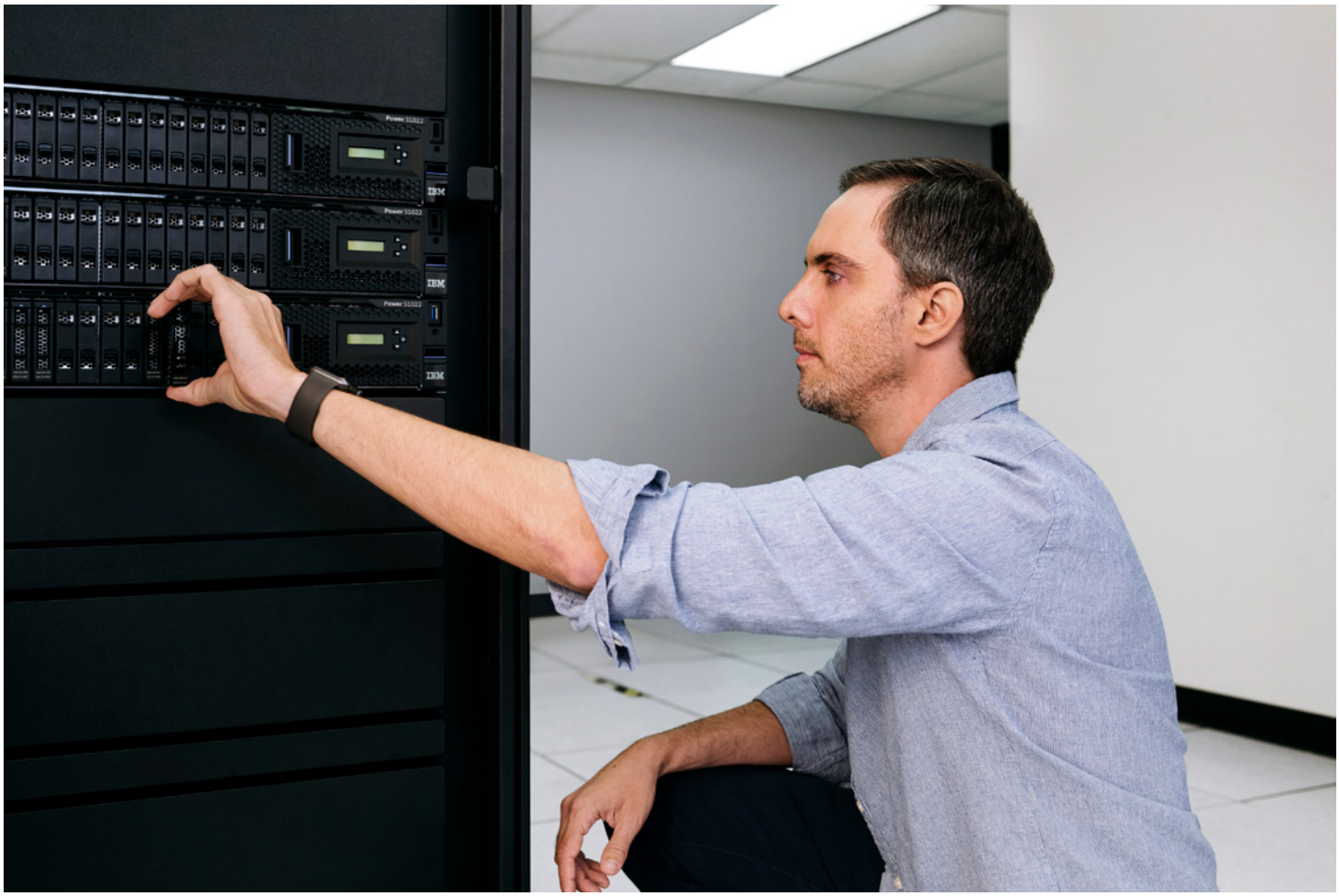
Un método de seguridad por capas con IBM Power

