ARTÍCULO TÉCNICO DE VERTIV

¿Cómo pueden los equipos de ciberseguridad y de TI trabajar hombro a hombro para fortalecer la seguridad en la gestión de los servidores?

El Ecosistema Vertiv™ Avocent® ADX aporta claridad y control para reducir los riesgos de seguridad en los servidores

La adaptación al cambio

Los últimos dos años han puesto muchísima presión en los equipos de TI en las compañías y las empresas pequeñas y medianas (PYMES) alrededor del mundo. Sin embargo, se han movilizado para facilitar una fuerza laboral híbrida y desarrollar una plataforma digital para apoyar el crecimiento a largo plazo. Asimismo, los equipos de seguridad han hecho frente a una avalancha de ataques a medida que los criminales cibernéticos redirigieron su atención de las redes a las terminales, las cuales son más fáciles de penetrar.

Sin embargo, mantener la estabilidad empresarial en medio de las turbulencias del mercado y los constantes retrocesos ha tenido graves consecuencias. Tanto los equipos de seguridad como de TI están experimentando una menor visibilidad de las condiciones y el rendimiento de la red a la vez que se enfrentan a una creciente demanda de servicios. Estos equipos tienen la responsabilidad de mantener la seguridad y el rendimiento de las redes distribuidas, y rediseñar procesos para un mundo de confianza cero. Como resultado, los equipos de ciberseguridad y de redes de TI necesitan colaborar de forma más intensiva para mejorar la seguridad en la gestión de los servidores en todas las redes colaborativas. La buena noticia es que el 89% de los gerentes de redes indica estar haciéndolo. Un 37% de las organizaciones tiene equipos de gestión de seguridad y redes totalmente convergentes, mientras que el 26% mantiene equipos separados, pero cuenta con herramientas y procesos integrados.[1]

Los servidores son los burros de carga de la industria, ya que ofrecen una valiosa capacidad de procesamiento informático para los caudales de información que producen las compañías, los usuarios y sus clientes. Junto con otros dispositivos de red, los servidores alimentan los servicios digitales y facilitan las experiencias digitales que los clientes buscan. Por lo tanto, mantener un funcionamiento y un rendimiento continuos es crítico para la TI y la seguridad. Además, los atacantes cibernéticos que acceden a los servidores pueden manipular, controlar y sustraer o bloquear el acceso a los datos, lo cual puede paralizar las operaciones comerciales de una compañía y afectar a los clientes. El ataque de ransomware a Colonial Pipeline Co., que ocasionó escasez de combustibles en la costa este de EE. UU., es un ejemplo del impacto y el alcance que pueden tener estos ataques.[2]

Los desafíos y las oportunidades de la gestión de servidores por parte de los equipos de seguridad y de TI

Entonces, ¿a qué problemas se enfrentan los equipos de seguridad y de TI a la hora de intentar proteger los servidores ubicados en los centros de datos empresariales, las instalaciones de coubicaciones y los sitios de borde, entre otras ubicaciones?

Las empresas digitales crean la expansión digital: hoy, casi todo es digital: los procesos laborales, las interacciones con los clientes, el desarrollo de productos y las operaciones de la cadena de suministros. Una encuesta realizada a profesionales de TI reveló que el 47% espera un cambio permanente, mientras que el 13% indicó que su empresa se había transformado completamente debido a los eventos recientes.[3]

Las compañías han aumentado las inversiones en la nube y el borde para mantenerse al día, lo cual ha creado una expansión de dispositivos de TI. Los servidores ubicados en sitios de borde remotos podrían no ser gestionados tan proactivamente como aquellos en el núcleo, pero siguen presentando considerables riesgos de seguridad. Los equipos de seguridad y de TI necesitan más que nunca una visualización centralizada del rendimiento de la red. Además, necesitan aprovechar la gestión en banda y fuera de banda y el acceso remoto seguro para mantener las redes actualizadas y en funcionamiento, libres de problemas de rendimiento.

Cuando más tecnología significa más conjuntos de herramientas: como resultado del crecimiento digital, los equipos de seguridad y de TI actualmente gestionan un mayor número de servidores y dispositivos de red de una gran variedad de proveedores. Esto se traduce en más conjuntos de herramientas, más políticas y una mayor complejidad a menos que la TI consolide las labores de gestión de red en una sola herramienta y comparta los datos holísticos de forma segura. Aunque TI ha dado importantes pasos para reducir la complejidad de la gestión, el 64% de las empresas sigue utilizando 4-10 herramientas para gestionar su red.[4] Muchos desean una mayor consolidación. La buena noticia es que TI puede gestionar más dispositivos de TI que antes en una plataforma centralizada. Además, la seguridad se beneficia de poder integrar el monitoreo físico, ambiental y de dispositivos en una sola pantalla.

