DELL Technologies

intel®

Ciberresiliencia

Enfréntese a las amenazas con una estrategia de seguridad detallada que comienza con los servidores Dell PowerEdge, equipados con procesadores escalables Intel® Xeon®.

Empezar

Tabla de contenido

Haga clic en los iconos o capítulos que aparecen a continuación para ir a secciones específicas. Utilice los botones de flecha de la parte superior para desplazarse por las páginas. Utilice el botón de inicio de la esquina superior izquierda para volver al principio.

Parte 1: Panorama de ciberseguridad

Amenazas en constante evolución

Las ciberamenazas y los ataques son cada vez más malintencionados y generalizados, y se espera que sean muchos más. En 2020, Cybersecurity Ventures predijo que los costes globales del cibercrimen aumentarían un 15 % por año en los próximos cinco años, lo que supondría los 10 500 millones de dólares anuales para 2025, frente a los 3000 millones de 2015.[1] A medida que se accede a los datos en todos los dispositivos, en local y en la cloud, las vulneraciones de datos de gran impacto siguen aumentando. Para mantener un entorno más seguro, las empresas deben contar con un enfoque más completo.

La transformación digital era lo más importante en el año 2000, pero solo se aceleró en 2020 cuando las organizaciones tuvieron que adaptarse forzosamente a entornos empresariales nuevos y en constante cambio. Con una mayor adopción del modelo de centro de datos definido por software (SDDC), las organizaciones dependen más de los servidores como base para las funciones empresariales. Esto significa que la seguridad del servidor debe ser la base de su estrategia de defensa empresarial general, ya que protege contra las amenazas directamente en la capa de firmware.

Se espera que los costes por ataques de ransomware asciendan a

265 000 millones de dólares en todo el mundo para 2031.[3]

Retos de ciberseguridad

Las ciberamenazas llegan a su empresa por todas partes. Los responsables ya no solo son los típicos (hacktivistas, grupos terroristas, naciones hostiles, organizaciones criminales, hackers independientes o espía corporativos) sino que cada vez más llegan desde dentro.

Se ve en las noticias a diario. Los ciberataques son cada vez más comunes, sofisticados y eficaces, y suponen un impacto financiero importante. Por ejemplo, en 2021 se observó un 50 % más de ciberataques a la semana en redes corporativas en comparación con 2020.[2] Y aunque el ransomware costó 20 000 millones de dólares a nivel mundial en 2021, se espera que esa cantidad aumente a 265 000 millones de dólares para 2031. [3]

[1] CyberCrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 13 de noviembre de 2020

[2] DARKReading, Businesses Suffered 50% More Cyberattack Attempts per Week in 2021, 11 de enero de 2022.

[3] Cloudwards, Ransomware Statistics, Trends, and Facts for 2022 and Beyond, 22 de marzo de 2022.

Estos son los ataques más comunes:

Malware: Cualquier software malicioso, como spyware, adware o virus, que pueda dañar el rendimiento o la seguridad de su servidor.

Ransomware: Forma de software malicioso o malware que, si se descarga en un servidor, puede bloquear el acceso a los datos y a los archivos del dispositivo hasta que se pague un rescate.

Ataques de phishing o phishing: Acto de contactar de forma fraudulenta con varias personas o empresas en un intento de obtener acceso no autorizado a información personal o confidencial.

Cadena de suministros: Situaciones en las que los hackers buscan cada vez más aprovechar las debilidades de la cadena de suministros o de proveedores de terceros conforme organizaciones como la suya mejoran la seguridad. El ciberataque de 2020 contra SolarWinds, una importante empresa de administración de TI, pasó inadvertido durante meses, lo que supuso que SolarWinds infectase a sus clientes con código malicioso. Según Accenture, "el 40 % de los ciberataques van dirigidos a la cadena de suministros".[4]

Un 40 %
de los ciberataques están dirigidos a la cadena de suministros.[4]

