IBM **Power Systems**

Un enfoque multicapa de la seguridad con POWER9

Asegure y optimice de manera fluida su infraestructura de TI

TI empresarial en la era de los ciberataques sofisticados

Filtraciones de datos altamente publicitadas y devastadoras han puesto actualmente a la seguridad en el primer plano de la atención de muchos ejecutivos. Esto ha tenido como resultado que los presupuestos para la seguridad hayan crecido en las organizaciones. Pero, al menos en parte, el incremento en el gasto y el cambio tecnológico han introducido nuevas complejidades y riesgos que amenazan a la seguridad de la TI. Una encuesta de Forrester en 2019 orientada a los profesionales de la seguridad encontró que “menos de una cuarta parte” de ellos están “completamente satisfechos con sus carteras de seguridad para que les brinden apoyo desarrollando capacidades de inteligencia avanzada contra amenazas; aumentando la productividad del personal de seguridad; extrayendo perspectivas de los datos; e impulsando eficiencias.”[1]

Una de las principales inquietudes entre los profesionales de la seguridad es el creciente número y sofisticación de los ataques, los cuales exponen más aspectos de las empresas de hoy que nunca antes. Las vulnerabilidades en los niveles del hardware y el firmware pueden no haber sido puntos de gran inquietud en un pasado no muy lejano; ahora, sin embargo, estos se hallan entre los objetivos principales.

Las amenazas, mientras tanto, seguirán multiplicándose a medida que las arquitecturas de la TI evolucionan. En muchos aspectos, los desafíos de ciberseguridad que su empresa debe superar hoy se pueden resumir en dos verdades empíricas: La pila de TI se está expandiendo y —como resultado directo— los hackers están expandiendo sus horizontes.

Las realidades del actual panorama de amenazas

Las organizaciones dependen hoy de sus sistemas de seguridad para prevenir amenazas a la propiedad intelectual, información corporativa sensible, información personal sensible, y privacidad. Cómo enfocan estratégicamente la seguridad de la TI es una cuestión imperativa.

A menudo, esto se consigue adoptando un enfoque regido por el comercio, el cumplimiento, o monetario. Si bien este enfoque posee valor, por sí solo no proporciona una protección adecuada de los procesos empresariales contra el número cada vez mayor de riesgos para los sistemas de TI. Posiblemente también pasa por alto aspectos interdisciplinares clave.

El curso de acción ideal implica planificación y evaluación para identificar riesgos a través de áreas clave relacionadas con la seguridad. Los sistemas IBM® Power® y el procesador POWER9™ ofrecen un enfoque holístico multicapa para su estrategia de seguridad, para asegurar que su organización esté segura y cumpla con todas las normativas. Este enfoque multicapa incluye

- Hardware
- Firmware
- Hipervisor
- Sistema operativo
- PowerSC

Adoptar un enfoque holístico de la seguridad hace posible que su organización satisfaga las exigencias de cuatro realidades que afectan actualmente al panorama de la seguridad.

Los hackers se están volviendo más sofisticados. Cuanto más se sale una organización de las limitaciones de los tradicionales centros de datos in-situ, tanto más espacio tienen los ciberatacantes que pensar de una forma no convencional. Sus métodos ya no están confinados al nivel de red, lo que conduce a unos horizontes más amplios y ataques más capaces.

Más empresas se están dirigiendo desde dispositivos móviles y periféricos. Los datos internos de una organización pueden ahora almacenarse y los empleados acceder a ellos desde prácticamente cualquier lugar—a lo largo de servidores, entornos de nube híbrida y numerosos dispositivos móviles y periféricos. Este inextricable entrelazado de servidor y dispositivo es el producto secundario de la transformación digital en curso,—pero crea un vector de ataque completamente nuevo listo para ser explotado.

Las normativas más estrictas están afectando a los perfiles de riesgo.
Los procesos que se están poniendo en vigor para asegurar el cumplimiento normativo también pueden conducir a una exposición a riesgos no deseada. Y el GDPR de la UE es tan solo un desarrollo reciente de una tendencia en crecimiento: Las entidades de gobierno están prestando mayor atención a cómo su organización utiliza los datos. Pero también añaden capas de complejidad a las operaciones diarias de su empresa.