Infraestructura esencial para un método zero trust



Índice

TI empresarial en la era de los ciberataques sofisticados

El panorama actual de TI

Desde el inicio de la pandemia de COVID-19 se ha registrado una asombrosa cantidad de vulneraciones de datos demoledoras. El coste promedio de una vulneración de datos ahora es de 4,24 millones de dólares, un 10 % más que los 3,86 millones reportados el año pasado. Este es el aumento más grande que ha presenciado el sector en los últimos siete años[1], lo que hace que la seguridad sea una cuestión primordial. Mejorar su estrategia de seguridad y permitir que su empresa avance de forma rápida, segura y estable en este mundo constantemente conectado es el foco de muchos ejecutivos hoy en día, lo que se traduce en un aumento de los presupuestos de seguridad. No obstante, el aumento del gasto y de los cambios tecnológicos presenta nuevas complejidades y riesgos que siguen amenazando la seguridad de TI. Una de las preocupaciones principales de los profesionales de la seguridad es el creciente número de sofisticados vectores de ataque que continúan exponiendo más aspectos de las empresas actuales que nunca.

Las vulnerabilidades de hardware y firmware quizás no generaban mucha preocupación en tiempos no muy lejanos, pero ahora son los principales objetivos en el panorama de amenazas actual.

En muchos sentidos, los retos de ciberseguridad que su empresa debe superar en la actualidad pueden sintetizarse en dos verdades empíricas:

- La pila de TI está en expansión y los hackers están ampliando sus horizontes.
- Las organizaciones deben anticiparse a las amenazas futuras para proteger sus plataformas con el más alto nivel de seguridad para salvaguardar su infraestructura de cloud híbrido.

4,24 millones de dólares

El coste promedio de una vulneración de datos ahora es de **4,24 millones de dólares, un 10 % más** que los 3,86 millones reportados el año pasado.

Las realidades del panorama de amenazas actual

Un enfoque holístico

Las empresas dependen de sus sistemas de seguridad para prevenir amenazas actuales y futuras a la propiedad intelectual, la información corporativa confidencial, la privacidad de los datos de los clientes y las cargas de trabajo.

La forma en que los profesionales abordan estratégicamente la seguridad de TI es imprescindible para prevenir las vulneraciones de datos y los ciberataques. Estas vulnerabilidades de seguridad no solo generan tiempo de inactividad, sino que también son costosas para cualquier organización. Los ataques de ransomware representan la mayor amenaza y cuestan a las empresas 4,62 millones de dólares en promedio por ataque[1]. La integridad de la plataforma IBM® Power puede reducir el riesgo de ransomware implementando una solución de detección y respuesta de endpoints (EDR) y conceptos zero trust, como la autenticación multifactor continua (MFA).

La adopción de un método orientado a la empresa, al cumplimiento normativo o al aspecto monetario no puede por sí sola ofrecer una protección adecuada de los procesos empresariales contra el creciente número de riesgos de los sistemas de TI. Los métodos aislados pueden omitir los aspectos multidisciplinarios clave de una estrategia de seguridad integrada. La forma de proceder ideal implica tareas de planificación y evaluación para identificar los riesgos de las áreas clave relacionadas con la seguridad. La tecnología IBM Power y los sistemas basados en el procesador IBM® Power10 ofrecen un método por capas zero trust integral para su estrategia de seguridad a fin de garantizar que su organización esté protegida y cumpla con la normativa. Este método por capas incluye lo siguiente:

- Hardware
- Sistema operativo
- Firmware
- Tecnología IBM® PowerSC 2.0
- Hipervisor

Adoptar un método de seguridad holístico puede permitir a su organización satisfacer las exigencias de las amenazas que afectan al panorama de seguridad.

Los hackers se están volviendo más sofisticados

Cuanto más se aleje una organización de las limitaciones de los centros de datos locales tradicionales y migre a entornos multicloud o de cloud híbrido, más espacio les queda a los ciberatacantes para pensar con originalidad. La aplicación de privilegios mínimos y el aumento de controles basados en el perímetro ayudarán a gestionar la creciente cantidad de amenazas. Sus métodos del pasado ya no se limitan al ámbito de la red, lo que ha dado lugar a una ampliación de horizontes y a ataques más hábiles.