La centralización de la gestión de los dispositivos de TI con una sola plataforma

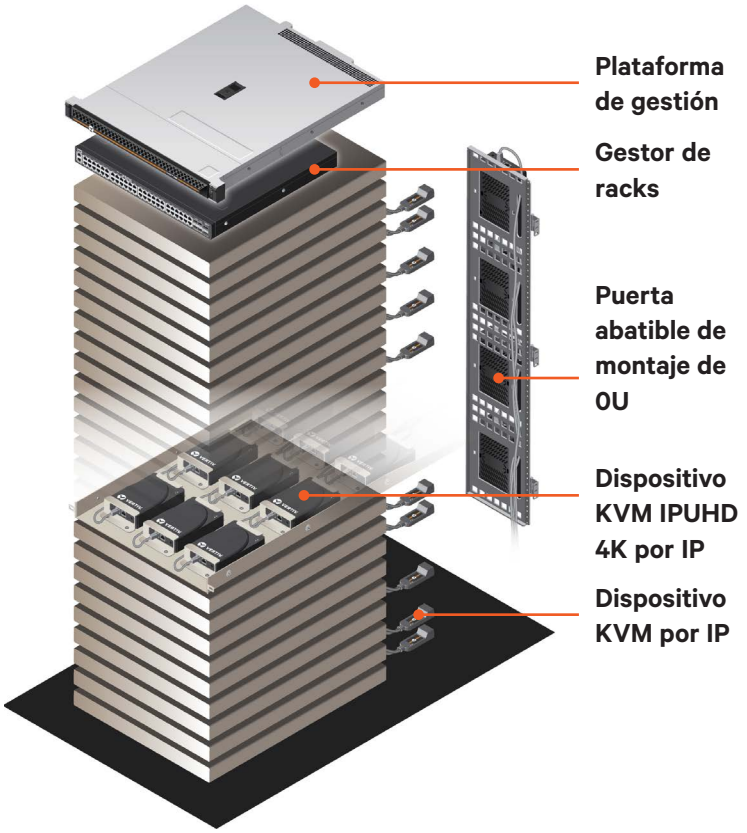
El Ecosistema Vertiv™ Avocent® ADX ayuda a los equipos de ciberseguridad y de TI a centralizar el monitoreo y la gestión, para mejorar la seguridad de los servidores y otros dispositivos de red.

Servidores: producción, desarrollo y servidores de prueba; servidores no esenciales.

Otros dispositivos de TI: escritorios administrativos, dispositivos de almacenamiento, equipo de red, unidades de distribución de energía en racks (rPDU), unidades de suministro ininterrumpido de energía (UPS) y sensores, cerraduras en puertas de racks, cámaras y mucho más.

Seguridad carece de visibilidad de las políticas:
Los equipos de seguridad desean gestionar las condiciones de todos los servidores, sin importar donde se ubiquen. Sin embargo, debido a que estos equipos utilizan múltiples proveedores y conjuntos de herramientas, los dispositivos probablemente cuentan con políticas incoherentes y podrían no ofrecer una visibilidad y un control detallados. Esto no funciona en un mundo de amenazas y riesgos constantes. Los equipos de seguridad querrán asociarse con TI para definir y gestionar privilegios de acceso específicos con base en las funciones y labores a realizar. Algunos ejemplos incluyen controlar quién pueden actualizar el firmware, adjuntar medios virtuales a los dispositivos y reiniciar los servidores. De este modo, los equipos pueden reducir los privilegios de acceso excesivos, los cuales pueden ser aprovechados por los criminales cibernéticos a través de devastadores ataques.

TI necesita coordinar la gestión de firmware:
La automatización de las actualizaciones de firmware es cada vez más importante ya que los criminales cibernéticos se centran en el núcleo, la memoria y otras vulnerabilidades en servidores y otros dispositivos. Por ejemplo, los atacantes pueden usar malware como Trickbot para escanear los dispositivos en búsqueda de vulnerabilidades y leer, escribir o borrar el firmware de la BIOS/UEFI.[5] Otra amenaza, el nuevo rootkit iLOBleed, va dirigido a servidores empresariales HP, manipula el firmware y borra los datos de los sistemas.[6] Además, los equipos de seguridad indican que siguen gastando un 41% de su tiempo en parches de firmware manuales que podrían automatizarse.[7] La automatización de estas actualizaciones elimina los riesgos creados por firmware desactualizados y les concede tiempo a los equipos de seguridad y de TI para las labores estratégicas.



