CÓMO SIMPLIFICAR LA SEGURIDAD Y REDUCIR LA SUPERFICIE DE ATAQUE

Implemente una protección integrada en su infraestructura de aplicaciones

vmware® | intel®

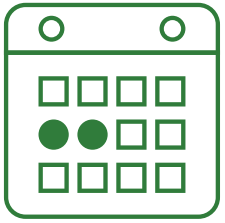
La superficie de ataque es mayor de lo que cree

No es ningún secreto que todo está cada vez más conectado. Está claro que vivimos en un mundo hiperconectado debido a la proliferación de aplicaciones, dispositivos móviles y conectados en red, etc. Las organizaciones deben lidiar con el auge de este tipo de terminales mientras se expanden a nuevos entornos utilizando centros de datos y múltiples clouds para gestionarlo todo.

Con cada nueva conexión, la superficie de ataque se hace más grande

Ahora hay más puntos vulnerables y en más sitios que nunca, algo que no dejará de aumentar en los próximos meses y años. Para los hackers y los ciberdelicuentes es muy fácil aprovecharse de estas vulnerabilidades. Además de crear nuevos vectores y metodologías de ataque cada día, también desarrollan herramientas sencillas de usar, de modo que cualquier persona sin conocimientos técnicos puede intentarlo.

Este documento le servirá para comprender por qué reducir la superficie de ataque le ayudará a proteger la infraestructura de aplicaciones frente a unas amenazas que no dejan de aumentar.



Se tarda una media de **197 días** en identificar una vulneración de seguridad, y una media de **69 días** en contenerla.[1]

1 Ponemon Institute, «2018 Cost of Data Breach Study», julio de 2018.

Seguridad compatible con la agilidad empresarial

Con los años, los procesos de seguridad se han ganado la fama de limitar o ralentizar la actividad empresarial, pero eso está cambiando. La naturaleza persistente del panorama de las amenazas indica que la seguridad no es únicamente una medida preventiva, sino que es esencial para el buen estado de las empresas en todos los sectores.

Sin embargo, no todas las soluciones son iguales: una que simplificara, automatizara e integrara la seguridad representaría una ventaja considerable.

Las soluciones de seguridad deben respaldar los objetivos empresariales, permitiéndole:

- Obtener información sobre las amenazas en todo momento y utilizar métodos innovadores para atajarlas.
- Prevenir, detectar, dar respuesta y predecir de forma fluida y continua.
- Proteger los elementos móviles y perimetrales con tácticas de eficacia probada para dispositivos y aplicaciones.
- Mejorar el ecosistema global de seguridad gracias a una visibilidad, un contexto y un control mejores.

Tenga en cuenta que es inútil perseguir amenazas

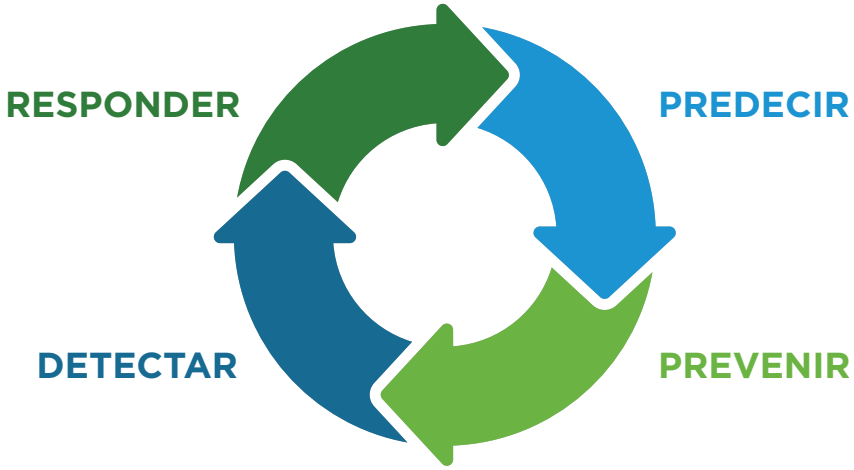
El primer paso para crear una infraestructura de aplicaciones más segura es replantearse la forma de abordar la seguridad. Para combatir la ciberdelincuencia, las organizaciones de TI suelen centrarse en amenazas o vulnerabilidades concretas, pero esto solo sirve para que los atacantes cambien de táctica y las vuelvan a coger desprevenidas. Si quiere ir por delante, deje de perseguir amenazas individuales y amplíe sus miras. Si estudia y comprende la naturaleza de las amenazas actuales, podrá abordarlas en su globalidad y obtener mejores resultados con el paso del tiempo.

