo, en 2021 se observó el 50 % más de ataques cibernéticos por semana en redes corporativas en comparación con 2020[2]. Y, si bien el ransomware le costó al mundo US$20 000 millones en 2021, se espera que ese número aumente a US$265 000 millones para 2031[3].

[1] CyberCrime Magazine, El crimen cibernético le costará al mundo US$10 500 billones por año para 2025, 13 de noviembre de 2020

[2] DARKReading, Las empresas sufrieron el 50 % más de ataques cibernéticos por semana en 2021, 11 de enero de 2022.

[3] Cloudwards, Estadísticas, tendencias y hechos del ransomware para 2022 y los años próximos, 22 de marzo de 2022.

Los ataques comunes incluyen los siguientes elementos:

Malware: esto comprende cualquier tipo de software malicioso como el spyware, el adware o los virus que pueden perjudicar el rendimiento o la seguridad del servidor.

Ransomware: es una forma de software malicioso o malware que, cuando se descarga en un servidor, puede bloquear el acceso a datos y archivos en el dispositivo hasta que se pague un rescate.

Ataques de suplantación de identidad o phishing: la suplantación de identidad es el acto de contactar de forma fraudulenta a varias personas o empresas en un intento de obtener acceso no autorizado a información confidencial o personal.

Cadena de suministro: son situaciones en las que los hackers cada vez más buscan aprovecharse de las debilidades de la cadena de suministro o de proveedores externos a medida que las empresas como la suya mejoran su seguridad. El ataque cibernético de 2020 a SolarWinds, una importante empresa de administración de TI, pasó desapercibido durante meses, lo que permitió que SolarWinds infectara a sus clientes con código malicioso. Según Accenture, “el 40 % de los ataques cibernéticos está dirigido a la cadena de suministro”[4].

40 %

de los ataques cibernéticos está dirigido a la cadena de suministro[4].

[4] Accenture, Asegurar la cadena de suministro, 2020

Cumplimiento y presión normativa

A medida que aumentan las amenazas globales, existe una presión normativa continua para definir la orientación de prácticas recomendadas a fin de asegurar no solo las infraestructuras críticas y gubernamentales, sino también el sector privado. Es importante porque, en los Estados Unidos, casi el 90 % de la infraestructura crítica —que integran los servicios de salud, la energía, las finanzas, el transporte, las telecomunicaciones y las utilidades— es propiedad del sector privado[5].

En mayo de 2021 y enero de 2022, en los Estados Unidos se emitieron órdenes ejecutivas desde la Casa Blanca en las que se describió una infraestructura para, a su vez, proteger la infraestructura de la nación, y se proporcionó una orientación detallada sobre la arquitectura de confianza cero. El Gobierno de los Estados Unidos no es el único que desea actuar. Los gobiernos internacionales están desarrollando una orientación normativa en respuesta a las amenazas cibernéticas, y las instituciones privadas están creando políticas e indicaciones para mitigar las amenazas persistentes avanzadas. Estos requisitos no se aplican solo a los organismos federales, sino que también se extienden a la infraestructura crítica y otros mercados verticales.

A medida que los gobiernos buscan reducir o minimizar los ataques cibernéticos, las empresas también deben esperar más orientación e indicaciones, como los siguientes:

- **Autenticación de múltiples factores (MFA)**: la MFA, también conocida como autenticación de dos factores (2FA)[6], protege los datos para prohibir el acceso de un tercero no autorizado. Es una tecnología de seguridad que requiere la verificación de un usuario para obtener acceso mediante el uso de dos o más credenciales independientes. Los sectores como "finanzas, servicios de salud, defensa, aplicación de la ley y el Gobierno federal ya requieren la autenticación de dos factores para acceder a sistemas, redes, sitios web e instalaciones físicas"[7].
- **Cifrado de datos en reposo**: unidades de autocifrado con administración de claves de clase empresarial.

[5] Casa Blanca, Conferencia de prensa: Convocatoria de prensa de fondo acerca de la mejora en la seguridad cibernética de la infraestructura crítica estadounidense, 28 de julio de 2021.

[6] NIST, Repaso de los elementos básicos: ¿Qué es la autenticación de múltiples factores y por qué debería interesarme?, 16 de junio de 2016.

[7] Okta, ¿Qué industrias requieren la autenticación de dos factores?, recuperado en junio de 2022.