La seguridad es vital a medida que aumenta el acceso a los datos

Ahora los empleados pueden almacenar y acceder a los datos de una organización prácticamente desde cualquier lugar, entre servidores, entornos de cloud híbrido y numerosos dispositivos móviles y edge. Este entrecruzamiento inextricable de servidores y dispositivos es producto de la continua transformación y modernización digital. Como resultado, esta accesibilidad crea un sinfín de vectores de ataque listos para ser explotados.

Regulaciones más estrictas afectan los perfiles de riesgo

Los procesos que se usan para garantizar el cumplimiento normativo también pueden provocar una exposición involuntaria a riesgos. El reglamento general de protección de datos (GDPR) es solo una de las novedades recientes de esta tendencia creciente. Las entidades reguladoras están prestando mucha más atención a cómo usan los datos las organizaciones. Sin embargo, también añaden capas de complejidad a las operaciones empresariales diarias.

Los empleados son vulnerabilidades previsibles

Las credenciales comprometidas de los empleados son las culpables del 20 % de todas las vulnerabilidades de datos del último año[1]. Además de la información de registro, los fraudes por phishing y correos electrónicos que se han visto comprometidos son otras formas en que los empleados, sin saberlo, ponen en riesgo la información de la compañía. Su personal siempre planteará algún riesgo, sin importar qué controles de seguridad utilice o cómo de bien maneje las vulnerabilidades. En la era de la ciberdelincuencia es fundamental entrenar a los empleados sobre estas amenazas de seguridad comunes y contar con un sistema de notificación. El arduo trabajo que realiza para proteger los endpoints y cumplir con las normas podría ser irrelevante por un error o por un ataque malintencionado ingenioso.

Mientras tanto, muchas organizaciones intentan encontrar y retener personal de ciberseguridad competente, y se encuentran con una escasez de cualificación perpetua. Para combatir esta escasez, las organizaciones pueden implementar una gestión simplificada de la seguridad que automatiza las operaciones, la conformidad y la supervisión. Benefíciese de una seguridad de extremo a extremo diseñada para ofrecer protección con detección adicional de endpoints sin recursos adicionales.

El volumen, la variedad y la velocidad del panorama de ciberataques actual se multiplicarán a medida que la arquitectura de TI continúe evolucionando y adaptándose a los cambios de la tecnología, la cultura de trabajo y la conformidad. Eso significa que su estrategia de seguridad también debe evolucionar más allá del nivel de red.

Es fundamental contar con una estrategia zero trust

Un enfoque holístico

Implementar conceptos zero trust puede ayudar a las organizaciones a abordar la cuestión de seguridad en un entorno de TI que suele ser complejo. Los profesionales de TI tienen problemas de visibilidad y control en los entornos de cloud híbrido y multicloud. La metodología zero trust gestiona los riesgos usando una estrategia más exhaustiva que restringe los controles de acceso pero no afecta al rendimiento ni a la experiencia del usuario. Se puede mejorar la seguridad en cada nivel de su pila implementando soluciones de seguridad de varios proveedores externos. Sin embargo, este método empeora la complejidad ya existente e introduce incluso más vulnerabilidades y puntos de exposición en su red. Su mejor recurso es adoptar un método zero trust de varias capas. De este modo protege todos los datos y sistemas de su organización a la vez que también minimiza la complejidad. Teniendo eso en cuenta, IBM® Information Security Framework ayuda a garantizar que cada aspecto de la seguridad de TI pueda abordarse correctamente al usar un enfoque holístico de la seguridad empresarial.

