Sugerencias técnicas

Diez sugerencias para mejorar la seguridad de la implementación de VMware Horizon

Protección del entorno de TI en la era de la virtualización
Convencidas por las ventajas de la movilidad empresarial, las organizaciones de TI buscan eliminar las limitaciones de la arquitectura heredada para obtener la libertad que ofrece la nueva generación de escritorios. Al utilizar VMware® Horizon® para transformar los escritorios, los usuarios finales disfrutan de un acceso flexible a aplicaciones y escritorios virtualizados a través de una única plataforma.

Sin embargo, esta mayor flexibilidad, que incluye prestaciones para los usuarios finales como servicios de uso de dispositivos personales (BYOD), supone un nuevo desafío para la seguridad de TI. Ofrecer acceso más amplio requiere mayor vigilancia para garantizar la seguridad de los datos. Además, en una era en la que la seguridad de TI de las empresas ya requiere mucha atención (el número de incidencias crece a una velocidad del 66 % de la tasa de crecimiento anual compuesta, con un coste por vulneración de 5,9 millones de dólares[1]), debe garantizar que la transformación de escritorios sea eficiente y segura.

¿QUÉ ES VMWARE HORIZON?

VMware Horizon aumenta la potencia de la virtualización de las aplicaciones y los escritorios, ya que los distribuye a los usuarios finales mediante una única plataforma. Es posible acceder a estos servicios de escritorios y aplicaciones (que incluyen aplicaciones alojadas en RDS y aplicaciones empaquetadas con VMware ThinApp®) a través de un área de trabajo unificada desde cualquier dispositivo, medio, conexión y ubicación. Para obtener más información sobre Horizon, visite vmware.com/go/horizon.

Las nuevas consideraciones que plantean los usuarios de sistemas virtualizados para la seguridad de TI
Aunque la transformación de escritorios ofrece una gran cantidad de ventajas para los usuarios finales y las organizaciones de TI (por ejemplo, ahorros en gastos operativos, aumento de la productividad del usuario final, alta disponibilidad y reducción de la inversión en capital), es importante comprender los desafíos que conllevan para los responsables de TI.

- La distribución de aplicaciones y escritorios en tiempo real permite a los administradores de TI aprovechar la transformación de escritorios para configurar rápidamente todo lo que necesitan los usuarios nuevos para empezar a trabajar, mediante la distribución de auténticos «escritorios sin estado» en cuestión de segundos. ¿Cómo se puede establecer la escalabilidad horizontal en las implementaciones sin perder la visibilidad ni el control de la red?

- La organización puede ofrecer servicios a miles, incluso a cientos de miles de usuarios que utilizan infraestructuras esenciales. Si los escritorios virtuales se encuentran en riesgo, la vulneración puede suponer un coste elevado.

- Puede volverse más vulnerable debido a la actividad «este-oeste», el tráfico interno entre servidores o entre escritorios. Las acciones cotidianas que realizan los usuarios de confianza pueden suponer amenazas para la red. Por ejemplo, debido a los correos electrónicos con virus o a los sitios web peligrosos a los que acceden cuando navegan por Internet.

Teniendo en cuenta estas consideraciones, le presentamos diez sugerencias técnicas para que la implementación de Horizon sea más segura:

1 Utilizar imágenes maestras

Con una «imagen maestra» (una plantilla de escritorios virtuales) los equipos de TI pueden adaptar los escritorios virtuales con el fin de que los usuarios solo vean las actividades que son relevantes para sus necesidades empresariales. Así, el departamento de TI se puede centrar en mantener la pureza de la imagen maestra que reside segura en el centro de datos. Si un escritorio virtual está en riesgo, el equipo de TI puede eliminar la imagen y volver a implementar un escritorio nuevo.

2 Utilizar seguridad en capas

En un entorno virtualizado, vale la pena afrontar los riesgos de seguridad bajo distintos aspectos. Al adoptar medidas de seguridad adicionales como la creación de «listas blancas» de aplicaciones mediante VMware NSX™, puede aprobar las aplicaciones que se ejecutarán en su red. Este mecanismo protege la red y hace que los usuarios cumplan los requisitos de conformidad ahora que las empresas se enfrentan a las soluciones de TI en la sombra, en las que los usuarios y los responsables de las líneas de negocio adquieren servicios y aplicaciones empresariales fuera del dominio de TI. Se puede conservar también la integridad de las aplicaciones gracias a los métodos de distribución de aplicaciones, utilizando herramientas como VMware App Volumes™.

1. PwC, «Managing cyber risks in an interconnected world», septiembre de 2014

ACERCA DE VMWARE APP VOLUMES

Los administradores de TI pueden distribuir aplicaciones y datos a los usuarios o escritorios en segundos y según las necesidades gracias a VMware App Volumes. Con esta solución, puede utilizar volúmenes gestionados para disminuir los costes de gestión y de infraestructura. Las aplicaciones funcionan como aplicaciones nativas y los usuarios finales pueden acceder a ellas en cualquier sesión y desde cualquier dispositivo.