¿Qué está en juego?

Los ataques cibernéticos pueden ser devastadores para una empresa. Según lo generalizado que sea el ataque y el daño causado, el tiempo de recuperación puede ser considerable. Se necesitan, en promedio, 22 días para recuperarse de un ataque de ransomware[8]. Desafíos a los que las empresas pueden enfrentarse:

- Tiempo de inactividad para intentar descubrir lo que sucedió y, luego, recuperar los datos perdidos
- Pérdida permanente de datos internos y de clientes, lo que pone en peligro a los posibles clientes a largo plazo
- Pago de multas y readaptaciones para garantizar el cumplimiento de todas las reglas y normativas
- Mala publicidad y pérdida de negocios inmediatamente después de un ataque cibernético
- Pérdida de reputación a largo plazo, ya que los clientes no quieren continuar haciendo negocios con empresas que han sido atacadas

En promedio, se necesitan 22 días para recuperarse de un ataque de ransomware[8].

Algunas empresas están tan enfocadas en el crecimiento del negocio que pueden pasar por alto los aprovisionamientos de seguridad adecuados para proteger y sustentar la empresa. Sin embargo, una vulneración puede cambiar rápidamente la capacidad de rendimiento de su empresa. Si esto se combina con el aumento en la complejidad de la infraestructura, las cargas de trabajo y el uso de datos, el resultado es también un importante incremento en la dificultad para mantener la infraestructura y las operaciones de TI seguras.

Si bien la transformación digital crea oportunidades ilimitadas, persisten los desafíos de crear un entorno de TI ágil y moderno, a la vez que se sostiene la confianza de los clientes y partes interesadas. Si no puede mantenerse un paso adelante de las crecientes amenazas de seguridad, el daño podría ser catastrófico. Un dato a tener presente es que el 64 % de los estadounidenses culparía a una empresa en lugar de a los hackers por perder sus datos personales en un ataque[9]. Además, el 84 % de los consumidores confirmó que son más leales a las empresas que consideran que cuentan con controles de seguridad sólidos[10].

84 %

de los consumidores confirmó que son más leales a las empresas que consideran que cuentan con controles de seguridad sólidos[9].

[8] Statista, Duración del impacto después de un ataque de ransomware durante el primer trimestre de 2020 y el tercer trimestre de 2021, noviembre de 2021.

[9] Forbes, 50 estadísticas que demuestran por qué las empresas deben priorizar la privacidad del consumidor, 22 de junio de 2020.

[10] Informe de investigación de Salesforce, Estado del cliente conectado: tercera edición, junio de 2019.

Recursos

Arquitectura con resiliencia cibernética: infografía

Arquitectura con resiliencia cibernética: video

Seguridad con resiliencia cibernética en los servidores Dell PowerEdge: documentación técnica

Parte 2: Prácticas óptimas de la industria

Confianza cero

es un enfoque arquitectónico compuesto por una infraestructura de principios de seguridad y prácticas recomendadas.

La confianza cero es una respuesta a la complejidad de los entornos de TI modernos, incluidos los de nube y nube híbrida, que son aquellos recursos basados en la nube que no se encuentran dentro del límite de red de su empresa. El problema de la complejidad también se agrava con el reciente aumento de usuarios remotos, millones de dispositivos personales (BYOD) y otras normativas gubernamentales.

La confianza cero no es una arquitectura única, sino un conjunto de principios rectores para el flujo de trabajo, el diseño del sistema y las operaciones. Los enfoques de seguridad eficaces han evolucionado de un conjunto estático de perímetros generales a algo de naturaleza mucho más fluida, en los que no se otorga ninguna confianza a los activos o las cuentas de usuario en función únicamente de su ubicación física o de red o propiedad de los activos.

En otras palabras, un enfoque de confianza cero evalúa y valida muchos puntos en el entorno de TI antes de otorgar permisos. El elemento crítico de confianza cero es la verificación de los activos dentro de la empresa antes de proporcionar acceso, y la verificación continua antes de la ejecución del proceso o el movimiento lateral dentro de la red.