[4] Accenture, Securing the Supply Chain, 2020

Cumplimiento normativo y presión normativa

A medida que aumentan las amenazas globales, la presión normativa por definir las mejores prácticas con el fin de proteger no solo las infraestructuras críticas y gubernamentales, sino también las del sector privado, es continua. Esto es muy significativo. En Estados Unidos, por ejemplo, prácticamente el 90 % de las infraestructuras críticas (servicios de salud, energía, finanzas, transporte, telecomunicaciones y servicios públicos) es gestionado en el sector privado.[5]

En mayo de 2021 y enero de 2022, Estados Unidos emitió una serie de decretos presidenciales que describían un marco para proteger la infraestructura del país, además de incluir una guía detallada para lograr una arquitectura de confianza cero. Estados Unidos no es el único país que quiso actuar. Otros gobiernos están desarrollando orientación normativa en respuesta a las ciberamenazas, y las instituciones privadas están creando políticas y exigencias para mitigar las amenazas persistentes avanzadas. Estos requisitos van más allá de las agencias federales: llegan a infraestructuras críticas y a otros mercados verticales.

Conforme los gobiernos buscan evitar o minimizar los ciberataques, las organizaciones también deben esperar más orientación y exigencias, como las siguientes:

- **Autenticación multifactor (MFA)**: La autenticación multifactor, también conocida como autenticación de dos factores (2FA),[6] protege los datos frente a accesos de terceros no autorizados. Esta es una tecnología de seguridad que requiere la verificación del usuario para obtener acceso mediante el uso de dos o más credenciales independientes. Sectores como el "financiero, servicios de salud, defensa, legal y de administración oficial federal ya requieren la autenticación de dos factores para acceder a sistemas, redes, sitios web y ubicaciones de edificios físicos".[7]
- **Cifrado de datos en reposo**: Unidades de cifrado automático con gestión de claves de clase empresarial

[5] La Casa Blanca, Informe de prensa: Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure, 28 de julio de 2021.
[6] NIST, Back to Basics: What's multi-factor authentication - and why should I care?, 16 de junio de 2016.
[7] Okta, Which Industries Require Two-Factor Authentication?, con acceso en junio de 2022.

Qué hay en juego

Los ciberataques pueden ser devastadores para una organización. En función de cuál sea el alcance del ataque y del daño causado, el tiempo de recuperación se puede prolongar bastante. De media, se tardan 22 días en recuperarse de un ataque de ransomware.[8] Estos son algunos de los retos a los que se pueden enfrentar las organizaciones:

- Tiempo de inactividad para intentar descubrir lo que ha ocurrido y recuperar, a continuación, cualquier dato que se haya perdido
- Pérdida permanente de datos internos y de clientes, lo que puede poner en peligro a los posibles clientes a largo plazo.
- Pago de sanciones y reequipamientos para garantizar que se cumplen todas las reglas y normativas
- Mala publicidad y pérdida de negocio en el momento inmediatamente posterior a un ciberataque
- Pérdida de reputación a largo plazo, ya que los clientes son reticentes a seguir haciendo negocios con empresas que hayan sido atacadas

De media se necesitan **22 días** para recuperarse de un ataque de ransomware.[8]

Algunas organizaciones están tan centradas en hacer crecer el negocio que pueden pasar por alto las disposiciones de seguridad adecuadas para proteger y mantener el negocio. Aun así, una vulneración puede cambiar rápidamente la capacidad de su organización para actuar. Si esto se combina con el hecho de que la infraestructura, las cargas de trabajo y el uso de datos son cada vez más complejos, el resultado es que mantener la seguridad de infraestructura y operaciones de TI es cada vez más complicado.