Por ejemplo, los programas de secuestro pueden aprovecharse de las diversas variaciones y vulnerabilidades. Conocer las pautas de los ataques de los programas de secuestro le ayudará a proteger tanto la infraestructura como los datos esenciales. Muchos de los ataques contra las organizaciones de mayor tamaño son únicos porque se han confeccionado específicamente para atacar a una organización determinada, por tanto, generar una respuesta a un ataque en concreto no sirve de mucho.

Hay que centrarse en cómo reducir la superficie de ataque para limitar la exposición y el daño que pueda infligir un atacante.

Un marco de aprendizaje continuo en materia de seguridad

En 2016, Gartner publicó un modelo de seguridad basado en cuatro principios fundamentales que se retroalimentan entre sí para crear un proceso proactivo de protección de las aplicaciones.[2] Este enfoque escalonado no se ocupa de amenazas individuales, es más bien una forma de actuar que permite a los departamentos de TI evolucionar al ritmo de las amenazas.



La reducción de la superficie de ataque se corresponde con la fase **Prevenir**. Le prepara para las fases posteriores mejorando la detección a través de una mayor visibilidad y una supervisión continua; además, le permite ser más rápido en sus respuestas y actualizar los protocolos de seguridad para predecir amenazas futuras.

2 Gartner Research, «Using the Predict, Prevent, Detect, Respond Framework to Communicate Your Security Program Strategy», abril de 2016.

Es complicado proteger un blanco móvil

No hace mucho tiempo, las aplicaciones estaban confinadas en el centro de datos, donde podían ser supervisadas y protegidas cuidadosamente. Esos tiempos han quedado atrás. Las aplicaciones ya no están en pilas monolíticas en un único servidor, sino que se encuentran distribuidas en muchos servidores y contenedores virtuales y servidores físicos. Además, son muy dinámicas y se desplazan por ubicaciones, centros de datos, clouds y redes de sucursales. El perímetro del centro de datos, que anteriormente era la primera línea de defensa, ahora es penetrable.

Las arquitecturas en evolución requieren una respuesta avanzada ante las amenazas

La naturaleza de las aplicaciones ha cambiado de forma que cada vez son más importantes para el éxito de las empresas. Con el fin de ofrecer una protección suficiente, los controles de seguridad deben ser igual de omnipresentes y ágiles que las aplicaciones.

Las empresas tienen un **27,9 % de posibilidades** de volver a sufrir otra vulneración importante en los dos años posteriores.[3]

3 Ponemon Institute, «2018 Cost of Data Breach Study», julio de 2018.

La situación actual debe llegar a su fin: la seguridad intrínseca es la clave para avanzar

La infraestructura centrada en el hardware no dispone de las herramientas suficientes para gestionar las aplicaciones modernas ni las amenazas sofisticadas que evolucionan a toda velocidad. Los enfoques tradicionales requieren una implementación, configuración y gestión manuales. También dependen de tecnologías de protección añadidas, que tardan mucho tiempo en adaptarse y no cubren todas las carencias.

Una infraestructura virtual y definida por software crea una estructura digital que ofrece conectividad omnipresente y una seguridad intrínseca para las aplicaciones, independientemente de donde se encuentren, desde el centro de datos al perímetro, pasando por la cloud.

Una red de cloud virtual permite:

- Proteger las aplicaciones de forma predeterminada.
- Obtener visibilidad de las aplicaciones en todos los entornos.
- Adoptar un enfoque centrado en las aplicaciones para las políticas de seguridad.

Veamos con mayor detenimiento estas prestaciones.