La presión normativa aumentó de manera significativa desde que los ataques exitosos de ransomware afectaron a entidades federales, infraestructura crítica y el sector privado. Un ejemplo de esto es la orden ejecutiva de la Casa Blanca emitida el 12 de mayo de 2021. Desde entonces, se ha generado mucha documentación en la que se explicitan los detalles de la implementación de seguridad y las nuevas normativas. A medida que la orientación normativa continúa evolucionando, la búsqueda de soluciones para la seguridad de la empresa se ha convertido en un imperativo en lugar de una opción. Los requisitos de confianza cero que comenzaron con SP800-207 en el Departamento de Defensa continuaron y fueron definidos en conjunto con la orden ejecutiva de la Casa Blanca y en colaboración con la CISA y la OMB. Notamos que gobiernos internacionales están siguiendo el ejemplo de requisitos más estrictos en todo el mundo[11].

Recursos

Arquitectura de confianza cero: infografía

[11] NIST, Arquitectura de confianza cero, 10 de agosto de 2020.

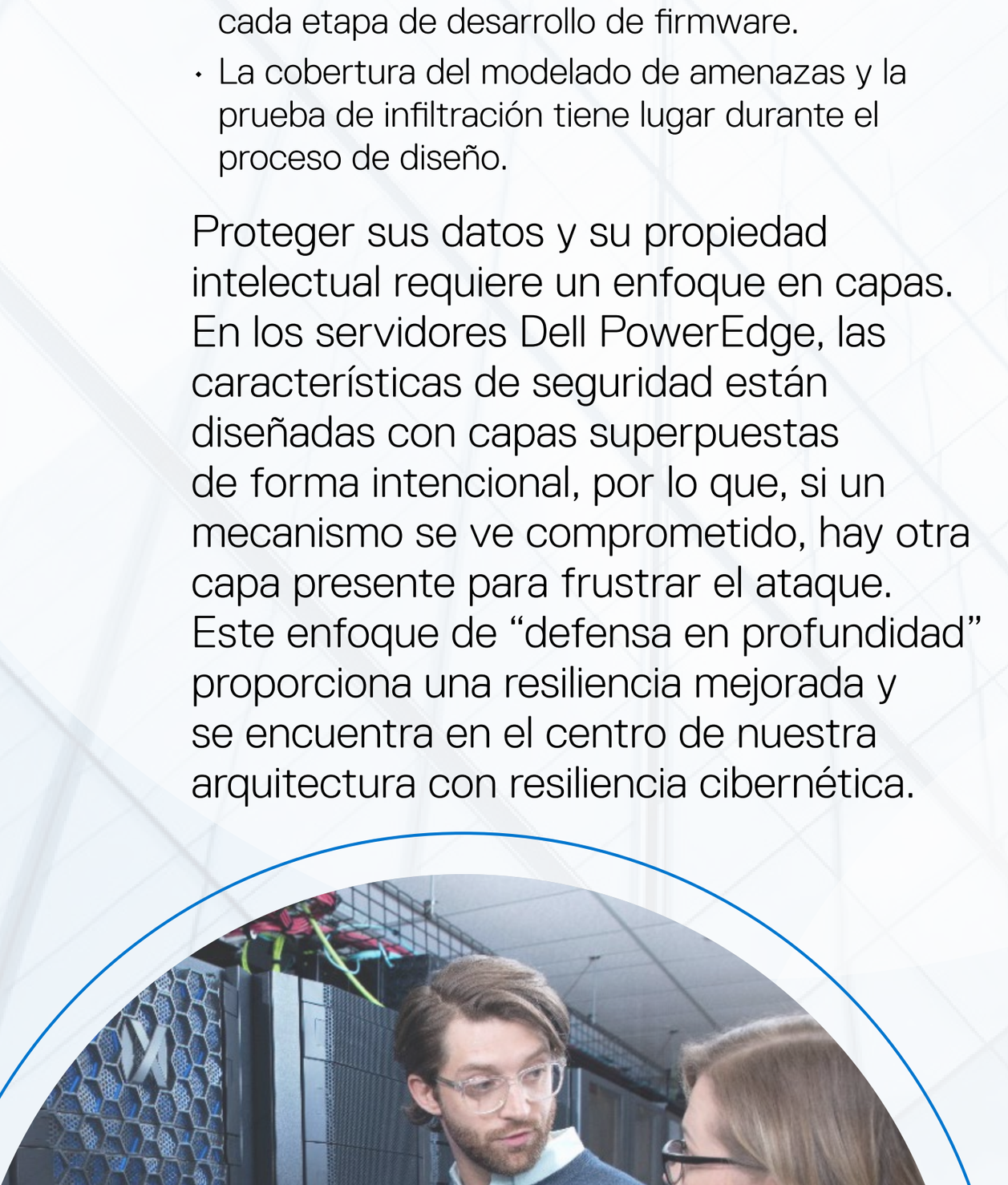
Parte 3: Comenzar con una base segura

La filosofía de la seguridad de Dell radica en nuestra resiliencia cibernética.