IBM Information Security Framework se centra en lo siguiente:

1. Infraestructura: protéjase contra ataques sofisticados con información de los usuarios, el contenido y las aplicaciones.
2. Seguridad avanzada e investigación de amenazas: conozca las vulnerabilidades y las metodologías de ataque, y aplique esa información mediante tecnologías de protección.
3. Personas: gestione y amplíe la identidad empresarial en todos los dominios de seguridad con inteligencia de identidad exhaustiva.
4. Datos: proteja la privacidad y la integridad de los activos más fiables de su organización.
5. Aplicaciones: reduzca el coste del desarrollo de aplicaciones más seguras.
6. Inteligencia y análisis de seguridad: optimice la seguridad con más contexto, automatización e integración.
7. Filosofía zero trust: conecte y proteja a los usuarios correctos con los datos correctos a la vez que protege su organización.

Obtenga información adicional sobre IBM Security Framework (PDF, 25,2 MB) y cómo puede profundizar aún más.

Cómo la tecnología IBM Power protege la pila

Descubra IBM Power

Con la tecnología IBM Power puede aumentar la ciberresiliencia y gestionar los riesgos con seguridad exhaustiva de extremo a extremo que se integra en toda la pila, desde el procesador y el firmware al SO y los hipervisores, pasando por las aplicaciones y los recursos de red, hasta la gestión de los sistemas de seguridad.

Hardware, firmware e hipervisor

Aceleradores en chip
El chip del procesador IBM Power10 está diseñado para mejorar el rendimiento de la mitigación de los canales laterales y está equipado con un mejor aislamiento de la CPU de los procesadores de servicio. Este procesador de 7 nm está diseñado para ofrecer hasta el triple de capacidad, lo que genera un rendimiento mucho mejor[2].

Cifrado de extremo a extremo
El cifrado de memoria transparente de las soluciones IBM Power está diseñado para permitir una seguridad de extremo a extremo que cumple con los exigentes estándares de seguridad a los que se enfrentan las empresas hoy en día. También está diseñado para ofrecer aceleración criptográfica, criptografía postcuántica y cifrado homomórfico completo para proteger contra futuras amenazas. El cifrado acelerado del último modelo de sistema IBM Power ofrece un rendimiento criptográfico del estándar de cifrado avanzado (AES) 2,5 veces más rápido por núcleo que el de la tecnología IBM Power E980[3]. Las organizaciones pueden obtener beneficios del cifrado de memoria transparente sin configuración adicional de la gestión.

Software de EDR
El aumento de las amenazas externas hace que la seguridad de endpoints sea fundamental a la hora de proteger los datos de los clientes y los activos digitales. Al detectar cualquier amenaza potencial en el punto final, las organizaciones pueden

2,5 veces

El cifrado acelerado del último modelo de sistema IBM Power tiene **un rendimiento criptográfico del estándar de cifrado avanzado (AES) 2,5 veces más rápido por núcleo** que el de la tecnología IBM Power E980[3].

Habilitar principios como una autenticación multifactor y privilegios mínimos genera más protección al asegurar todas las API, los endpoints, los datos y los recursos de cloud híbrido.

actuar rápidamente y resolver los incidentes sin interferir en la continuidad empresarial. Un método integrado elimina las complicaciones y protege a su organización incluso de los ataques más peligrosos.

Principios zero trust
Las organizaciones están evolucionando hacia la adopción de principios zero trust para ayudar a gestionar estas amenazas crecientes. Habilitar principios como una autenticación multifactor y privilegios mínimos genera más protección al asegurar todas las API, los endpoints, los datos y los recursos de cloud híbrido.

El marco zero trust de IBM hace que este concepto cobre vida.

- **Reúna información**: comprenda a los usuarios, los datos y los recursos para crear las políticas de seguridad necesarias para garantizar una protección total.
- **Protección**: proteja a la organización validando el contexto y aplicando políticas de forma rápida y sistemática.
- **Detección y respuesta**: resuelva las infracciones de seguridad con mínimo impacto en las operaciones empresariales.
- **Analice y mejore**: mejore continuamente la posición de seguridad adaptando las políticas y las prácticas para tomar decisiones más informadas.

Al implementar principios zero trust las empresas pueden innovar y escalar con seguridad.