A pesar de que la transformación digital genera oportunidades ilimitadas, el reto de crear un entorno de TI ágil y moderno y mantener, al mismo tiempo, la confianza de los clientes y partes interesadas sigue estando presente. Si no puede adelantarse a las crecientes amenazas de seguridad, las consecuencias pueden ser catastróficas. Un dato que tener en cuenta: el 64 % de los estadounidenses culparía a una empresa (y no al hacker) de perder sus datos personales por un ataque. [9]Además, el 84 % de los consumidores confirma que son más fieles a empresas que, según perciben, cuentan con controles de seguridad sólidos.[10]

84 % de los consumidores confirma que son más fieles a empresas que, según perciben, cuentan con controles de seguridad sólidos.[9]

[8] Statista, Length of impact after a ransomware attack Q1 2020- Q3 2021, noviembre de 2021.
[9] Forbes, 50 Stats Showing Why Companies Need To Prioritize Consumer Privacy, 22 de junio de 2020.
[10] SalesForce Research Report, State of the Connected Customer: Third Edition, junio de 2019.

Recursos

Infografía Cyber Resilient Architecture

Vídeo: Cyber Resilient Architecture

Documento técnico Cyber Resilient Security in Dell PowerEdge Servers

Parte 2: Procedimientos recomendados del sector

Confianza cero

Enfoque arquitectónico compuesto por una infraestructura de principios de seguridad y procedimientos recomendados.

La confianza cero es una respuesta a la complejidad de los entornos de TI modernos, en cloud y en cloud híbrida: recursos basados en la cloud que no están dentro de la límite de la red de su organización. El problema de complejidad también se ve agravado por el reciente aumento de usuarios remotos, millones de BYOD (Bring Your Own Device) y otras normativas oficiales.

La confianza cero no es una única arquitectura, sino un conjunto de principios rectores aplicables al flujo de trabajo, el diseño del sistema y las operaciones. Los enfoques de seguridad eficaces han evolucionado de un conjunto estático e impreciso de perímetros a algo mucho más fluido per se, en el que el hecho de saber a quién pertenece un activo o de dónde procede una cuenta de usuario no es sinónimo de confiar en ellos.

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

La presión normativa se ha intensificado significativamente desde el éxito de los ataques de ransomware en entidades federales, infraestructuras crítica y el sector privado. Un ejemplo de ello es el decreto presidencial emitido el 12 de mayo de 2021. Desde entonces, se ha generado una gran cantidad de documentos con detalles sobre la implementación de la seguridad y las nuevas normativas. Puesto que la orientación normativa sigue evolucionando, la búsqueda de soluciones de seguridad se ha convertido en algo imperativo, no opcional. Los requisitos de confianza cero que empezaron con la certificación SP800-207 del departamento de defensa de Estados Unidos (DoD) se han ido perfilando con otros decretos presidenciales en colaboración con la CISA y la OMB. Y hemos observado que, a nivel mundial, hay otros países que siguen normas con requisitos más estrictos.[11]

Recursos

Infografía Zero-trust architecture

[11] NIST, Zero Trust Architecture, 10 de agosto de 2020.

Parte 3: El fundamento de una base segura

La filosofía de Dell en materia de seguridad radica en nuestra ciberresiliencia.

El primer paso para crear una ciberresiliencia eficaz es contar con una visión de protección de las organizaciones frente a actores maliciosos a lo largo del ciclo de vida del equipo. En consonancia con la infraestructura de ciberseguridad del NIST, Dell aplica un enfoque de ciclo de vida de desarrollo de seguridad (SDL) (NIST SP800-160) para crear productos y soluciones que abarquen las necesidades de seguridad, desde el diseño hasta la retirada del producto, pasando por la cadena de suministros y la gestión.

- El firmware del servidor se ha diseñado para obstaculizar, evitar y contrarrestar la introducción de código malicioso durante todas las fases del ciclo de vida del desarrollo del producto.
- En cada etapa del desarrollo del firmware se aplican prácticas de codificación seguras.
- Durante el proceso de diseño, se realiza el modelado de amenazas y se comprueba la cobertura de las pruebas de penetración.