La creación de una resiliencia cibernética eficaz comienza con la visión de proteger a sus empresas de actores maliciosos durante todo el ciclo de vida útil de los equipos. En alineación con la infraestructura de seguridad cibernética de NIST, Dell utiliza un enfoque de ciclo de vida útil del desarrollo de la seguridad (SDL) (NIST SP800-160) para crear productos y soluciones que abarcan las necesidades de seguridad, desde el diseño, la fabricación, la cadena de suministro y la administración hasta el desmantelamiento.

- El firmware de servidor se diseña para obstruir, resistir y contrarrestar la inyección de código malicioso durante todas las fases del ciclo de vida útil de desarrollo de los productos.
- Se aplican prácticas de codificación seguras en cada etapa de desarrollo de firmware.
- La cobertura del modelado de amenazas y la prueba de infiltración tiene lugar durante el proceso de diseño.

Proteger sus datos y su propiedad intelectual requiere un enfoque en capas. En los servidores Dell PowerEdge, las características de seguridad están diseñadas con capas superpuestas de forma intencional, por lo que, si un mecanismo se ve comprometido, hay otra capa presente para frustrar el ataque. Este enfoque de "defensa en profundidad" proporciona una resiliencia mejorada y se encuentra en el centro de nuestra arquitectura con resiliencia cibernética.



Los servidores PowerEdge cuentan con la tecnología de los procesadores escalables Intel Xeon que ofrecen funcionalidades de seguridad avanzadas, incluido Intel SGX, el cual ayuda a proteger los datos y el código de las aplicaciones en tiempo real desde el borde hasta el centro de datos y la nube pública de varios grupos de usuarios. Esto permite una colaboración mejorada (por ejemplo, para el aprendizaje federado en IA) mediante el uso de datos compartidos, sin comprometer la privacidad. La aceleración criptográfica de Intel aumenta el rendimiento de las cargas de trabajo con uso intensivo del cifrado, incluidos los servicios web SSL, la infraestructura 5G y los VPN o firewalls, y reduce el impacto en el rendimiento del cifrado generalizado.

Esta arquitectura se basa en una seguridad heredada de PowerEdge con funcionalidades mejoradas que protegen con eficacia su infraestructura gracias a la detección confiable de amenazas y la rápida recuperación tras los ataques cibernéticos. Es un enfoque que se alinea con los componentes clave de la infraestructura de NIST (NIST SP 800-193).

Raíz de confianza de silicio

Los servidores PowerEdge utilizan una raíz de confianza inmutable basada en silicio para certificar criptográficamente la integridad del BIOS y del firmware de Integrated Dell Remote Access Controller (iDRAC). Esta raíz de confianza se basa en claves públicas programables únicas de solo lectura que protegen contra la manipulación de malware. Uno de los aspectos más críticos de la seguridad de los servidores es garantizar que se pueda verificar la seguridad del proceso de arranque. La raíz de confianza proporciona un anclaje de confianza para las operaciones de arranque. Como complemento, el proceso de arranque del BIOS aprovecha la tecnología Intel Boot Guard, que verifica que la firma digital del hash criptográfico de la imagen de arranque coincida con la firma almacenada por Dell Technologies en el silicio en la fábrica.

