PROTECCIÓN DE LA INFRAESTRUCTURA DE APLICACIONES

Aplicación de nuevos modelos innovadores para transformar la seguridad

Nuevos modelos de seguridad para las amenazas en evolución

En los últimos años, empresas de todos los sectores han experimentado diferentes infracciones de datos de alto perfil que pusieron en riesgo la información confidencial, generaron costos millonarios para las organizaciones y ocasionaron enormes daños en la marca. Aunque los métodos específicos variaron, la mayoría de las infracciones utilizaron una estrategia común que expone la debilidad fundamental del modelo de seguridad de red centrado en el perímetro. Tradicionalmente, las organizaciones se centraban en proteger el centro de datos mediante firewalls perimetrales. Sin embargo, las amenazas modernas actuales penetran cada vez más la seguridad perimetral y se propagan de forma lateral de servidor a servidor (horizontalmente).

Para intentar resolver este problema, muchas organizaciones implementaron una variedad de productos puntuales, lo que generó una red de sistemas desconectados y complejos. Estas soluciones ad hoc son inflexibles y difíciles de aprovisionar y no se alinean con las aplicaciones que pretenden proteger. Al mismo tiempo, los atacantes son cada vez más sofisticados, mientras que las herramientas disponibles para ellos también se vuelven más potentes y fáciles de usar, lo que produce como resultado una variedad de actores más amplia para llevar a cabo ataques maliciosos.

Las empresas necesitan agilidad para impulsar el crecimiento

A medida que las organizaciones buscan acelerar el tiempo de salida al mercado y la obtención de resultados para las líneas de negocios y otras partes internas interesadas, también necesitan controlar la seguridad y administrar el riesgo de manera más eficaz. Para las empresas, es más importante que nunca no solo reducir el riesgo de una infracción de datos, sino también reducir el impacto en caso de que surja un problema. Sin embargo, la seguridad y el cumplimiento pueden afectar la agilidad del negocio. Es posible que los equipos de TI no siempre tengan las herramientas y los recursos necesarios para seguir el ritmo de las operaciones comerciales y, a la vez, mantener la seguridad de la infraestructura.

TI necesita seguridad y agilidad

Para cumplir con las expectativas de los líderes empresariales, las organizaciones de TI deben ser capaces de suministrar los servicios y las aplicaciones necesarios con rapidez y seguridad. No obstante, a medida que se esfuerzan por proteger el negocio, los equipos de TI enfrentan varios obstáculos, entre ellos los siguientes:

- La arquitectura de las aplicaciones está cambiando, desde aplicaciones monolíticas en las instalaciones hacia aplicaciones distribuidas y microservicios.
- Falta de visibilidad y de contexto del tráfico de red.
- Modelos y políticas de seguridad rígidos, centrados en el perímetro.
- Dificultad para lograr, mantener y demostrar el cumplimiento.

LAS AMENAZAS CONTRA LA SEGURIDAD SON UN ASUNTO SERIO

- El delito cibernético representa la causa de más rápido crecimiento en lo que respecta a interrupciones del centro de datos: ha aumentado desde un 2 % en 2010 hasta un 22 % en 2016.[1]
- El costo del espionaje cibernético global es de alrededor de 500.000 millones de USD por año, y alcanza 1 billón de USD si se incluyen los costos relacionados con el robo de la propiedad intelectual.[2]
- En 2016, el costo promedio de una filtración de datos ascendió a 4.000.000 de USD o 158 USD por registro perdido o robado.[3]

[1] Cost of Data Center Outages, Ponemon Institute, enero de 2016
[2] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/
[3] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, junio de 2016

Ventajas de separar las aplicaciones de la infraestructura

Para abordar estos problemas, las organizaciones deben transformar radicalmente la manera en que protegen la infraestructura de aplicaciones. VMware ofrece una cartera completa de soluciones que le permite a TI implementar una plataforma virtualizada, que separa la infraestructura de las aplicaciones que se ejecutan en ella, independientemente de si esa infraestructura se encuentra en las instalaciones o en la nube pública. Con VMware vSphere® y VMware NSX®, las organizaciones pueden aprovechar las ventajas de plataformas de virtualización sólidas y flexibles para respaldar aplicaciones nuevas y existentes, sin comprometer la seguridad y el cumplimiento. VMware vRealize® Network Insight™ mejora las capacidades mediante una administración empresarial de la nube para obtener visibilidad y protección adicionales.