Entre las ventajas, se incluyen las siguientes:

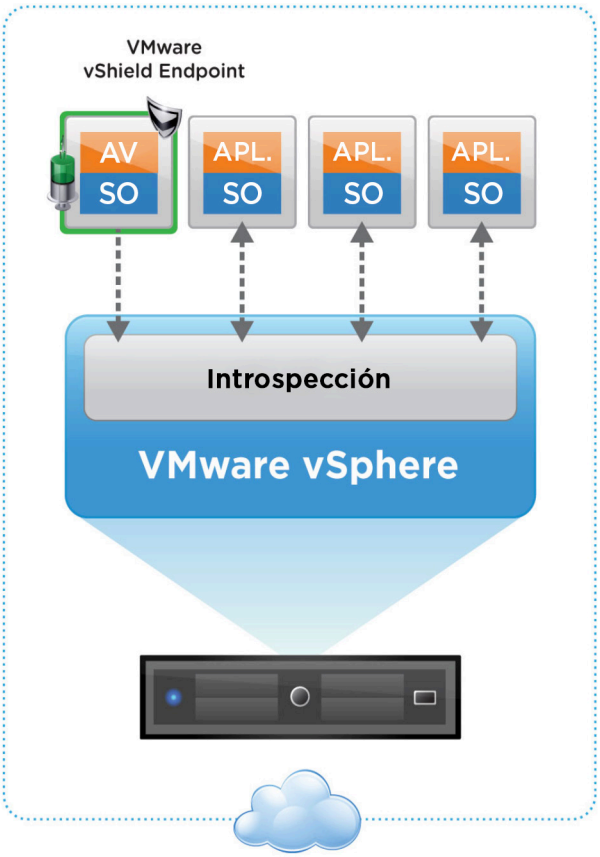
- Aplicaciones gestionadas de forma centralizada
- Facilidad para implementar aplicaciones
- Aplicaciones distribuidas por usuario

Para obtener más información sobre App Volumes, visite https://www.vmware.com/es/products/appvolumes/.

3 Aplicar la seguridad adecuada a los dispositivos terminales

Al invertir en prestaciones de hardware y software, puede reforzar la seguridad de los dispositivos terminales de Horizon. Por ejemplo, si un dispositivo se pierde o alguien lo roba, las características basadas en hardware, como el Módulo de plataforma de confianza (TPM), activan la autenticación de la plataforma para que el dispositivo no se inicie. Por otro lado, se debe asegurar de que cuenta con las versiones actuales de las soluciones de antivirus y de protección ante programas maliciosos y que el cortafuegos del dispositivo terminal está actualizado y activo.

Existen administradores de TI que no emplean prácticas antivirus en los escritorios virtuales para reducir el efecto en la memoria, la CPU y los discos. No obstante, el daño que puede provocar un virus en un escritorio virtual puede ser tan grave como el de un virus en un escritorio físico, especialmente si pasa por alto actualizar las máquinas virtuales de forma habitual. VMware vShield Endpoint™ puede ser una alternativa excelente. Esta solución descarga software para procesar los agentes antivirus y contra programas maliciosos de las máquinas virtuales en un dispositivo virtual seguro.



Por último, también puede aumentar la seguridad para los dispositivos terminales con soluciones externas. Proveedores como Trend Micro Deep Security ofrecen funciones avanzadas, entre las que se incluyen soluciones contra programas maliciosos, IDS/IPS, supervisión de la integridad, filtrado de URL y aplicación de parches. Las funciones de Deep Security se ejecutan desde el nivel del hipervisor y ofrecen una protección instantánea cuando se pone en marcha un escritorio remoto nuevo. La seguridad también se aplica automáticamente al terminal en cualquier punto del centro de datos.

ACERCA DE VMWARE VSHIELD ENDPOINT

VMware vShield Endpoint aumenta la seguridad de las máquinas virtuales al mismo tiempo que mejora la protección de los puntos de acceso. Esta solución está diseñada para utilizar las mejoras existentes, permitiendo a los clientes gestionar políticas antivirus y contra programas maliciosos en entornos virtualizados con las mismas interfaces de gestión que usan para proteger los entornos físicos. Además, se integra con productos de los siguientes proveedores: Trend Micro, Intel Security, Symantec, Sophos y Kaspersky.