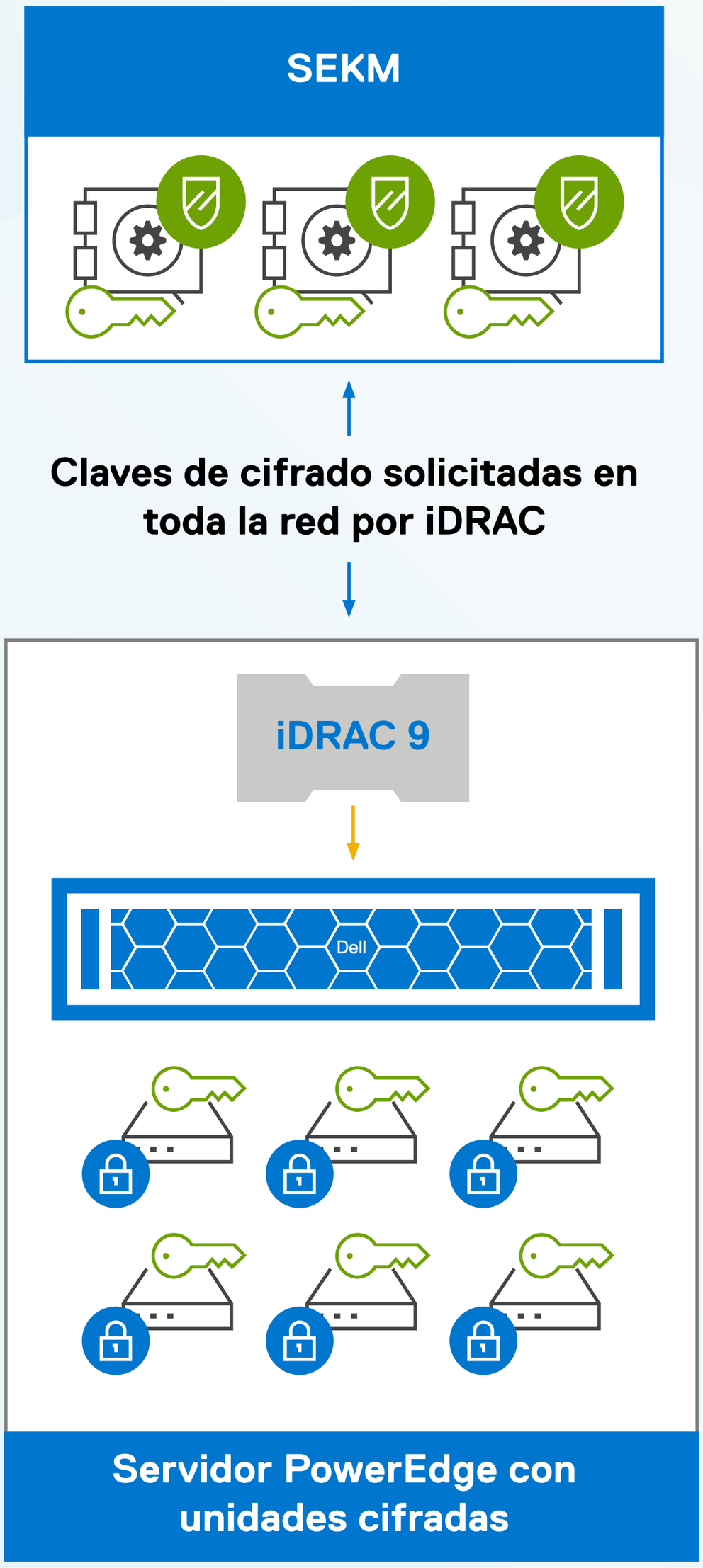
Administración de identidades y acceso

La administración de identidades y acceso (IAM) es un área clave, en especial para la protección contra ataques de ransomware, con controles como MFA para permitir el menor nivel de privilegios y un enfoque de seguridad orientado a la confianza cero. IAM se diseñó con el fin de garantizar que solo las personas correctas puedan acceder a los recursos y los datos de TI adecuados, y de controlar el alcance del acceso.

Protección avanzada de datos

La protección de datos implica proteger los datos de la empresa, ya sea en uso, tránsito o reposo, por lo general, a través del cifrado. Los servidores PowerEdge ofrecen un amplio arreglo de opciones de almacenamiento seguro para sus datos.

La administración de claves externas es una práctica recomendada en la que las claves se almacenan lejos de las unidades y del servidor de hosting. El administrador de clave empresarial segura (SEKM) permite que los clientes de PowerEdge administren sus claves de manera centralizada para SED en servidores PowerEdge y escalen con la expansión de la capacidad de almacenamiento. La administración de claves locales (LKM) también está disponible para entornos en los que el acceso central puede ser difícil o los requisitos de seguridad son menos estrictos.