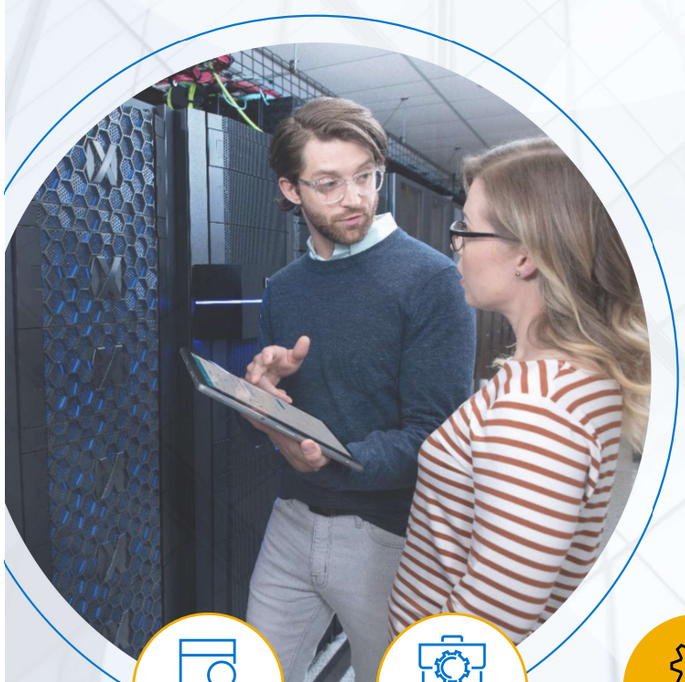
Para proteger los datos y la propiedad intelectual, se debe adoptar un enfoque en capas. En los servidores Dell PowerEdge, las características de seguridad están diseñadas con capas superpuestas intencionadamente: si un mecanismo se ve comprometido, otra capa se encarga de evitar el ataque. Este enfoque de "defensa en profundidad" mejora la resiliencia y es el núcleo de nuestra arquitectura ciberresilente.

Los servidores PowerEdge están equipados con procesadores escalables Intel Xeon que ofrecen capacidades de seguridad avanzadas, incluido Intel SGX, que ayuda a proteger los datos y el código de las aplicaciones en tiempo real desde el perímetro hasta el centro de datos, pasando por la cloud pública de múltiples grupos de usuarios. Esto permite mejorar la colaboración (por ejemplo, para aprendizaje federado en IA) mediante datos compartidos, sin poner en riesgo la privacidad. Intel Crypto Acceleration aumenta el rendimiento de las cargas de trabajo con uso intensivo de cifrado, incluidas las de los servidores web SSL, infraestructura 5G y VPN/firewalls y reduce el impacto en el rendimiento del cifrado generalizada.

Esta arquitectura se basa en seguridad de PowerEdge heredada con capacidades mejoradas que protegen eficazmente su infraestructura, ya que detectan amenazas de forma fiable y se recuperan rápidamente de ciberataques. Es una enfoque que se alinea con los componentes clave del marco de la infraestructura del NIST (NIST SP 800-193).

Raíz de confianza de silicio

Los servidores PowerEdge utilizan la raíz de confianza inmutable del chip de silicio para confirmar criptográficamente la integridad del BIOS y del firmware Integrated Dell Remote Access Controller (iDRAC). Esta raíz de confianza se basa en claves públicas programables de un solo uso y de solo lectura que proporcionan protección contra las manipulaciones del malware. Uno de los aspectos más importantes de la seguridad del servidor es garantizar que el proceso de arranque es seguro. La raíz de confianza proporciona un punto de anclaje de confianza para las operaciones de arranque. Además de esto, 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 coincide con la firma almacenada en el chip por Dell Technologies de fábrica.