4 Implementar políticas de grupo y ampliadas

Las políticas de grupo permiten evitar posibles riesgos, en el caso de una infracción del terminal, por ejemplo, si un dispositivo no tiene actualizado el software antivirus o contra programas maliciosos. Con una política de grupo, puede hacer que los escritorios virtuales sean uniformes, desactivar servicios que el usuario no necesite y prevenir el acceso a ciertas partes del escritorio y la red. La configuración de las políticas evita que los usuarios realicen modificaciones que puedan provocar que el escritorio sea vulnerable.

También es recomendable usar VMware User Environment Manager™, una solución de gestión del entorno del usuario ampliable, simple y eficaz que ayuda al departamento de TI a gestionar usuarios y aplicaciones, así como a establecer políticas dinámicas. Las operaciones de TI diarias son más eficientes y seguras mediante la configuración de aplicaciones y políticas que se aplican a los usuarios en todos los dispositivos y ubicaciones, y que gestionan el acceso de los usuarios dependiendo de si acceden a través de un escritorio interno o un dispositivo externo.

Además, con los archivos de plantilla de administración de las políticas de grupo (ADM) de Horizon, que amplía la política de grupo de Active Directory, puede regular la información que pasa por el escritorio, por ejemplo, desactivando el portapapeles.

5 Garantizar una arquitectura adecuada

Con Horizon, efectuar una implementación segura precisa prestar atención a la configuración de la zona desmilitarizada y del cortafuegos, así como a la segregación de depósitos de escritorios. Lo primero que debe hacer es colocar un cortafuegos entre la red del centro de datos y la red de la oficina. Si utiliza LAN virtuales o cortafuegos para separar los servidores de los escritorios, el entorno VDI debe estar en la parte del cortafuegos que corresponde al escritorio.

Para proteger a los usuarios remotos, debe configurar el servidor de seguridad o el punto de acceso en la zona desmilitarizada. Así, proporciona a los usuarios un punto de conexión sin permitir que accedan directamente a la red. Si incluye una función de puerta de enlace, tenga en cuenta las ventajas de Access Point frente a las que ofrece un servidor de seguridad. Con Access Point, por ejemplo, puede implementar una máquina virtual reforzada, bloqueada, preconfigurada y basada en Linux en lugar de implementar solo el software que se ejecuta en el sistema operativo Windows de uso general. También puede configurar Access Point en un View Connection Server individual o conectarlo a través de un equilibrador de carga que se encuentre frente a varios View Connection Servers para ofrecer una mayor disponibilidad.

Se recomienda segregar los depósitos de escritorios cuando estos se deban separar del resto de la organización, como en el caso de los escritorios del departamento de recursos humanos, trabajadores externos o desarrolladores. Usar VMware NSX como complemento de la plataforma VMware vSphere® puede ser útil para realizar este proceso.

6 Utilizar la autenticación multifactor y de transmisión

Al ser compatible con soluciones de autenticación multifactor, como RSA SecurID, VASCO DIGIPASS, SMS Passcode y SafeNet, Horizon ofrece lo esencial para garantizar la seguridad del escritorio. Por otro lado, Horizon también emplea la tecnología de autenticación de transmisión, en la que los usuarios introducen las credenciales dos veces o inician sesión en el escritorio con otra cuenta.

Además, puede usar VMware Identity Manager™. Esta solución de gestión de identidades ofrece un acceso condicional y de inicio de sesión único (SSO) para que pueda simplificar la movilidad empresarial y proporcionar una experiencia de usuario óptima en todos los dispositivos sin poner en peligro la seguridad del entorno.

Proteger los periféricos

Los dispositivos externos pueden introducir virus perjudiciales o permitir que los usuarios roben datos de propiedad intelectual. Con Horizon puede tomar medidas para proteger los datos y evitar que se copien en dispositivos de almacenamiento portátiles locales, como impresoras y USB no seguros. Además, si se instala la función de redirección de unidad del cliente en el escritorio virtual, los usuarios pueden acceder de forma «remota» a los archivos almacenados en el PC local. Cuando se envían archivos del terminal al escritorio virtual se utiliza compresión y cifrado.

7 Realizar periódicamente análisis y procesos de mantenimiento

Es fundamental prestar atención al mantenimiento para garantizar la seguridad. Siga estos pasos para protegerse frente a vulneraciones potenciales:

- Actualice el software con funciones antivirus y contra programas maliciosos que informen al personal correspondiente cuando los ataques sean inminentes.
- Defina una política aceptable para recomponer o actualizar los escritorios de Horizon de forma periódica para que incluyan los parches de seguridad, los parches y las actualizaciones de las aplicaciones, además de las actualizaciones del sistema operativo.
- Aplique las actualizaciones y los parches de seguridad de forma regular y no solo en el sistema operativo, sino también en las aplicaciones que se encuentran en la «imagen maestra».
- Realice análisis periódicos de los puertos de los cortafuegos principal y secundario para que la política del cortafuegos se implemente correctamente y no permita el acceso no autorizado a la zona desmilitarizada.
- Analice los patrones de tráfico para conocer el tráfico permitido en los cortafuegos y en la zona desmilitarizada, y supervise el cortafuegos para determinar los puertos que no se utilizan.
- Realice auditorías de forma periódica. Por ejemplo, lleve a cabo auditorías regulares de la configuración del equilibrador de carga y del cortafuegos para comprobar que no se haya producido un acceso sin autorización.
- Cuando se apliquen los parches y las actualizaciones, actualice la imagen principal en primer lugar, pruébela y distribúyala a todos los escritorios virtuales de forma rápida y fiable.