Los tres aspectos básicos para proteger la infraestructura de aplicaciones

La implementación de una estrategia de seguridad nueva para la infraestructura de aplicaciones les permite a las organizaciones de TI posicionarse para aprovechar las ventajas de varias capacidades potentes:

Aplicaciones separadas de la infraestructura

Si se separan las aplicaciones de la infraestructura, se puede tener una visibilidad completa de la ruta de datos de las aplicaciones, lo que permite comprender mejor los patrones de tráfico. Además, esta capacidad permite que TI aumente significativamente la comprensión contextual sobre cómo la infraestructura y las aplicaciones interactúan entre ellas y con los datos. Mediante una visión completa y unificada de los datos, las aplicaciones y la infraestructura, las organizaciones pueden crear políticas y responder a las amenazas de manera más eficaz.

Política de seguridad detallada y alineada con las aplicaciones

Una estrategia virtualizada les permite a las organizaciones una alineación más estrecha de las políticas de seguridad con las aplicaciones que deben proteger, tanto en las nubes públicas como en las privadas. Asimismo, hace posible la microsegmentación de red para evitar la propagación lateral de amenazas (horizontalmente) entre las cargas de trabajo y las aplicaciones. Facilita también la inserción inteligente de servicios de seguridad de terceros en la plataforma cuando se necesitan nuevas capacidades.

Protección de la infraestructura basada en el hipervisor

Un modelo que permite separar las aplicaciones de la infraestructura subyacente también proporciona un punto ideal dentro de la infraestructura para protegerse de poner en riesgo la infraestructura en sí. Las organizaciones pueden proteger los datos estáticos mediante el cifrado a nivel de la carga de trabajo en cada host del hipervisor. Y pueden cifrar los datos en desarrollo para mitigar el riesgo de componentes de red en riesgo, como enrutadores y switches.

Una cartera de soluciones para proteger la infraestructura de aplicaciones

No importa dónde se encuentren las organizaciones en el camino hacia la adopción de la virtualización; VMware les ofrece soluciones líderes del sector que permiten mejorar los entornos de seguridad de las aplicaciones.

VMware vSphere

Para proteger los recursos empresariales fundamentales en un entorno virtualizado, las organizaciones necesitan capacidades de seguridad regidas por políticas y simples desde el punto de vista operacional, y una administración optimizada.

VMware vSphere, la plataforma de virtualización líder del sector, ofrece una base segura, flexible y potente para la agilidad del negocio que ayuda a las organizaciones a acelerar la transformación digital hacia la computación en nube. La solución es compatible con las aplicaciones existentes y de próxima

generación gracias a su experiencia simplificada para el cliente con respecto a la automatización y a la administración según las necesidades; seguridad integral incorporada para proteger los datos, la infraestructura y el acceso; y una plataforma de aplicaciones universal para ejecutar cualquier aplicación, en cualquier lugar. vSphere les permite a las organizaciones ejecutar, administrar, conectar y proteger sus aplicaciones en un entorno operativo común, en diferentes nubes y dispositivos.

VMware vSphere incluye funciones de seguridad enriquecidas que permiten que las organizaciones protejan sus entornos y reduzcan los problemas en caso de que se produzca una infracción.

- Seguridad según las necesidades:seguridad regida por políticas que simplifica la protección de la infraestructura desde el punto de vista operacional.
- Cifrado:con el cifrado a nivel de la máquina virtual (Virtual Machine, VM), se protege el acceso no autorizado a datos estáticos y móviles.
- Registro de auditorías de calidad:con el registro mejorado, se brinda información forense sobre las acciones de los usuarios.

Una red de proveedores líderes de terceros también proporciona un mejor respaldo de seguridad para VMware NSX.

VMware NSX

Para ofrecer una protección contra las amenazas sofisticadas actuales, las organizaciones necesitan un entorno de red virtual que les permita dividir el centro de datos en segmentos lógicos.