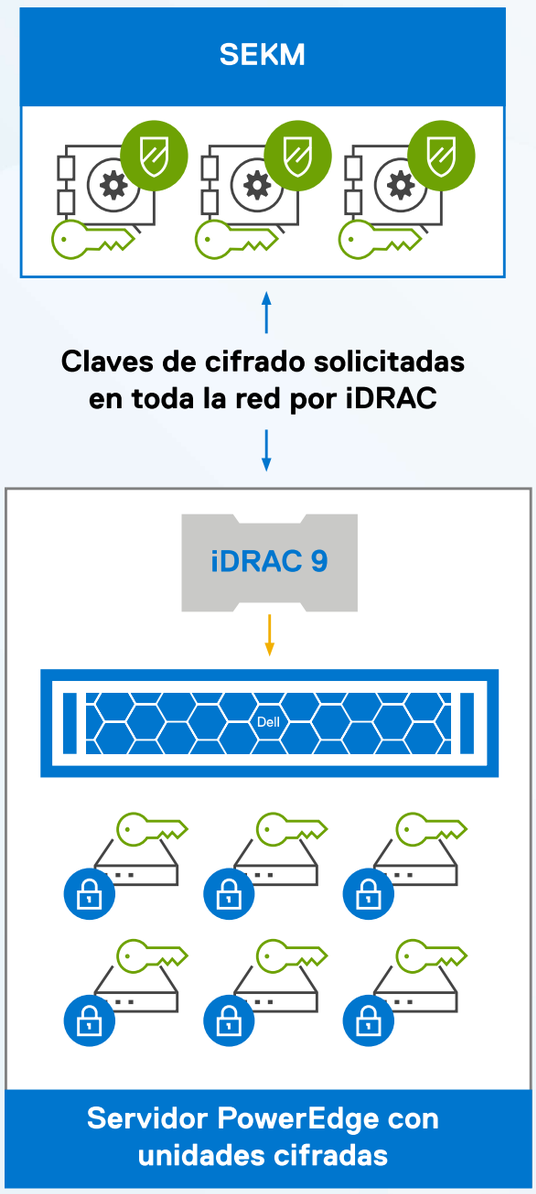
Gestión del acceso y las identidades

La administración de acceso e identidades (IAM) es un área crítica en especial para la protección contra ataques de ransomware con controles como MFA para habilitar el mínimo privilegio y un enfoque orientado a la seguridad de confianza cero. El modelo de IAM está diseñado para garantizar que solo las personas adecuadas puedan acceder a los recursos y datos de TI adecuados y controlar el alcance de acceso.

Protección de datos avanzada

La protección de datos implica proteger los datos de su negocio, en uso, en tránsito o en reposo, normalmente mediante cifrado. Los servidores PowerEdge ofrecen una amplia cabina de opciones de almacenamiento seguro para sus datos.

La gestión de claves externas es una práctica recomendada en la que las claves se almacenan lejos de unidades y servidores de hosting. Con Secure Enterprise Key Manager (SEKM), los clientes de PowerEdge pueden gestionar las claves de forma centralizada para SED en servidores PowerEdge y escalar mediante la expansión de la capacidad de almacenamiento. La gestión de claves local (LKM) también está disponible para entornos en los que el acceso central puede ser difícil o en los que los requisitos de seguridad son menos estrictos.



Ejemplo de implementación de SEKM

Recursos

Infografía Data Protection

Página web de SEKM

Vídeo: SEKM

Documento técnico Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell PowerEdge Servers

Infografía SEKM

Vídeo: Cyber Resilient Architecture

Ciclo de vida del desarrollo de la seguridad de Dell

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

Garantía verificada de la cadena de suministros

El enfoque integral de Dell Technologies aplicado a la garantía de la cadena de suministros incluye disposiciones básicas como controles de ciberseguridad, físicos y personales. Dell Technologies también mejora la garantía de integridad de los componentes con su oferta de verificación de componentes seguros SCV. Dell Secured Component Verification permite a los clientes verificar criptográficamente que los componentes definidos de fábrica coinciden con los que se les han entregado.

Seguridad

Proporciona la confidencialidad, la integridad y la disponibilidad de la información que describe la cadena de suministros de TI o que transita por la cadena de suministros de TI, así como información sobre las partes que participan en la cadena de suministros de TI.

Integridad

Garantiza que los productos o servicios de TI de la cadena de suministros de TI sean auténticos y no tengan modificaciones, y que funcionarán de acuerdo con las especificaciones del comprador y sin funcionalidad adicional no deseada.

Calidad

Reduce las vulnerabilidades que pueden limitar la función prevista de un componente, provocar fallos en este o proporcionar oportunidades de vulneración.