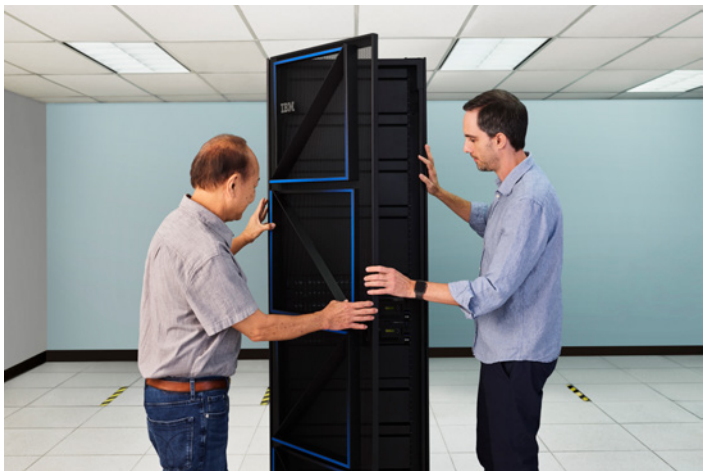
Inicio seguro en las soluciones IBM Power10
El inicio seguro está diseñado para proteger la integridad del sistema verificando y validando todos los componentes del firmware mediante firmas digitales. Todo el firmware publicado por IBM está firmado y verificado digitalmente como parte del proceso de inicio. Todos los sistemas IBM Power se ofrecen con un módulo de plataforma de confianza que acumula mediciones de todos los componentes de firmware cargados en un servidor, lo que permite su inspección y verificación remota.

Hipervisor empresarial IBM PowerVM
El hipervisor empresarial IBM® PowerVM tiene un historial de seguridad excelente en comparación con los principales competidores, de modo que puede proteger con confianza sus máquinas virtuales (VM) y entornos de cloud.

Sistema operativo

Los sistemas IBM Power ofrecen prestaciones de seguridad líderes para una amplia gama de sistemas operativos, como IBM® AIX, IBM i y Linux®. La tecnología de EDR para IBM Power puede ofrecer más seguridad para cargas de trabajo de VM, lo que garantiza una protección completa en cada endpoint dentro de la red. Para sistemas cuya seguridad depende de contraseñas, los sistemas operativos AIX y Linux utilizan la autenticación multifactor (MFA) de IBM PowerSC que requiere niveles adicionales de autenticación para todos los usuarios, lo cual protege del malware que descifra contraseñas. Las funciones varían según el SO, pero algunos ejemplos de estas prestaciones incluyen las siguientes capacidades:

- Asignar funciones administrativas típicamente reservadas para el usuario root sin comprometer la seguridad
- Cifrar los datos en el nivel de archivos mediante almacenes de claves individuales
- Obtener más control sobre los comandos y las funciones disponibles para los usuarios, junto con el control de a qué objetos pueden acceder
- Registrar el acceso a un objeto en el diario de auditoría de seguridad usando valores del sistema y los valores de auditoría de objetos para usuarios y objetos
- Aplicar cifrado a una unidad completa, cifrando primero un objeto y luego escribiéndolo en la forma cifrada
- Medir y verificar cada archivo antes de abrirlo para el usuario que lo solicita