Ejemplo de implementación de SEKM

Recursos

Protección de datos: infografía

SEKM: página web

SEKM: video

Activar OpenManage Secure Enterprise Key Manager (SEKM) en los servidores Dell PowerEdge: documentación técnica

SEKM: infografía

Arquitectura con resiliencia cibernética: video

Ciclo de vida útil del desarrollo de la seguridad de Dell

Dell Technologies crea intencionalmente un código de controles de seguridad para cada fase del ciclo de vida útil del servidor, desde la recopilación de requisitos hasta el mantenimiento del servidor. Esto incluye el código desarrollado para obstruir, resistir y contrarrestar inyección.

Panorama de la seguridad cibernética

Prácticas óptimas de la industria

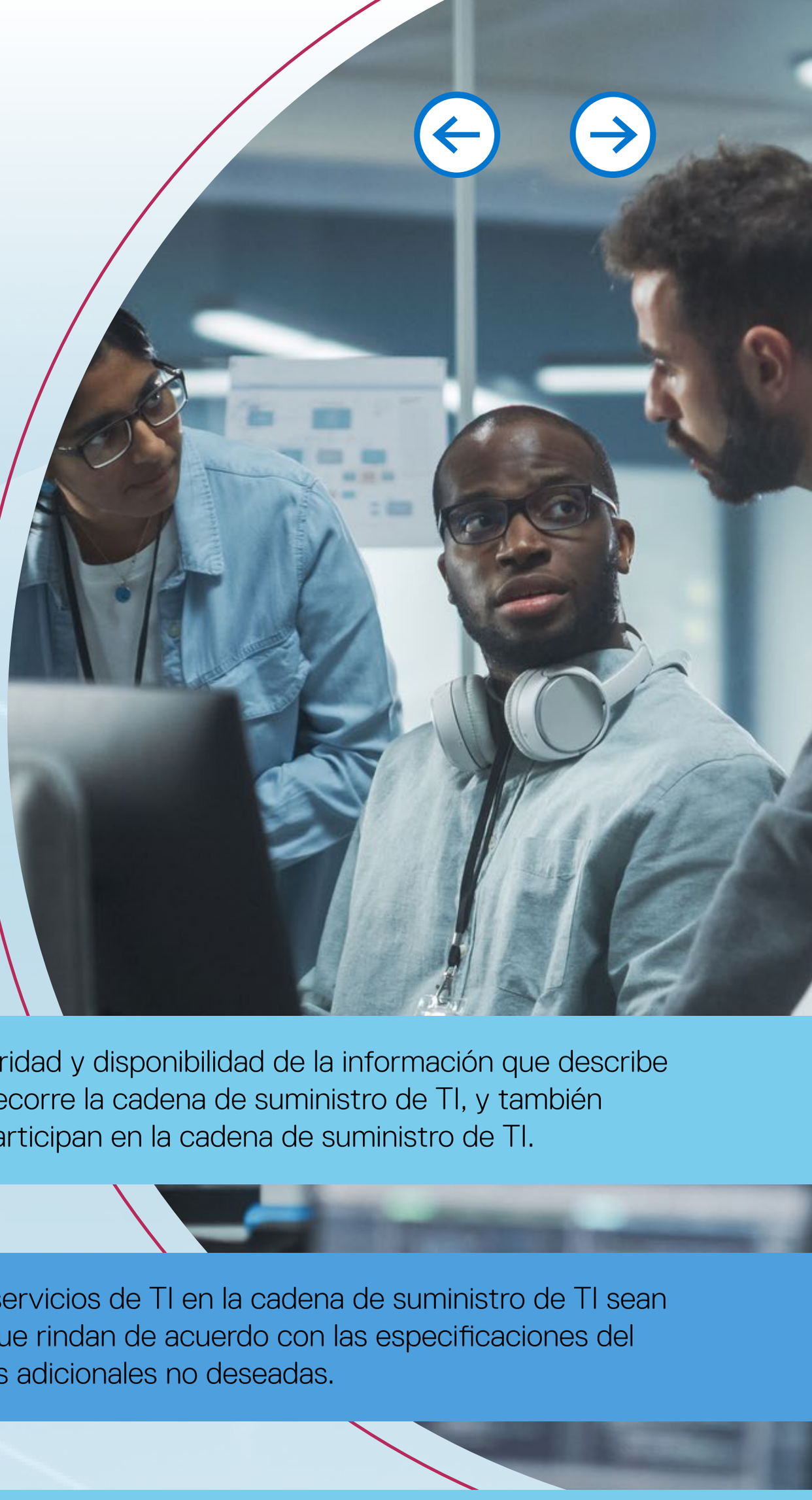
Soporte para la infraestructura de NIST

Modelo de confianza cero

Éxito de su empresa

Garantía de la cadena de suministro verificada

El enfoque completo de Dell Technologies en cuanto a la garantía de la cadena de suministro incluye aprovisionamientos fundamentales, como el personal físico y los controles de seguridad cibernética. Dell Technologies también mejora la garantía de integridad de los componentes con su oferta de verificación segura de componentes (SCV). SCV permite que los clientes verifiquen de forma criptográfica que los componentes configurados en la fábrica coincidan con lo que se les entregó.



Seguridad

Proporciona la confidencialidad, integridad y disponibilidad de la información que describe la cadena de suministro de TI o que recorre la cadena de suministro de TI, y también la información sobre las partes que participan en la cadena de suministro de TI.

Integridad

Garantiza que los productos o servicios de TI en la cadena de suministro de TI sean originales y sin alteraciones, y que rindan de acuerdo con las especificaciones del comprador y sin funcionalidades adicionales no deseadas.

Calidad

Reduce las vulnerabilidades que pueden limitar la función deseada de un componente, causar fallas en los componentes o proporcionar oportunidades de explotación.

Resiliencia

Garantiza que la cadena de suministro de TI proporcionará los productos y servicios de TI necesarios a pesar de las interrupciones.

Recursos

Verificación segura de componentes: video

Verificación segura de componentes: nota técnica

Verificación segura de componentes: charla tecnológica

Grupo de NCC: Evaluación de seguridad de la verificación segura de componentes: documentación técnica de la cadena de suministro

