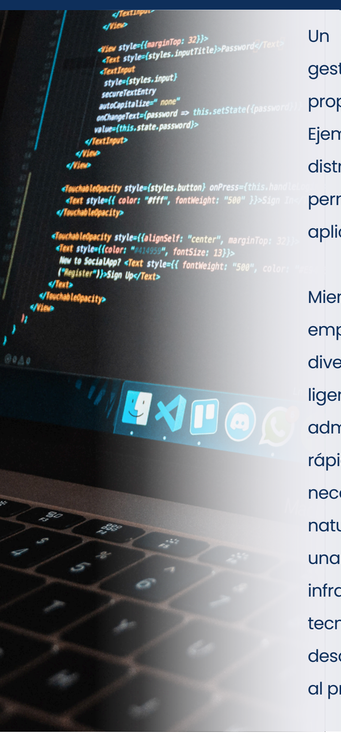
NEWSLETTER

¿Qué son los sistemas operativos (SO) y los Contenedores?



Un sistema operativo (SO) es el software fundamental que gestiona los recursos de hardware de una computadora y proporciona servicios comunes para los programas de aplicación. Ejemplos populares incluyen Windows, macOS y varias distribuciones de Linux (SUSE, etc...). Los sistemas operativos permiten a los usuarios interactuar con sus dispositivos y ejecutar aplicaciones de manera eficiente.

Mientras que los contenedores son una tecnología para empaquetar y ejecutar aplicaciones de Windows y Linux en diversos entornos locales y en la nube. Proporcionando un entorno ligero y aislado que facilita el desarrollo, implementación y administración de las aplicaciones. Se inician y detienen rápidamente, por lo que son ideales para las aplicaciones que necesitan adaptarse rápidamente a la demanda cambiante. La naturaleza ligera de los contenedores también los convierte en una herramienta útil para aumentar la densidad y el uso de la infraestructura. Docker y Kubernetes son ejemplos destacados de tecnologías de contenedores. Los contenedores facilitan el desarrollo, la implementación y la escalabilidad de aplicaciones al proporcionar un entorno consistente y reproducible.

Tendencias y futuro

En 2025, los sistemas operativos se benefician enormemente del hardware avanzado diseñado para ejecutar modelos de inteligencia artificial de manera eficiente. Los Neural Processing Units (NPU) se han integrado en procesadores como los Intel Ultra, AMD Ryzen PRO y Apple M-series, permitiendo realizar operaciones de IA localmente con menor consumo de energía y mayor velocidad. Estos chips aceleran tareas como el procesamiento de lenguaje natural, el reconocimiento de imágenes y la generación de contenido en tiempo real.

Por ejemplo, Windows 11 ha incorporado funciones como Copilot+, que utiliza NPUs para ofrecer asistentes de escritura, resúmenes automáticos y optimización de videollamadas con desenfoque de fondo basado en IA. Apple, por su parte, ha lanzado Apple Intelligence, un conjunto de herramientas integradas en MacOS que generan avatares, corrigen textos y gestionan tareas mediante modelos locales entrenados con Llama 3 de Meta.

Por otro lado, el 95% de las nuevas aplicaciones se desarrollan en contenedores, debido a que pueden ejecutarse con una densidad mucho mayor que las cargas de trabajo virtuales tradicionales, lo que significa que son necesarios menos servidores. Como consecuencia de ello, se reducen los costes de las licencias y, lo que es más importante, las necesidades de energía. Dando paso a un dato relevante de Gartner, donde nos dice que el 85% de las organizaciones utilizarán los contenedores en producción en el año 2025, frente al 35% de 2019.

Ciberseguridad en sistemas operativos (SO) y Contenedores

- La ciberseguridad es crucial para proteger los sistemas operativos y los contenedores contra amenazas potenciales. Algunas razones clave incluyen:

- Protección de datos sensibles: Los sistemas operativos y los contenedores manejan datos críticos que deben protegerse contra accesos no autorizados y ataques maliciosos.

- Aislamiento de aplicaciones: Los contenedores proporcionan una capa adicional de aislamiento, reduciendo el riesgo de que una brecha en una aplicación afecte a otras.

- Respuesta rápida a amenazas: Herramientas como SUSE Security permiten una respuesta automatizada a las amenazas, mejorando la capacidad de las organizaciones para mitigar riesgos de manera proactiva.

MARZO 2025

NEWSLETTER

¿Quién es SUSE y que nos brinda?