Cargas de trabajo, VM y contenedores

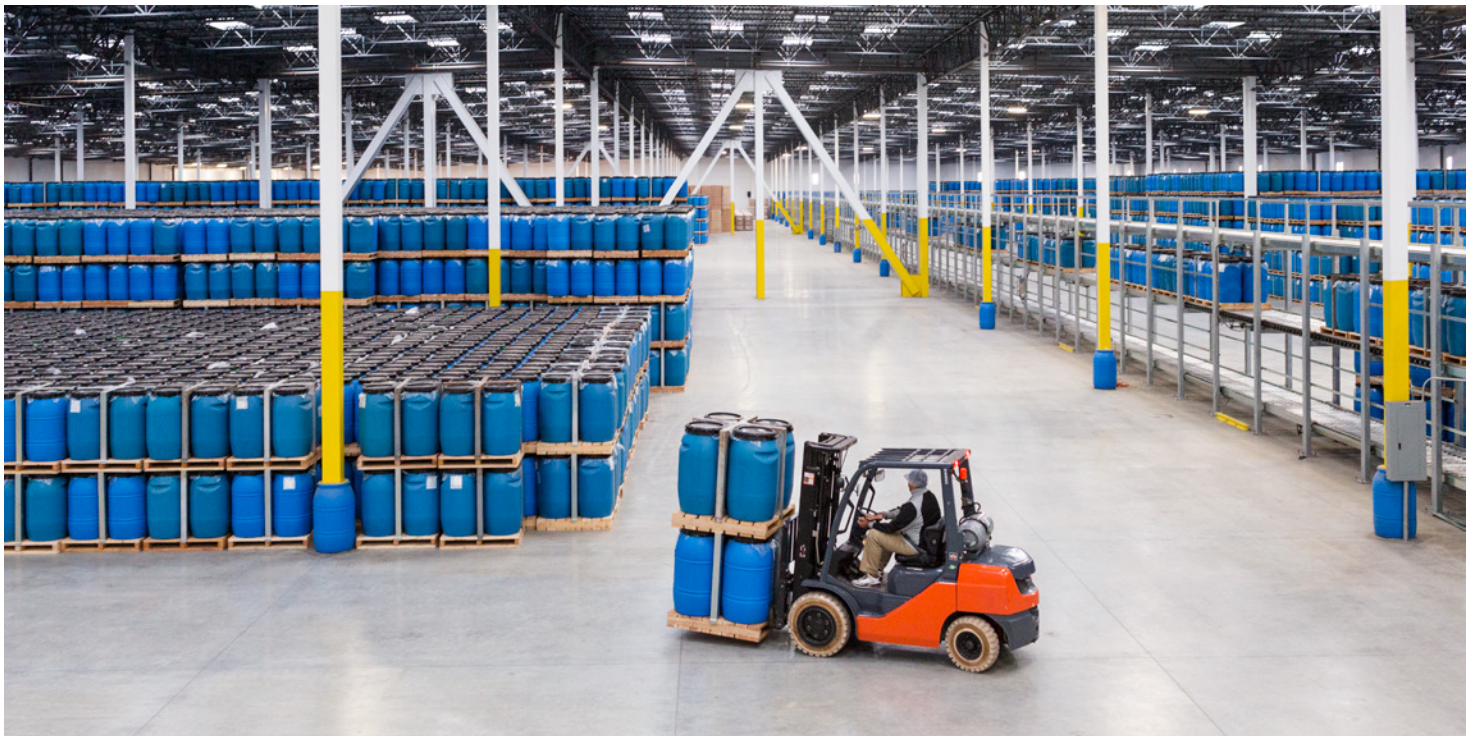
Las cargas de trabajo ya no están restringidas a los centros de datos locales; están en continuo movimiento a entornos de cloud híbrido y multicloud. Por ejemplo, muchas organizaciones están adoptando contenedores para implementar aplicaciones nuevas y existentes en infraestructuras híbridas.

Estos entornos y cargas de trabajo cada vez más dinámicos requieren prestaciones de seguridad con la misma versatilidad. Las soluciones IBM Power pueden satisfacer las necesidades de seguridad preservando la privacidad de las cargas de trabajo con aceleración de los algoritmos criptográficos, almacenamiento seguro de claves y compatibilidad con CPU para criptografía postcuántica y algoritmos criptográficos de cifrado homomórfico total (FHE).

Para abordar los requisitos de seguridad únicos de las implementaciones contenerizadas, IBM también se ha asociado con proveedores de software independientes (ISV) como Aqua Security, que utiliza la tecnología IBM Power y la Red Hat® OpenShift® Container Platform para ampliar la seguridad de los contenedores durante su ciclo de vida.

Los servidores IBM Power están diseñados para proteger los datos de centros locales hasta el cloud con cifrado de memoria de extremo a extremo y rendimiento criptográfico acelerado. Las políticas integradas para cargas de trabajo nativas en cloud, incluyendo VM, contenedores y funciones sin servidor, se han creado para dar soporte a los clientes de IBM Power y Red Hat OpenShift al integrar sus requisitos de seguridad y conformidad para la modernización de las aplicaciones.