Resiliencia

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

Recursos

Vídeo: Secured Component Verification

Nota técnica de Secured Component Verification

Charla técnica de Secured Component Verification

NCC Group: Secured Component Verification Security Assessment (documento técnico sobre la cadena de suministros)

Beneficios de los productos ciberresilentes

- Tiempo de actividad máximo para la productividad del personal
- Integridad de la reputación del negocio
- Confianza de los clientes
- Cumplimiento normativo para evitar costosas sanciones y reequipamientos
- Libertad para innovar sin distracciones

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

El enfoque de confianza cero de Dell Technologies se ha perfeccionado para ajustarse a los estándares del Departamento de Defensa de Estados Unidos (DoD). Para habilitar el modelo de arquitectura de confianza cero, aplicamos amplias capacidades ciberresilentes y un enfoque de siete pilares que permite a los usuarios realizar una comprobación en cada punto del entorno de TI antes de otorgar ningún permiso.

Pilar 1: Confianza de dispositivos

Nuestra raíz de confianza de hardware en chip proporciona un nivel de seguridad en todo el ciclo de vida del servidor, desde el diseño hasta la retirada del producto. Nuestra cadena de suministros segura incluye varias capas de controles, como la verificación de componentes, para ayudar a garantizar que nuestros servidores y software no hayan sido manipulados ni modificados de forma maliciosa. SCV incluye certificados de inventario firmados criptográficamente en toda la cartera de servidores PowerEdge, incluida la autoverificación segura, para que no tenga que preocuparse por la integridad de su hardware en el trayecto hacia el centro de datos.

Pilar 2: Confianza de los usuarios

Con iDRAC, los administradores de TI pueden implementar, actualizar y supervisar servidores PowerEdge en local o en remoto. Para mejorar la seguridad, iDRAC ofrece MFA mediante RSA SecureID, también con integraciones a través de Active Directory, integración de LDAP con SSO y con auditorías y control de acceso basado en funciones.

Pilar 3: Confianza en el transporte y la sesión

PowerEdge BMC (iDRAC) tiene un módulo de red dedicado y las opciones de shell seguro (SSH) y seguridad de capas de transporte (TLS) que se dedican a cifrar y autenticar los datos que se transfieren entre el servidor o navegador que ejecuta la interfaz de usuario web de iDRAC. iDRAC habilita la gestión remota y supervisa el sistema en caso de eventos críticos utilizando sensores en la placa base. Las alertas y los eventos de registro se envían cuando los parámetros exceden sus umbrales actuales.

Pilar 4: Confianza en el software

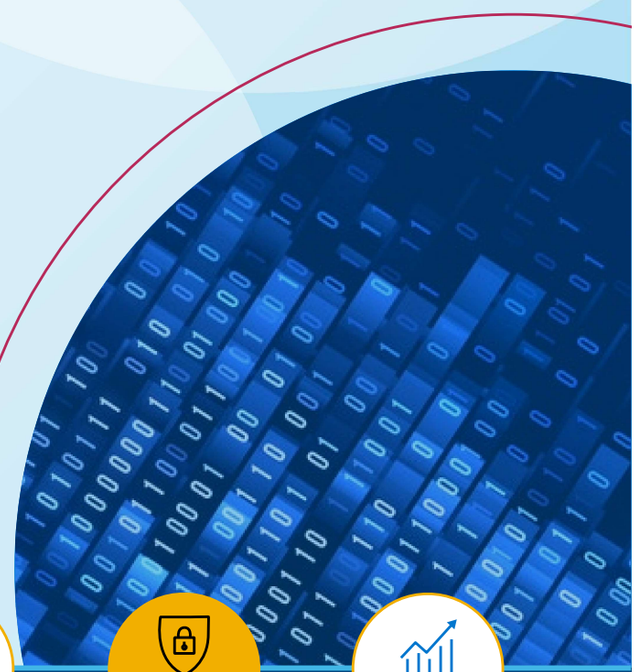
Realizamos pruebas de verificación, validación y seguridad proactivas en todo el ciclo de vida del software para proteger nuestro software y reducir la probabilidad de que se introduzcan vulnerabilidades de codificación o malware en él. El arranque integral verificado incluye imágenes de BIOS y firmware firmadas, lo que garantiza que el código no autorizado no se ejecute en un servidor PowerEdge. Entre otras funciones ciberresilentes se incluyen la detección de desfases automatizada, las capacidades de arranque seguras de UEFI y la recuperación del BIOS y los sistemas operativos.