Según un informe de Microsoft, "Más del 80% de las empresas han experimentado al menos un ataque de firmware en los últimos dos años. Sin embargo, solo el 29% de los presupuestos en seguridad de estas compañías se enfocan en proteger el firmware."[8]

Ofrecer una mayor funcionalidad: los equipos de seguridad y de TI podrían usar plataformas separadas de automatización y monitoreo de red. Sin embargo, ¿por qué no converger estas capacidades? Tanto los equipos de seguridad como de TI se benefician de obtener una visualización integral del rendimiento y compartir y actuar con base en los datos en tiempo real. Esto incluye la capacidad de conceder privilegios de acceso de forma conjunta, revisar anomalías, planificar la respuesta ante incidentes e implementar buenas prácticas como la automatización.

Ecosistema Vertiv™ Avocent® ADX - Una plataforma centralizada para la colaboración entre los equipos de seguridad y de TI

Por lo tanto, los desafíos de gestión y seguridad son cada vez mayores. Sin embargo, la buena noticia es que los equipos de seguridad y de TI pueden trabajar en estrecha colaboración para hacer frente a estos problemas y fortalecer la seguridad, lo cual contribuye con los objetivos de sus compañías de crear arquitecturas de confianza cero. Para ello deben implementar y compartir una plataforma de gestión centralizada y adoptar una hoja de ruta sencilla de 4 pasos.

El Ecosistema Vertiv™ Avocent® ADX les ofrece a los equipos de seguridad y de TI la plataforma centralizada que necesitan para mejorar la seguridad y la gestión de los servidores. Ofrece una visualización única, herramientas de gestión y capacidades de automatización que ambos equipos necesitan para aportar claridad y control a la seguridad y la red. El Ecosistema Avocent ADX incluye:

- Una plataforma de gestión para la automatización, el acceso remoto y el control seguros
- Un gestor de racks que se conecta físicamente con los módulos de interfaz o directamente con los procesadores de servicio, las rPDU o el equipo de red
- Módulos de interfaz que se conectan con los dispositivos de agregación y objetivos finales

El Ecosistema Avocent ADX, basado en una arquitectura digital común con una plataforma abierta y API, permite que hasta 100 usuarios puedan monitorear y gestionar los dispositivos de forma simultánea. La seguridad multinivel garantiza que solo los usuarios autorizados tendrán acceso a los dispositivos y privilegios que necesitan para cumplir con sus labores.

Estos usuarios cuentan con opciones sobre cómo acceder y gestionar los dispositivos. Los administradores de seguridad y de TI pueden usar consolas seriales y dispositivos KVM Vertiv™ Avocent® ADX IPIQ 4K para gestionar físicamente los dispositivos empresariales conectados al gestor de racks. Como alternativa, pueden utilizar dispositivos KVM Vertiv™ Avocent® ADX IPIQ por IP como una solución rápida, de bajo costo y de cero U para gestionar los dispositivos sin la necesidad del gestor de racks.

Vertiv™ Avocent® Core Insight: estandarice la gestión de TI con firmare de código abierto. Los equipos de TI buscan estandarizar la gestión de los dispositivos por medio de eliminar las brechas de seguridad y aumentar la calidad del código y la salida al mercado. Vertiv™ Avocent® Core Insight (ACI) ofrece una implementación especial para empresas del proyecto OpenBMC para controladores de gestión de placa base (BMC). Los ingenieros pueden usar el firmware ACI para crear avanzados sistemas de gestión integrados, escalables y seguros para cualquier dispositivo.

Los desarrolladores cuentan con varias opciones y pueden elegir entre:

- Firmware de código abierto listos para desarrollarse
- Avanzados módulos de aplicaciones ACI que pueden agregarse a una pila existente
- Un servicio de subscripción, que ofrezca un paquete ACI especial para empresas, junto con acceso total de código fuente, herramientas y soporte superior

Vertiv ACI brinda una seguridad superior del tiempo operativo, lo cual elimina todo un vector de vulnerabilidades basadas en la memoria.

Implemente hoy mismo esta hoja de ruta para fortalecer la seguridad de los servidores

Ahora que los equipos de seguridad y de TI pueden visualizar y compartir datos y ejecutar procesos juntos, ¿cómo deberían proceder? Esta es una hoja de ruta sencilla para mejorar la seguridad del servidor.