¿POR QUÉ ACTUALIZAR? MAYOR SEGURIDAD Y MEJOR RENDIMIENTO

Si actualiza los escritorios virtuales cuando se cierran las sesiones, los usuarios accederán siempre a un escritorio funcional y sin rastro de la sesión anterior. Además de aumentar la seguridad al borrar del escritorio remoto los posibles programas maliciosos y virus, el siguiente usuario disfrutará de la misma usabilidad y, además, se reforzará el rendimiento.

8 Proteger la red

La combinación de VMware NSX y Horizon ofrece el marco para la automatización y la microsegmentación. Con VMware NSX, puede implementar un cortafuegos distribuido y por puertos, lo que le permite controlar el tráfico que puede recibir un escritorio, desde dónde puede recibirlo y hacia dónde puede enviarlo. También puede crear zonas para aislar a los trabajadores externos y proteger la red ante una navegación web de alto riesgo.

Con la microsegmentación, cada máquina virtual tiene su propia defensa perimetral. Un cortafuegos distribuido supervisa el tráfico entrante y saliente de cada máquina virtual, evitando el acceso sin autorización y bloqueando el acceso de las amenazas al centro de datos. Puede automatizar la distribución de la seguridad y microsegmentar las cargas de trabajo para adaptar el escritorio virtual de forma más rápida y segura al mismo tiempo que aumenta su rendimiento.

9 Exponerse solo a lo necesario

Debe dar una mayor importancia a la precisión de los permisos para evitar posibles vulnerabilidades. En su entorno predeterminado, es posible que las aplicaciones tengan acceso a otras aplicaciones. Entre otras cosas, los programas maliciosos pueden hacer que una aplicación sobrescriba la memoria de otra que esté ejecutando. Esto facilita que se produzcan daños importantes, ya que se pone en peligro todo aquello a lo que la aplicación tiene acceso. Gracias a la virtualización de aplicaciones mediante VMware ThinApp, cada aplicación se circunscribe a su propio entorno, acotado, del sistema operativo virtual. De esta manera, las aplicaciones no tienen acceso a otras aplicaciones ni pueden ver sus archivos, y algunas partes del sistema operativo se pueden aislar de la aplicación. Por lo tanto, se reduce el alcance de posibles contagio y puede eliminar las infecciones fácilmente si se produce una vulneración.

CONSIDERACIONES DE SEGURIDAD COMUNES QUE SE SUELEN PASAR POR ALTO

- Si es posible, no otorgue derechos administrativos a los usuarios.
- Trate los escritorios virtuales como si fueran escritorios tradicionales en cuestiones de seguridad. Utilice aplicaciones antivirus, aplique políticas e implemente herramientas de bloqueo.
- Reemplace los certificados predeterminados y autofirmados que utiliza para proteger canales SSL por uno creado por una entidad de certificación de confianza con el fin de reducir los ataques de intermediarios.
- Si los usuarios utilizan un escritorio virtual remoto para utilizar el acceso remoto o realizar tareas de teletrabajo, limite su acceso a datos confidenciales.
- Use VMware vRealize® Operations Manager™ para supervisar los picos de tráfico.
- En las implementaciones externas, utilice servidores de seguridad o servidores de Access Point en la zona desmilitarizada.

Conclusión

Aunque prometa muchas características para conseguir que la gestión sea eficiente y los usuarios finales más flexibles, la transformación de escritorios por sí sola no hará que su organización de TI sea más segura. De hecho, como ya se ha mencionado, puede enfrentarse a más desafíos de seguridad si no actúa de forma proactiva. Con la implementación adecuada y siguiendo los consejos que aparecen en este documento, puede mejorar la seguridad de la red y ofrecer las ventajas de TI que conlleva la transformación de escritorios.

Puede probar Horizon de forma gratuita con el laboratorio práctico. Además, podrá empezar a utilizarlo en el navegador en cuestión de minutos, sin necesidad de instalarlo. Registrarse: https://www.vmware.com/horizon-hol-labs.

Síganos

Blog: https://blogs.vmware.com/euc

Twitter: @vmwarehorizon

Facebook: https://www.facebook.com/vmwarehorizon

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.es