Proteger las aplicaciones de forma predeterminada

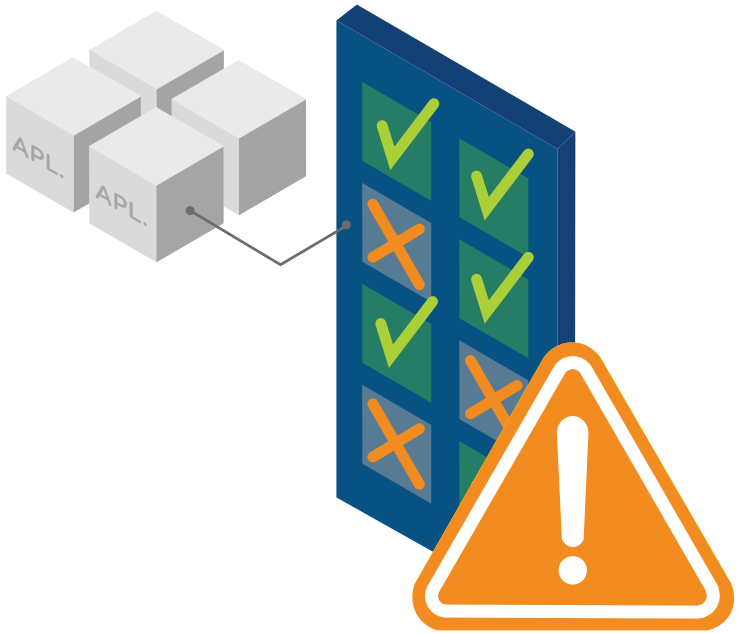
VMware protege las aplicaciones y las cargas de trabajo de forma automática mediante la generación de controles de seguridad directamente en una capa de software omnipresente, donde residen las aplicaciones.

Cuando los puntos de acceso del centro de datos se ponen en marcha como parte de las aplicaciones, se cifran automáticamente. Heredan políticas y controles de seguridad que permanecen con ellas durante todo su ciclo de vida, incluso aunque se desplacen entre diferentes entornos.

Obtener visibilidad de las aplicaciones en todos los entornos

Una solución que le ayude a entender la forma en que se comunican la red y las aplicaciones le proporcionará un mejor conocimiento de la situación para cumplir sus objetivos en materia de seguridad.

Una infraestructura de aplicaciones segura ofrece una visibilidad esencial en todas las actividades de las aplicaciones, desde sus procesos, hasta sus flujos y patrones de comunicación. Busque soluciones que ofrezcan una visibilidad total en redes virtuales, físicas y multicloud.



Adoptar un enfoque centrado en las aplicaciones para las políticas de seguridad

La capacidad de diseñar y aplicar políticas de seguridad flexibles y centradas en las aplicaciones puede ayudar a reducir la superficie total de ataque de las aplicaciones y los datos. Las políticas de seguridad deben diseñarse y aplicarse en función de las aplicaciones y los datos, independientemente de que residan en la red o en el punto de acceso del centro de datos.

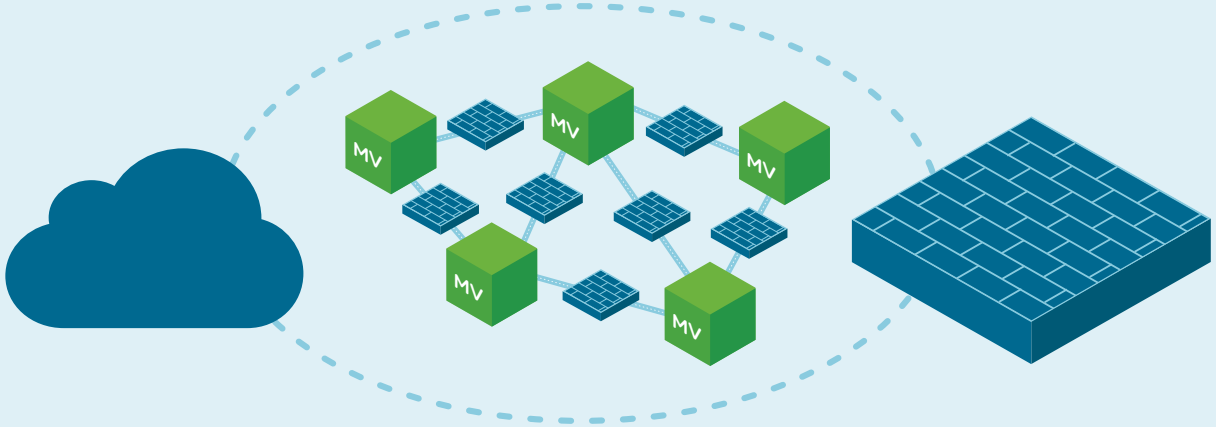
Podrá utilizar el estado y el comportamiento deseados de los puntos de acceso del centro de datos en los que residen aplicaciones para asegurarse de que el funcionamiento es correcto, en lugar de estar al acecho de las acciones malintencionadas.