Los empleados son vulnerabilidades esperando a que sucedan.
Su personal laboral siempre presenta algún nivel de riesgo, con independencia de los controles de seguridad que usted instaure, o de cómo se ocupe de las vulnerabilidades. El trabajo duro que usted dedica a asegurar los puntos finales y ceñirse al cumplimiento puede quedar obsoleto por un error no intencionado o un inteligente ataque malicioso. Mientras tanto, muchas organizaciones luchan por encontrar y retener personal de seguridad competente, y se encuentran atrapadas con una escasez perpetua de habilidades.

El volumen, la variedad y la velocidad de los ciberataques de hoy solo pueden multiplicarse a medida que las arquitecturas de TI siguen evolucionando y adaptándose a las cambiantes mareas de la tecnología, la cultura laboral y el cumplimiento. Y eso significa que su estrategia de seguridad debe también evolucionar para ir más allá del nivel de red.

Es necesario un enfoque holístico multicapa de la seguridad

Crear y desarrollar seguridad en cada capa de su pila puede lograrse implementando distintas soluciones de seguridad de terceros. Sin embargo, este enfoque se suma a la complejidad ya existente, e introduce aun más vulnerabilidades y puntos de exposición a su red. El mejor recurso es adoptar un enfoque holístico y multicapa, uno que asegure todos los datos y sistemas de su organización minimizando al mismo tiempo la complejidad.

Teniendo esto presente, IBM® creó el IBM Security Framework (Marco de Seguridad de IBM) para ayudar a asegurar que cada aspecto de la seguridad de la TI se aborde de una manera adecuada cuando se use un enfoque holístico de la seguridad orientada a la empresa.

El IBM Security Framework se centra en:

1. **Infraestructura**—Protéjase contra ataques sofisticados con perspectiva de los usuarios, el contenido y las aplicaciones.
2. **Investigación avanzada de seguridad y amenazas**—Obtenga conocimiento de las vulnerabilidades y las metodologías de los ataques y aplique esas perspectivas a través de tecnologías de protección.
3. **Personas**—Gestione y extienda la identidad empresarial a lo largo de dominios de seguridad con inteligencia integral de la identidad.
4. **Datos**—Asegure la privacidad y la integridad de los activos en los que más confía su organización.
5. **Aplicaciones**—Reduzca el costo de desarrollar aplicaciones más seguras.
6. **Inteligencia y analítica de seguridad**—Optimice la seguridad con contexto adicional, automatización e integración.

Conozca más acerca del IBM Security Framework y cómo usted puede examinar aun más a fondo con el IBM Security Blueprint.

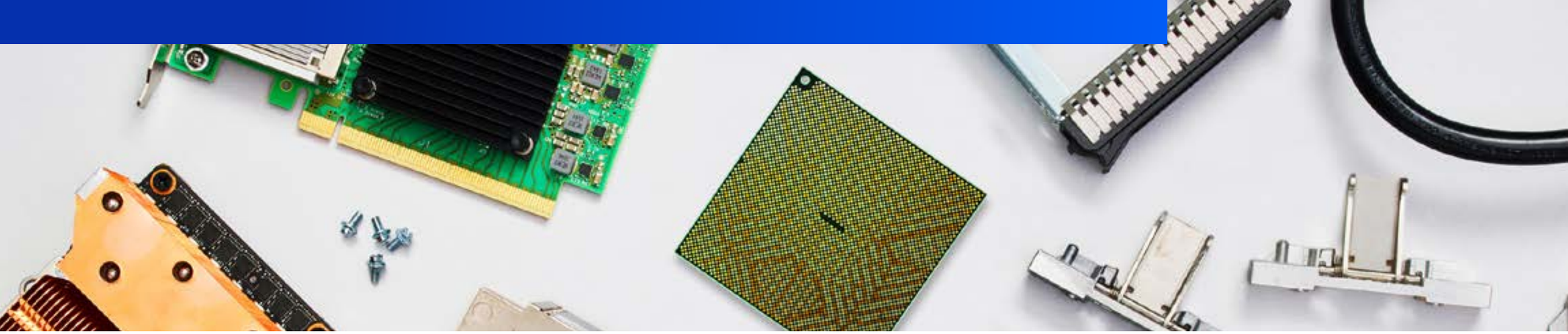
Cómo IBM Power Systems y POWER9 aseguran la pila

Con IBM Power Systems, usted obtiene seguridad integral de punta a punta que se integra estrechamente en la pila al completo—desde el procesador y el firmware hasta el SO y los hipervisores, las aplicaciones y los recursos de red, hasta llegar a la gestión del sistema de seguridad.