Pilar 5: Confianza de datos

SEKM colabora con unidades de cifrado automático para el cifrado basado en hardware, así como con una gestión de claves central ampliable que le ayude a implementar y supervisar claves de cifrado en ubicaciones remotas, incluso en la cloud. Esto proporciona protección contra el acceso no autorizado a discos duros 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 proteger los datos en uso en la CPU y la memoria, e incluye tecnologías de Intel (SGX, TME). Intel SGX proporciona aislamiento a nivel de la aplicación o de la función para minimizar el perímetro de confianza.

La combinación del cifrado de datos en reposo, la gestión de claves ampliable y la computación confidencial permite ofrecer los niveles de protección necesarios para responder a las amenazas cambiantes de hoy en día.



Pilar 6: Visibilidad y análisis

La capacidad para ver lo que está ocurriendo en su entorno es fundamental. Por ejemplo, la detección de desfases de firmware proporciona información en tiempo real del estado del firmware, incluidos los cambios no autorizados. Si se detectan cambios, el sistema se puede revertir a un estado seguro conocido. Además, los eventos de cambio se pueden seguir a través de registros y alertas automatizados, lo que servirá de apoyo a auditorías y análisis para evaluar el estado general del sistema.

Pilar 7: Automatización y coordinación

OpenManage Enterprise es una aplicación de monitorización y gestión de sistemas que ofrece una vista completa de los servidores PowerEdge, el almacenamiento interno y otros componentes. Incluye la detección de desviaciones para detectar cambios a partir de una plantilla de configuración definida por el usuario, crear alertas y registros para realizar un seguimiento del estado del sistema y permitir la corrección de configuraciones erróneas en función de las políticas configuradas anteriormente. OpenManage incluye reversión de firmware, actualizaciones centralizadas, renovación automática de certificados de capa de socket seguro (SSL) e implementaciones automatizadas para una configuración de seguridad coherente.

Recursos

Resumen de solución: OpenManage Secure Enterprise Key Manager

Modelos base: Understanding Confidential Computing with Trusted Execution Environments and Trusted Computing

Infografía Zero-trust architecture

Vídeo: Zero Trust

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

El aumento de la sofisticación y la cada vez mayor superficie de ataque de las amenazas exigen contar con un enfoque modernizado en lo que a ciberresiliencia respecta. Nuestra respuesta es ayudarle en la creación de una arquitectura de confianza cero con una serie de herramientas y tecnologías. Nuestro enfoque de seguridad habilita controles más granulares, empezando por el acceso y la autorización, y hasta los datos y la resiliencia del sistema y logra ofrecer, al mismo tiempo, una experiencia del usuario superior.

Con Dell Technologies e Intel como sus socios, obtendrá:

- Ciberresilencia probada en la que la seguridad está integrada, no se incorpora
- Simplicidad al equilibrar los objetivos del negocio y la productividad con la seguridad y la privacidad
- Una suite de hardware y software diseñada para proteger su infraestructura de TI y proporcionar, al mismo tiempo, confianza, control y escala para su posicionamiento frente a la seguridad
- Vigilancia continua para mantener un estado de seguridad sólido mediante una respuesta rápida a todo tipo de vulnerabilidades

Recursos

Página web sobre soluciones de seguridad

Servicios para la resiliencia de la empresa

Managed Detection and Response

Para obtener más información sobre los servidores PowerEdge ciberresilentes, visite Dell.com/Servers.

Suscríbase a nuestro popular podcast Power2Protect de Dell Technologies y manténgase al tanto de los últimos episodios sobre seguridad y ciberresiliencia.

DELL Technologies

intel