Beneficios de los productos con resiliencia cibernética

- Tiempo de actividad máximo para lograr la productividad del personal
- Preservación de la reputación de la empresa
- Confianza del cliente
- Cumplimiento para evitar multas y readaptaciones costosas
- Libertad para innovar sin distracciones

Parte 4: Uso de la resiliencia cibernética para cumplir con los requisitos de confianza cero

El enfoque de confianza cero de Dell Technologies se refinó para alinearse con los estándares del Departamento de Defensa (DoD) de los Estados Unidos. Habilitamos una arquitectura de confianza cero a través de extensas funcionalidades con resiliencia cibernética y un enfoque de siete pilares que permite que los usuarios realicen una verificación en cada punto del entorno de TI antes de que se otorguen permisos.

Pilar 1: Confianza en el dispositivo

Nuestra raíz de confianza de hardware basada en silicio proporciona un nivel de seguridad en todo el ciclo de vida útil del servidor, desde el diseño hasta el desmantelamiento. Nuestra cadena de suministro segura incluye varias capas de controles, como la verificación de componentes, para ayudar a garantizar que nuestros servidores y software no se hayan manipulado o modificado de manera maliciosa. SCV cuenta con certificados de inventario firmados criptográficamente en todo el portafolio de servidores PowerEdge, incluida la verificación automática segura, para que no se preocupe por la integridad de su hardware durante el tránsito hacia su centro de datos.

Pilar 2: Confianza en el usuario

Con iDRAC, los administradores de TI pueden implementar, actualizar y monitorear con seguridad los servidores PowerEdge de manera local o remota. Para mejorar la seguridad, iDRAC ofrece una MFA mediante RSA SecureID, también con integraciones a través de Active Directory, integración en LDAP con Single Sign On (SSO), y auditoría y control de acceso basados en funciones.

Pilar 3: Confianza en el transporte y la sesión

PowerEdge BMC (iDRAC) tiene un módulo de red dedicado y las opciones Secure Shell (SSH)/seguridad de capa de transporte (TLS), que funcionan para cifrar y autenticar los datos que pasan entre sus servidores y el navegador que ejecuta la interfaz de usuario web de iDRAC. iDRAC permite la administración remota y monitorea el sistema en busca de eventos críticos mediante sensores en la tarjeta madre. Las alertas y los eventos de registro se envían cuando los parámetros superan sus umbrales actuales.

