Protección de las aplicaciones en entornos virtualizados y de cloud mediante VMware AppDefense

Pese a que el gasto en la seguridad de TI no para de aumentar en todo el mundo, la probabilidad de que una organización sufra una vulneración de datos se ha incrementado hasta el 25 %.[1] A pesar de los millares de productos de seguridad que hay en el mercado y los enormes presupuestos dedicados a su compra, los datos no están más protegidos. Esto plantea un desafío importante para los directores de seguridad de la información, que tienen que proteger aplicaciones y datos ubicados en entornos de TI cada vez más distribuidos y dinámicos. A medida que crece el número de organizaciones que adoptan modelos ágiles y modernos de desarrollo de aplicaciones, es más difícil implementar la seguridad al ritmo que exige la empresa. La seguridad a menudo se ve como un obstáculo para el progreso.

Los directores de seguridad de la información y sus equipos se enfrentan a dos desafíos principales cuando intentan proteger sus datos y aplicaciones:

Amenazas no detectadas y falsas alarmas

Las soluciones de seguridad de terminales existentes activan numerosas falsas alarmas que obligan a los equipos de operaciones de seguridad a perder tiempo investigando manualmente amenazas inexistentes. Pero lo peor es que a veces no detectan amenazas reales.

Entornos dinámicos a ritmo acelerado

Las soluciones de seguridad existentes se diseñaron sin tener en cuenta la velocidad a la que se desarrollan e implementan las aplicaciones modernas, por lo que no pueden seguir el ritmo de lanzamiento y actualización de las nuevas aplicaciones.

Transformar la seguridad con la virtualización

VMware AppDefense está en una posición inmejorable para afrontar estos dos desafíos. AppDefense es un producto de seguridad de terminales del centro de datos que integra la funcionalidad de detección y respuesta a amenazas en la capa de virtualización donde residen las aplicaciones y los datos. AppDefense utiliza VMware vSphere® para ofrecer tres ventajas principales con respecto a las soluciones de seguridad de terminales existentes:

Conocimiento fidedigno del estado previsto de una aplicación (si sabe cómo debe funcionar, puede detectar las desviaciones)

AppDefense utiliza el hipervisor vSphere para obtener información relevante sobre el comportamiento de los terminales del centro de datos, y es el primero en saber cuándo se han realizado cambios. Gracias a esta información contextual es posible determinar qué cambios son legítimos y cuáles son amenazas reales, sin necesidad de hacer conjeturas.

Respuesta precisa y automatizada a las amenazas: la respuesta adecuada en el momento oportuno

Cuando se detecta una amenaza, AppDefense puede activar vSphere y VMware NSX® para coordinar la respuesta adecuada, sin requerir intervención manual. Por ejemplo, AppDefense puede realizar las siguientes acciones automáticamente:

- Bloquear la comunicación de los procesos
- Crear una instantánea de un terminal para realizar un análisis forense
- Suspender un terminal
- Apagar un terminal

INFORMACIÓN BÁSICA

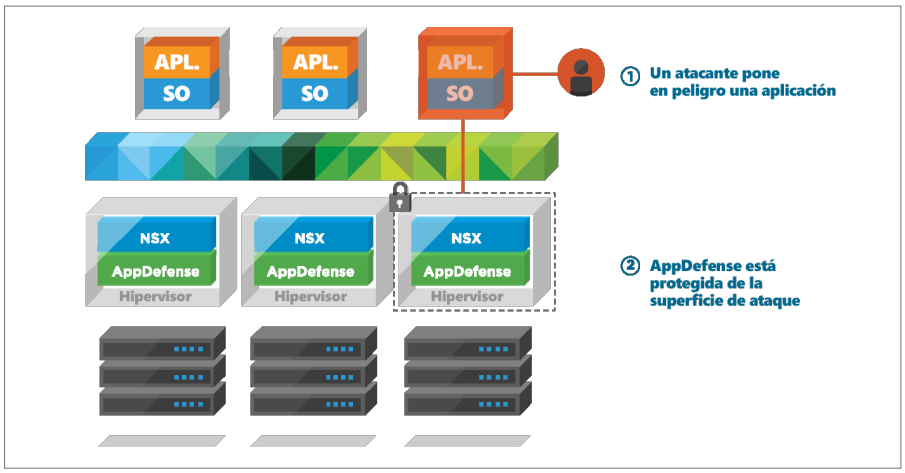
VMware AppDefense™ es un nuevo producto de seguridad para los terminales del centro de datos que protege las aplicaciones que se ejecutan en entornos virtualizados. A diferencia de las soluciones de seguridad de terminales existentes, que buscan amenazas, AppDefense se centra en supervisar si las aplicaciones están en su estado previsto (hacen lo que tienen que hacer) y responde automáticamente cuando se desvían de ese estado previsto, lo que indicaría una posible amenaza. De este modo se potencia al máximo la eficacia y la efectividad de las operaciones de seguridad, y se optimiza el proceso de revisión y el nivel de preparación de la seguridad de las aplicaciones.