SUSE es una empresa líder en soluciones de código abierto que ofrece una gama de productos diseñados para satisfacer las necesidades de sistemas operativos y contenedores en entornos modernos de TI. Con un respaldo de 33 años en el sector de soluciones de código abierto, con más del 60% de las empresas de Fortune 500 confiando en SUSE y considerándola pionera en el desarrollo de distribuciones de Linux, proporcionando soluciones robustas y seguras como:

SUSE Linux Micro (SLM)
Es un sistema operativo ligero y ultra fiable, optimizado para cargas de trabajo en contenedores y entornos de IoT. Este sistema operativo inmutable está diseñado para casos de uso en el perímetro, como dispositivos integrados y aplicaciones en tiempo real. SUSE Linux Micro combina componentes de seguridad y cumplimiento normativo de nivel empresarial con una plataforma moderna y orientada a los desarrolladores.

SUSE Linux Enterprise Server (SLES)
Es una plataforma de servidor Linux segura, adaptable y fácil de gestionar. Permite a los desarrolladores y administradores implantar cargas de trabajo esenciales para el negocio en entornos locales, en la nube y en el perímetro. SLES está optimizado para ofrecer altas cotas de rendimiento, seguridad y fiabilidad, y fomenta la agilidad de los desarrolladores con soluciones creadas para aumentar la productividad, incluyendo una biblioteca expandida de imágenes de contenedor base y KubeVirt para la gestión de máquinas virtuales con Kubernetes.

SUSE Security
Ofrece una plataforma de seguridad de contenedores de código abierto y de confianza cero, proporcionando seguridad integral desde el núcleo hasta la nube. Esta plataforma realiza análisis constantes durante todo el ciclo de vida del contenedor, eliminando los obstáculos de seguridad y asegurando que las aplicaciones se ejecuten en un entorno seguro.

Integración con Microsoft Sentinel: Un paso adelante en Ciberseguridad

SUSE ha dado un paso significativo en el ámbito de la ciberseguridad al integrar sus soluciones con Microsoft Sentinel, una plataforma de gestión de eventos e información de seguridad (SIEM) nativa de la nube. Esta integración permite una respuesta automatizada a las amenazas, mejorada por las capacidades de IA generativa de Microsoft Security Copilot.

Beneficios claves de la integración

- **Visibilidad Mejorada:** La integración de las señales de SUSE Security en Sentinel proporciona una visión completa de las amenazas de seguridad en entornos de TI híbridos.
- **Respuesta Rápida:** Microsoft Sentinel puede emitir alertas y poner en cuarentena nodos de forma autónoma para evitar la propagación de amenazas mientras espera una revisión humana.
- **Análisis Avanzado:** Microsoft Security Copilot analiza los datos y comparte recomendaciones basadas en IA para la mitigación de amenazas, ayudando a identificar patrones y anomalías que podrían indicar un ataque sofisticado.

Reflexión empresarial

En el competitivo y dinámico entorno empresarial actual, la colaboración estratégica entre líderes del sector puede generar sinergias que impulsen la innovación y la eficiencia operativa. SUSE, con su sólida trayectoria en soluciones de código abierto, y Grupo BeIT, con su experiencia y liderazgo en el mercado mexicano, representan un ejemplo perfecto de cómo dos entidades pueden unirse para ofrecer soluciones integrales y de alto valor a sus clientes.

Grupo BeIT, con más de 20 años de experiencia en el mercado mexicano, se ha consolidado como un líder en ciberseguridad e infraestructura tecnológica. Ofrecen soluciones avanzadas para proteger los activos digitales y fortalecer la infraestructura tecnológica, garantizando la protección y continuidad del negocio para sus clientes.

La integración de las soluciones de SUSE con la experiencia de Grupo BeIT puede ofrecer múltiples beneficios:

1. Seguridad Integral: Protección desde el núcleo hasta la nube.
2. Optimización de Infraestructura: Mejora de la eficiencia operativa y reducción de costos.
3. Transformación Digital: Aceleración de la adopción de tecnologías de contenedores y nube híbrida.
4. Soporte y Consultoría: Implementación y gestión especializada de soluciones SUSE.

En conclusión, la colaboración entre SUSE y Grupo BeIT tiene el potencial de transformar el panorama tecnológico en México, ofreciendo soluciones que combinan innovación, seguridad y eficiencia.

Hasta la próxima semana, ciberlectores

Referencias

1. *SUSE*
2. *Revistabyte*
3. *Microsoft*

admmarketing@buromc.com

Contáctanos ahora