Live Partition Mobility (LPM)
La tecnología IBM Power le permite proteger datos en movimiento. LPM protege las VM mediante cifrado cuando necesita migrar de un sistema a otro. Si ha virtualizado centros de datos locales, entornos de cloud híbrido o ambos, esta prestación es esencial.



Productos de seguridad integrados en las soluciones IBM Power

Tecnología IBM PowerSC 2.0

La tecnología IBM® PowerSC 2.0 es una cartera integrada que ofrece seguridad empresarial y conformidad en entornos de cloud y virtuales. Reside en la parte superior de su pila y proporciona una IU basada en web para gestionar las funciones de seguridad de la tecnología IBM Power a partir de las soluciones de menor nivel hacia arriba.

Con sus prestaciones de simplificación y automatización, la tecnología IBM PowerSC 2.0 puede reducir el tiempo, el coste y el riesgo al mejorar la supervisión y el cumplimiento de las normas. Esta solución puede dar soporte a procesos de auditoría y permite a los clientes obtener certificaciones de conformidad con más eficiencia. También puede reducir los riesgos de seguridad al aumentar la visibilidad en toda la pila.

Funciones de IBM PowerSC 2.0 Standard Edition

Tecnología de autenticación multifactor (MFA)
Las soluciones IBM PowerSC 2.0 integran ahora MFA. Esto simplifica la implementación de mecanismos de MFA siguiendo el principio zero trust de “nunca confiar, siempre verificar”. Este método es compatible con factores alternativos para que los usuarios inicien sesión con opciones de autenticación basadas en RSA SecurID y en certificados, como una tarjeta de acceso común (CAC) y tarjetas de verificación de identidad personal (PIV). La MFA de IBM PowerSC eleva los niveles de seguridad de los sistemas al solicitar factores de autenticación adicionales para los usuarios.

La tecnología IBM PowerSC 2.0 puede reducir el tiempo, el coste y el riesgo

Prestaciones de EDR
Las soluciones IBM PowerSC 2.0 introducen EDR para Linux en cargas de trabajo de IBM Power, ofreciendo las últimas prestaciones estándar del sector para la gestión de la seguridad de endpoints, incluyendo detección y prevención de intrusiones, inspección y análisis de registros, detección de anomalías y respuesta a incidentes.

Automatización de la conformidad
La familia IBM Power viene con perfiles predefinidos que son compatibles con una gran cantidad de estándares del sector. Puede personalizar estos perfiles y fusionarlos con reglas empresariales sin tener que tocar el lenguaje de marcado extensible (XML).

Conformidad en tiempo real
Detecta y le alerta cuando alguien abre o interactúa con archivos críticos para la seguridad.

Conexión de red de confianza
Le alerta cuando una VM no está en el nivel de parche prescrito. También le notifica cuando hay correcciones disponibles.

Inicio de confianza
Permite la inspección y la verificación remota de la integridad de todos los componentes de software que se ejecutan en particiones lógicas de AIX.

Firewall de confianza
Protege y redirige el tráfico interno de la red entre los sistemas operativos AIX, IBM i y Linux.

Registro de confianza
Crea registros de auditoría centralizados de los cuales se pueden hacer copias de seguridad y se pueden archivar y gestionar fácilmente.

Elaboración de informes preconfigurados y líneas temporales interactivas
IBM PowerSC Standard Edition admite auditorías con cinco informes preconfigurados. También tiene una línea temporal interactiva para ver la duración y los eventos de una VM.