Si un atacante penetra las defensas del perímetro del centro de datos, es fundamental impedir que la amenaza se mueva de forma lateral dentro del centro de datos. Una estrategia virtualizada permite que los equipos de TI definan políticas de seguridad para cada carga de trabajo, según grupos de seguridad dinámicos. De esta manera, pueden responder inmediatamente a las amenazas que surgen dentro del centro de datos. VMware NSX es la plataforma de virtualización de redes que suministra el modelo operacional de una máquina virtual para la red del centro de datos. VMware NSX les permite a las organizaciones crear, almacenar, migrar, eliminar y restaurar de forma programática redes completas, como así también tomar snapshots de dichas redes, con la misma simplicidad y velocidad de apuntar y hacer clic de una máquina virtual. Esto proporciona un nivel de seguridad, agilidad y disponibilidad nunca antes visto con estrategias centradas en el hardware o estrategias operacionales tradicionales. Con la solución, las organizaciones pueden cumplir con las políticas de seguridad hasta el nivel de la máquina virtual individual.

VMware NSX respalda a las organizaciones que desean obtener las ventajas de la virtualización en cuanto a rendimiento y seguridad. Entre las capacidades clave, se incluyen las siguientes:

- Seguridad:funciones incorporadas de seguridad dentro del hipervisor, lo que proporciona microsegmentación y seguridad detallada a la carga de trabajo individual.
- Automatización:los servicios de redes y seguridad están conectados a las cargas de trabajo con una estrategia regida por políticas, para obtener automatización y lograr un rendimiento mejorado.
- Continuidad de las aplicaciones:se separan las redes del hardware subyacente y se relacionan las políticas de redes y seguridad con las cargas de trabajo asociadas.

vRealize Network Insight

Para administrar un entorno de nube híbrida heterogéneo, las organizaciones necesitan una plataforma de administración empresarial de la nube diseñada específicamente para dicho entorno.

vRealize Network Insight proporciona operaciones inteligentes para redes y seguridad del centro de datos definido por software (Software-Defined Data Center, SDDC), con visibilidad convergente en redes físicas y virtuales, además de recomendaciones en cuanto a la planificación de la microsegmentación y administración de operaciones para VMware NSX.

vRealize Network Insight ofrece una amplia variedad de funciones que ayudan a las organizaciones a optimizar la seguridad.

- Visibilidad:proporciona visibilidad convergente en la nube pública y privada, física y virtual, en overlay y underlay, con integración entre capas físicas y virtuales.
- Comportamiento de las aplicaciones para modelar la microsegmentación:permite a los usuarios comprender fácilmente quiénes participan en la comunicación y qué flujos hay que permitir o bloquear.
- Auditoría y cumplimiento:permite realizar un seguimiento de todos los cambios a los fines de las auditorías y el cumplimiento.

MÁS INFORMACIÓN

Obtenga más información sobre las prioridades e iniciativas de TI adicionales en vmware. com/latam/it-priorities/transform-security.

Protección de la infraestructura de aplicaciones con VMware

Las organizaciones de TI actuales enfrentan desafíos sin precedentes como resultado de la transformación digital y un panorama de amenazas dinámicas. En este entorno dinámico, resulta más importante que nunca asociarse con un proveedor de tecnología probado para garantizar la seguridad de las operaciones comerciales. Coalfire, un asesor de administración de riesgo cibernético independiente, recientemente reconoció las capacidades de VMware en su informe comparativo. En el informe, se llegó a la conclusión de que el producto VMware NSX "proporciona un control detallado de las políticas de seguridad y visibilidad del tráfico que facilita la operativización de la seguridad y permite que los clientes alcancen los requisitos de cumplimiento normativo". [4]

VMware les permite a las organizaciones transformar su estrategia de seguridad mediante el aprovisionamiento de una capa de software omnipresente en la infraestructura de aplicaciones. Al separar la infraestructura de las aplicaciones compatibles, VMware hace posible que los equipos de TI extiendan la visibilidad de la ruta de datos, para obtener mejor información y control. Junto con la microsegmentación, la solución ayuda a las organizaciones a simplificar las políticas de seguridad y lograr una mejor alineación de la protección para suplir las necesidades de determinadas aplicaciones. Para esto, VMware ofrece una gran variedad de soluciones de virtualización y seguridad, que cuentan con el respaldo de una amplia red de socios. Cuando se tiene una solución sólida de cumplimiento y seguridad, las organizaciones pueden liberar a los equipos de TI para que se centren en impulsar el crecimiento y la innovación en el negocio.

[4] "Micro-segmentation Cybersecurity Benchmark Report", septiembre de 2016, Coalfire

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com/latam

N.º de elemento: SecureApplicationInfrastructure_SolutionBrief
5/17