La importancia fundamental de la microsegmentación

Actualmente, las organizaciones no se plantean si habrá vulneraciones de seguridad, sino cuándo se llevarán a cabo. La microsegmentación forma parte de los enfoques definidos por software por lo que limita la propagación transversal de las amenazas aplicando políticas de seguridad de red a nivel granular: en cada punto de acceso individual de un centro de datos.

Gracias a los controles transversales que permite la microsegmentación, las amenazas ya no podrán campar a sus anchas. La inserción dinámica de servicios hace posible enrutar eficientemente el tráfico de red a través de otros servicios de seguridad, como los cortafuegos de nueva generación, sin que se requiera una intervención manual.

Para que la microsegmentación sea efectiva, es fundamental poder ponerla en marcha. Es necesario que las soluciones ofrezcan visibilidad en las comunicaciones, con recomendaciones sobre cómo implementarlas.

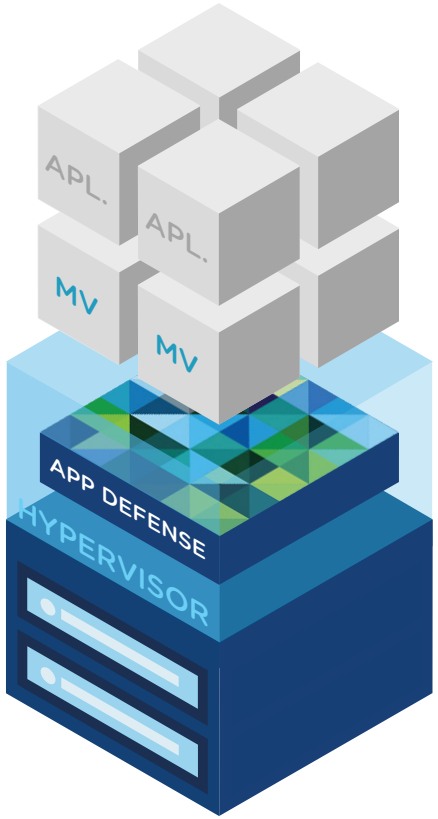


La ubicación lo es todo

Una solución que integre los controles de seguridad directamente en el hipervisor ofrecerá protección integral desde el núcleo, con un modelo basado en políticas y de sencillo funcionamiento.

Ventajas de encontrarse cerca del hipervisor:

- **Se simplifica la implementación y la gestión.** Dado que está integrado con las herramientas de la máquina virtual, se puede gestionar como parte del proceso y del conjunto de herramientas habituales para la gestión de máquinas virtuales.
- **Mejora la visibilidad y el contexto.** Con el hipervisor obtendrá una visión global de los flujos este-oeste y norte-sur, entrantes y salientes de las máquinas virtuales, junto con el contexto que le indicará si el tráfico es el esperado o entraña posibles problemas.
- **Activación de controles de seguridad adicionales.** Se sirve del hipervisor para mejorar la visibilidad y la seguridad de las aplicaciones, además de los procesos que ya hubiera implementado.



Cómo empezar a reducir la superficie de ataque

Las aplicaciones modernas seguirán siendo dinámicas y distribuidas, por lo que la superficie de ataque seguirá expandiéndose. Para proteger su empresa necesita una infraestructura donde la seguridad sea un componente integrado y no un añadido «a posteriori».

VMware reduce la superficie de ataque de las aplicaciones gracias a una seguridad intrínseca y uniforme en el centro de datos, la cloud y el perímetro. VMware NSX® permite la microsegmentación en la red para evitar la propagación lateral de las amenazas. VMware AppDefense™ impone el estado y el comportamiento esperados de las aplicaciones en los puntos de acceso de los centros de datos, mientras que VMware vSphere® y VMware vSAN™ ofrecen cifrado para los datos en reposo.

VMware e Intel transforman las redes y la seguridad con una solución integral de software y hardware para conectar y proteger las aplicaciones y los datos con independencia de dónde residan, ya sea en el centro de datos, la cloud o el perímetro.

DÉ EL SIGUIENTE PASO

Más información sobre una infraestructura de aplicaciones segura >

Pruebe las soluciones NSX con un laboratorio práctico >

Síganos:

vmware® | intel®

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