- **Conectar los dispositivos físicamente para una mayor seguridad:**
  TI puede conectar dispositivos con el gestor de racks Avocent ADX y ocultarlos de la visualización y el acceso de red al colocarlos en una red privada. De esta manera, la red privada es únicamente accesible para individuos autorizados por medio de una interfaz de gestión de racks, lo cual disminuye el riesgo humano o el sabotaje interno.
- **Utilizar protocolos para comunicarse con los dispositivos:**
  Los equipos de seguridad y de TI no siempre pueden controlar la seguridad de los dispositivos. Puede que necesiten utilizar dispositivos antiguos o de proveedores nuevos que no cuentan con los cifrados ni protocolos más actualizados. Sin embargo, estos equipos pueden colocar estos dispositivos menos seguros detrás del gestor de racks Avocent ADX para una mayor protección. De esta manera, los equipos de seguridad y de TI pueden obtener más valor de los dispositivos más antiguos o las nuevas innovaciones en prueba, sin comprometer la red ni la seguridad del sitio.

- **Mantener el firmware actualizado en los procesadores de servicio:** Los administradores de sistemas pueden usar la Plataforma de gestión Avocent ADX para automatizar las actualizaciones de firmware de los servidores mediante API RESTful y kits de desarrollo de software (SDK), para aportar consistencia y estandarización a esta necesaria tarea. Finalmente, la Plataforma de Gestión Avocent ADX simplifica las actualizaciones, lo cual elimina los periodos de inactividad de los dispositivos y reduce los riesgos de seguridad.

- **Fortalecer la seguridad de los dispositivos con controles específicos:**
  Con la Plataforma de gestión Avocent ADX, puede asignar, gestionar y controlar fácilmente los privilegios, para eliminar los riesgos que crean los privilegios de administrador excesivos. Los individuos que realizan construcciones iniciales de servidores pueden contar con una serie de privilegios, como instalar software e imágenes de sistemas operativos y reiniciar los servidores. El personal de TI que resuelve los problemas en los servidores podría estar autorizado a iniciar sesiones seriales o de KVM, y completar acciones clave, como la instalación de firmware.

Además, TI puede estandarizar estas acciones en los diferentes tipos de dispositivos. Por ejemplo, los administradores de sistemas pueden estar autorizados para reiniciar múltiples tipos de dispositivos. La plataforma también cuenta con capacidades de auditoría, las cuales permiten que los equipos de seguridad y de TI puedan revisar estos privilegios de forma continua para asegurarse de que los individuos no adopten medidas no autorizadas.

Conclusión

Mejorar la seguridad en la gestión de los servidores es una de las principales prioridades para las compañías y PYMES. Los servidores alimentan los procesos críticos que hacen funcionar los negocios digitales. Sin embargo, corren cada vez más peligro, debido a la expansión de la red, privilegios de administrador excesivos, firmwares desactualizados, vulnerabilidades de la memoria y otros problemas.

Los equipos de seguridad y de TI pueden identificar y eliminar de manera proactiva las brechas de seguridad en los servidores por medio de trabajar juntos, utilizar una plataforma de gestión y monitoreo centralizados y procesos automatizados. La Plataforma de Gestión Vertiv Avocent ADX ofrece estas capacidades esenciales, lo cual permite que los equipos de seguridad y de TI puedan trabajar hombro a hombro para proteger estos dispositivos de misión crítica tanto ahora como en el futuro.

[1] Shamus McGillicuddy, The Convergence of Network and Security Operations, artículo técnico de EMA, abril de 2021, pág. 1, https https://www.enterprisemanagement.com/research/asset.php/4037/The-Convergence-of-Network-and-Security-Operations

[2] "Hackers Breached Colonial Pipeline Using Compromised Password," artículo, Bloomberg, 4 de junio de 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[3] 2022 Tech Trends, Research Report, Info-Tech Research Group, diapositiva 3, https://www.infotech.com/research/ss/2022-tech-trends

[4] EMA: Network Management Megatrends, 2020, Kentik, pág. 1, https://www.kentik.com/resources/ema-network-management-megatrends-2020-report/

[5] "Assessing Enterprise Firmware Security Risk in 2021," artículo, 14 de enero de 2021, Eclypsium, https://eclypsium.com/2021/01/14/assessing-enterprise-firmware-security-risk-in-2021/

[6] Ravie Lakshmanan, "New iLOBleed Rootkit Targeting HP Enterprise Servers with Data Wiping Attacks," artículo, The Hacker News, 30 de diciembre de 2021, https://thehackernews.com/2021/12/new-ilobleed-rootkit-targeting-hp.html

[7] New Security Signals, ibid.

[8] "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats," artículo, Microsoft, 30 de marzo de 2021, https://www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/

Vertiv.com | Sede de Vertiv, 1050 Dearborn Drive, Columbus, OH, 43085, EE.UU.

SL-70977SP (R10/22)