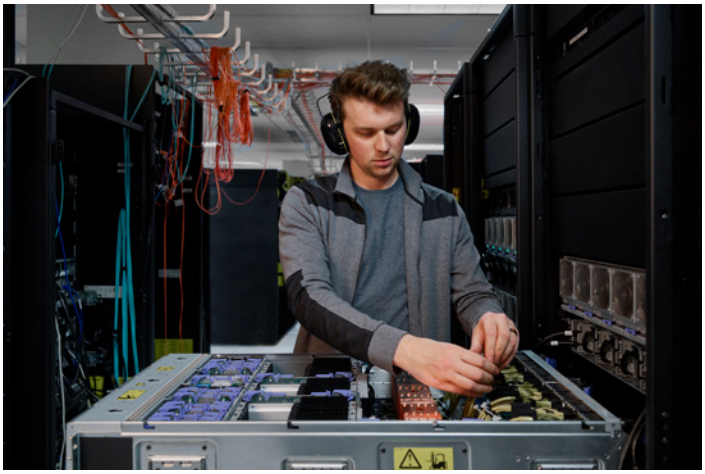
Obtenga más información sobre cómo simplificar la gestión de la seguridad y la conformidad de TI con IBM PowerSC en entornos virtualizados y de cloud.

El método más poderoso de seguridad es uno perfectamente integrado

Integración sin fisuras

A medida que los ciberdelincuentes continúan mejorando sus métodos y la evolución tecnológica introduce nuevas vulnerabilidades en las empresas de hoy, es fundamental integrar una solución de seguridad zero trust de varias capas que no añada complejidad a su organización. Las soluciones de IBM Power pueden proteger cada nivel de su pila desde el edge hasta el cloud y el núcleo con soluciones exhaustivas perfectamente integradas de un único proveedor. Trabajar con varios proveedores suma complejidades que pueden terminar por ser costosas, en más de un sentido. La tecnología IBM Power admite cifrado de extremo a extremo a nivel del procesador sin alterar el rendimiento. La integración de su infraestructura pone de relieve cada capa de la pila.

La seguridad de un único proveedor puede ofrecer ventajas naturales que simplifican y fortalecen su estrategia de seguridad. Con el respaldo de tres décadas de liderazgo en seguridad, la tecnología IBM Power trae consigo importantes asociaciones con otras organizaciones, dentro y fuera de IBM, que profundizan y amplían aún más su experiencia en seguridad. Estas asociaciones pueden permitir que la tecnología IBM Power acceda a una comunidad aún más grande de profesionales de seguridad y garantice que los problemas puedan identificarse rápidamente y abordarse con confianza. Además, con el respaldo de las unidades de negocio de IBM® Security e IBM® Research, junto con la cartera de PowerSC 2.0, los servidores Power10 pueden detener varias amenazas, incluyendo ataques internos, de arriba a abajo.



Programe una consulta para analizar el potencial de las soluciones de IBM Power

Póngase en contacto con nosotros →

Notas

1. Informe del coste de una vulneración de datos de 2021, IBM Security, julio de 2021 (PDF, 3,6 MB)
2. El rendimiento triplicado se basa en el análisis de ingeniería presilicio de entornos Integer, Enterprise y Floating Point en un servidor de socket dual POWER10 que se ofrece con 2 módulos de 30 núcleos en comparación con el servidor de socket dual POWER9 que se ofrece con 2 módulos de 12 núcleos; ambos módulos tienen el mismo nivel de energía. La mejora de inferencia entre 10 y 20 veces se basa en el análisis de ingeniería presilicio de varias cargas de trabajo (Linpack. Resnet-50 FP32, Resnet-50 Bfloat16 y Resnet-50 INT8) en un servidor de socket dual POWER10 que se ofrece con 2 módulos de 30 núcleos en comparación con el servidor de socket dual POWER9 que se ofrece con 2 módulos de 12 núcleos.
3. AES-256 en los dos modos GCM y XTS funciona alrededor de 2,5 veces más rápido por núcleo al comparar IBM Power10 E1080 (módulos de 15 núcleos) con IBM POWER9 E980 (módulos de 12 núcleos) de acuerdo con las medidas preliminares obtenidas en RHEL Linux 8.4 y la biblioteca OpenSSL 1.1.1g

IBM España, S.A.
Santa Hortensia, 26-28
28002 Madrid

Producido en los
Estados Unidos de América
Junio de 2022