Hardware, firmware e hipervisor

24 motores criptográficos

El procesador POWER9 contiene dos veces más motores criptográficos que su predecesor, el POWER8®. Usted puede cifrar datos en reposo o en movimiento al doble de velocidad, o más, a lo largo de todas las capas de la pila.



Aceleradores en chip

El POWER9 cuenta con aceleradores en chip que comprimen y descomprimen archivos GZIP mucho más rápido que el software. Usted puede comprimir y cifrar rápidamente VMs (máquinas virtuales) completas y moverlas de manera segura a lo largo de la red.

Arranque seguro en POWER9

El arranque seguro protege la integridad del sistema verificando y validando todos los componentes del firmware mediante firmas digitales. Todo el firmware que IBM pone en el mercado está firmado digitalmente y es verificable. Usted también puede instalar su propio firmware y reemplazar la jerarquía de claves públicas necesarias para la verificación.

Arranque confiable y Trusted Platform Module (Módulo de Plataforma Confiable, TPM)

La función de arranque confiable de POWER9 hace posible la inspección y verificación remota (atestación) de todos los componentes del firmware en su servidor. La función de arranque confiable usa el TPM, que sirve como la Root of Trust (Raíz de Confianza, RoT) para medir la pila de software. El mismo TPM firma la verificación, de manera que usted sabe que el firmware no ha sido alterado en modo alguno.

Hipervisor empresarial IBM PowerVM

IBM PowerVM® tiene un excelente historial de seguridad en comparación con sus competidores principales, de manera que usted puede asegurar confidencialmente sus máquinas virtuales (VMs) y entornos de nube.

Sistema operativo

IBM Power Systems ofrece capacidades de seguridad de avanzada para una amplia gama de sistemas operativos como IBM AIX®, IBM i y Linux®. Las características varían dependiendo del SO, pero entre los ejemplos de estas capacidades se incluye poder:

- Asignar funciones administrativas reservadas normalmente para el usuario raíz sin comprometer la seguridad
- Cifrar datos a nivel de archivo a través de repositorios de claves
- Obtener un mayor control de los comandos y funciones disponibles para los usuarios, junto con control sobre los objetos a los que pueden acceder
- Conceder acceso a un objeto en el diario de auditoría de seguridad usando valores del sistema y los valores de auditoría del objeto para los usuarios y objetos
- Extender el cifrado a un disco entero, cifrando primero un objeto y luego escribiéndolo en la forma cifrada
- Medir y verificar cada archivo antes de que se ejecute o abra para el usuario que lo solicita

Cargas de trabajo, VMs y contenedores

Las cargas de trabajo ya no están restringidas a centros de datos in-situ; se están moviendo continuamente a entornos virtualizados y de nube. Esto significa que muchas organizaciones están adoptando contenedores para desplegar aplicaciones nuevas y existentes a lo largo de infraestructuras híbridas. Estos entornos y cargas de trabajo cada vez más dinámicos requieren capacidades de seguridad igualmente versátiles.

Live Partition Mobility (Movilidad de Partición en Vivo, LPM)

IBM Power Systems le permite asegurar sus datos estando en movimiento. LPM protege VMs mediante cifrado cuando usted necesita migrar de un sistema a otro. Si usted tiene centros de datos in-situ virtualizados y/o entornos de nube híbrida, esta capacidad es crucial.

Servicio de Ejecución Protegida

El Protected Execution Facility (Servicio de Ejecución Protegida) es un ejemplo de cómo IBM Power Systems protege este nivel de la pila. Se trata de una característica de POWER9 que cifra y ejecuta sus VMs en memoria segura, lo que significa que un hipervisor comprometido no tendrá acceso. Adicionalmente, en un entorno de nube, administradores o personal interno malicioso con acceso a la VM no tendrán acceso a las cargas de trabajo que se estén ejecutando en la memoria segura. El proceso de cifrado solo sucede en un sistema verificado.