CARACTERÍSTICAS DESTACADAS

- Simplifica la seguridad de terminales del centro de datos.
- Mejora la detección de amenazas en el centro de operaciones de seguridad.
- Automatiza la respuesta a las incidencias.
- Optimiza las evaluaciones de seguridad de las aplicaciones.

Aislamiento de la superficie de ataque para proteger al protector

Lo primero que la mayoría de los programas maliciosos hacen al entrar en un terminal es desactivar el antivirus y otras soluciones de seguridad de terminal basadas en agentes. El hipervisor proporciona una ubicación protegida desde la que AppDefense puede operar, garantizando la protección de AppDefense aunque el terminal se vea comprometido.



AppDefense en acción

AppDefense es un producto de seguridad esencial que puede influir ampliamente en la estrategia de seguridad de una organización.

Alertas centradas en aplicaciones para el centro de operaciones de seguridad (SOC)

AppDefense no genera muchas alertas, pero cuando da la voz de alarma, lo mejor es hacer caso. Las alertas concretas generadas por AppDefense, junto con las funciones de respuesta automatizada, permiten que los administradores de seguridad se centren en detectar y eliminar las amenazas del entorno, en lugar de tener que analizar datos superfluos e investigar amenazas inexistentes.

Transformar las revisiones de la seguridad de las aplicaciones

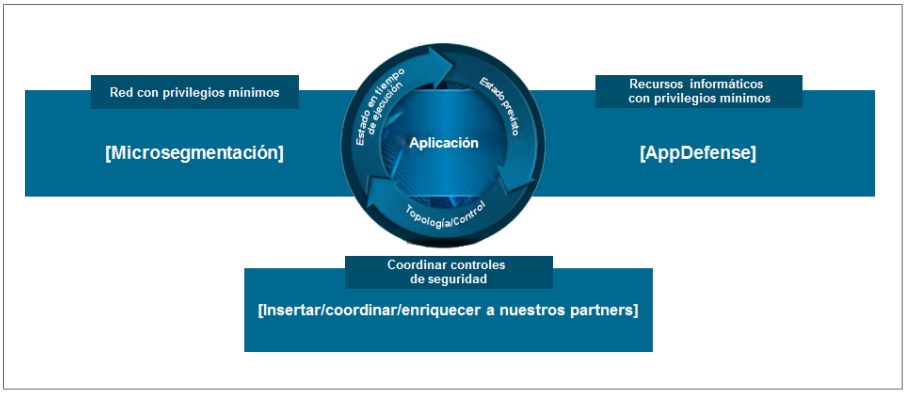
En el mundo del desarrollo moderno de aplicaciones, se publican, se cambian y se retiran aplicaciones con gran rapidez. A menudo, los equipos de seguridad saben de la existencia de una nueva aplicación cuando esta ya ha cambiado. AppDefense crea una fuente de información común para los equipos de aplicaciones y de seguridad. De este modo, se agiliza el proceso de revisión de la seguridad.

Seguridad centrada en las aplicaciones con VMware

VMware ha cambiado el panorama de la seguridad de red con su plataforma de virtualización de red, VMware NSX, y su capacidad de habilitar la microsegmentación en el centro de datos. NSX integra los servicios de red y de seguridad, como los cortafuegos, directamente en la arquitectura del hipervisor, estableciendo un modelo de privilegios mínimos para la red. De esta manera, los equipos de seguridad de red pueden evitar el desplazamiento lateral de las amenazas en sus entornos.

MÁS INFORMACIÓN

Para obtener más información o comprar VMware AppDefense, visite http://www.vmware.com/es/appdefense y pruebe el producto en nuestro laboratorio práctico.



AppDefense proporciona en capas la funcionalidad de detección y respuesta a amenazas en otra área principal de la infraestructura, estableciendo un modelo de privilegios mínimos para los terminales del centro de datos. Si una amenaza logra penetrar en un terminal, AppDefense la detectará inmediatamente y responderá de forma automática y con precisión. La combinación de NSX y AppDefense ofrece una solución sólida para la protección de la infraestructura de aplicaciones y de las aplicaciones y los datos que residen en ella.

[1] Ponemon Institute, junio de 2017, «2017 Cost of a Data Breach Study: Global Overview»

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.com/es
Copyright © 2017-2018 VMware, Inc. Todos los derechos reservados. Este producto está protegido por las leyes de derechos de autor y de propiedad intelectual de Estados Unidos e internacionales. Los productos de VMware están cubiertos por una o varias de las patentes enumeradas en http://www.vmware.com/go/patents. VMware es una marca comercial o marca registrada de VMware Inc. y sus filiales en Estados Unidos o en otras jurisdicciones. Las demás marcas y nombres mencionados en este documento pueden ser marcas comerciales de sus respectivas empresas.
N.º artículo: vmw53313-sb-securing-app-cloud-env-app-defense-es-ES-a4-101
8/17