Pilar 4: Confianza en el software

Realizamos pruebas proactivas de verificación, validación y seguridad durante todo el ciclo de vida útil del software para proteger nuestro software y reducir la probabilidad de que se inserte malware o vulnerabilidades de código en este. El arranque verificado integral incluye imágenes del BIOS y firmware firmadas, lo que garantiza que el código no autorizado no se ejecute en un servidor PowerEdge. Otras características con resiliencia cibernética incluyen la detección automatizada de desviaciones, las funcionalidades seguras de arranque de UEFI y la recuperación para el BIOS y los sistemas operativos.

Pilar 5: Confianza en los datos

SEKM funciona en combinación con unidades de autocifrado para el cifrado basado en hardware junto con la administración de claves central ampliable para ayudarlo a implementar y monitorear claves de cifrado, incluidas las de ubicaciones remotas y las que se encuentran en la nube. Esto brinda protección contra el acceso no autorizado a unidades o sistemas perdidos o robados. Este cifrado de hardware se puede combinar con el cifrado de software, como el cifrado de VMware® vSAN™ en VxRail.

La computación confidencial permite la protección de los datos en uso en la CPU y la memoria, e incluye tecnologías de Intel (SGX, TME). Intel SGX proporciona aislamiento a nivel de aplicación o función para minimizar el perímetro de confianza.

La combinación del cifrado de los datos en reposo, la administración ampliable de claves y la computación confidencial puede ofrecer los niveles de protección necesarios para contrarrestar las cambiantes amenazas actuales.

Pilar 6: Visibilidad y análisis

La capacidad de observar lo que está ocurriendo en su entorno es crítica. La detección de desviaciones del firmware, por ejemplo, proporciona información en tiempo real sobre el estado del firmware, incluido cualquier cambio no autorizado. Si se detectan cambios, el sistema se puede revertir a un estado seguro anterior. Además, los eventos de cambio se pueden rastrear a través del registro y las alertas automatizadas, que soportarán la auditoría y el análisis para evaluar el estado general del sistema.

Pilar 7: Automatización y orquestación

OpenManage Enterprise es una aplicación de administración y monitoreo de sistemas que proporciona una vista completa de los servidores PowerEdge, el almacenamiento interno y otros componentes. Incluye la detección de desviaciones para buscar cambios desde una plantilla de configuración definida por el usuario, crea alertas y registros a fin de realizar un seguimiento del estado del sistema, y permite la corrección de configuraciones incorrectas basadas en políticas previas a la configuración. OpenManage abarca reversión de firmware, actualizaciones centralizadas, renovación automática de certificados de la capa de conectores seguros (SSL) e implementaciones automatizadas para brindar una configuración de seguridad coherente.

Recursos

OpenManage Secure Enterprise Key Manager: resumen de la solución

Comprender la computación confidencial con entornos de ejecución de confianza y computación de confianza: modelos base

Arquitectura de confianza cero: infografía

Confianza cero: video

Parte 5: Posicionamiento de su empresa para lograr el éxito con Dell Technologies e Intel

El aumento en la sofisticación y en la superficie de ataque de las amenazas demandan que se aborde la resiliencia cibernética desde una perspectiva moderna. Nuestra respuesta es brindarle soporte en la creación de una arquitectura de confianza cero con una amplia variedad de herramientas y tecnologías. Nuestro enfoque de seguridad permite controles más granulares que comiencen con el acceso y la autorización, y se trasladen a la resiliencia de los datos y del sistema, a la vez que se ofrece una experiencia de usuario superior.

Con Dell Technologies e Intel como sus partners, obtendrá los siguientes beneficios:

- Resiliencia cibernética probada en la que la seguridad está incorporada, y no agregada
- Sencillez en el balanceo de los objetivos del negocio y la productividad con la seguridad y la privacidad
- Un conjunto de hardware y software diseñado para proteger su infraestructura de TI y, al mismo tiempo, brindarle confianza, control y escala a su postura de seguridad
- Vigilancia continua para mantener una postura de seguridad sólida mediante una respuesta rápida a vulnerabilidades y ataques comunes

Recursos

Soluciones de seguridad: página web

Servicios de resiliencia del negocio

Detección y respuesta administradas

Para obtener más información acerca de los servidores PowerEdge con resiliencia cibernética, visite Dell.com/Servers.

Suscríbase al popular podcast de Dell Technologies, Power2Protect, y manténgase al día con los episodios más recientes sobre la seguridad y la resiliencia cibernética.