Productos de seguridad integrados en IBM Power Systems

IBM PowerSC es una cartera integrada que ofrece cumplimiento y seguridad de grado empresarial en entornos de nube y virtuales. Reside en la parte superior de su pila proporcionando al mismo tiempo un interfaz de usuario basado en web para administrar las características de seguridad de IBM Power Systems que residen desde el nivel más bajo hasta el más alto.

IBM PowerSC reduce el tiempo, el costo y el riesgo

Con sus capacidades de simplificación y automatización, IBM PowerSC ayuda a ahorrar tiempo y reducir costos agilizando los procesos de auditoría y cumplimiento. También reduce los riesgos de seguridad aumentando la visibilidad en toda la pila.

Características de IBM PowerSC Standard Edition

Automatización del cumplimiento

IBM PowerSC viene con perfiles precargados con soporte para una miríada de estándares del sector. Usted puede personalizar estos perfiles y mezclarlos con normas empresariales sin tener que tocar XML.

Cumplimiento en tiempo real

Detecta y le alerta a usted cuando alguien abre o interactúa con archivos críticos para la seguridad.

Trusted Network Connect (Conexión de Red de Confianza, TNC)

Le alerta cuando una VM no está al nivel de parche prescrito. También le notifica cuando hay correcciones disponibles.

Arranque confiable

Hace posible la inspección y verificación remota de todos los componentes del firmware que se están ejecutando en su servidor.

Firewall confiable

Protege y dirige el tráfico de red interno entre los sistemas operativos AIX®, IBM i y Linux.

Registro confiable

Crea registros de auditoría centralizados, fáciles de crear copias de seguridad, archivar y administrar.

Cronograma interactivo y de reporte preconfigurado

El IBM PowerSC Standard Edition brinda apoyo a la auditoría con cinco reportes preconfigurados. Usted también tiene un cronograma interactivo para ver la actividad y sucesos de una VM.

Para conocer más sobre las muchas características de IBM PowerSC, consulte el siguiente Redbook de IBM, “Simplifique la gestión de la seguridad y el cumplimiento con IBM PowerSC en entornos de nube y virtualizados.”

El enfoque más poderoso a la seguridad es uno agilizado

A medida que las capacidades de los hackers se vuelven más sofisticadas y la evolución tecnológica introduce nuevas vulnerabilidades en las empresas de hoy, integrar una solución de seguridad holística multicapa que no sume a su complejidad organizacional es clave. IBM Power Systems protege cada nivel de su pila con las soluciones exhaustivas y estrechamente integradas de un único proveedor. Una estrategia de seguridad que se basa en una multitud de componentes de múltiples proveedores introduce complejidades que pueden, en última instancia, demostrarse costosas en más de una manera.

La seguridad de un único proveedor proporciona ventajas naturales que simplifican y refuerzan su estrategia de seguridad. Desarrollándose a partir de tres décadas de liderazgo en el campo de la seguridad, IBM Power Systems trae consigo amplias asociaciones con otras organizaciones dentro y fuera de IBM que profundizan y amplían aun más su experiencia y conocimiento en materia de seguridad.

Estas asociaciones hacen posible que IBM Power Systems obtenga provecho de una comunidad aun más grande de profesionales de la seguridad y garantizan que los problemas puedan identificarse rápidamente y abordarse con confianza. Y con el respaldo de las unidades comerciales IBM Security e™ IBM Research, junto con la cartera PowerSC, los servidores POWER9 desbaratan múltiples amenazas, incluyendo ataques de personas infiltradas, desde el nivel más alto hasta el más bajo.

Agilice su seguridad en la pila al completo con un enfoque holístico y multicapa, y mantenga la seguridad de su empresa.

Para saber más acerca de cómo los servidores POWER9 pueden ayudar a asegurar su infraestructura, contacte con su representante de IBM o IBM Business Partner®.

1. "Reporte sobre la Complejidad en la Ciberseguridad 2019 Cómo reducir la complejidad produce mejores resultados de seguridad," Forrester Research, Inc., Mayo de 2019

IBM Systems, 11501 Burnet Road, Austin, Texas 78758

33028633ESES-00