

¡El libro de seguridad en la nube y la virtualización para todos!
Edición especial de Trend Micro

Seguridad para la nube y la virtualización

FOR **DUMMIES**®

Aprende a:

- Hacer frente a los retos de seguridad virtual
- Usar la infraestructura de escritorio virtual para aumentar la seguridad
- Encontrar la solución de seguridad virtual que estás buscando

Por cortesía de



Daniel Reis



Acerca de Trend Micro

Trend Micro, líder mundial en software y soluciones de seguridad, trabaja para que el intercambio de información digital pueda realizarse de forma segura. Durante los últimos 25 años, su personal se ha esmerado en proteger a particulares, familias, empresas y gobiernos, tratando de aprovechar el potencial de las tecnologías emergentes y las nuevas formas de compartir la información.

Para las organizaciones de hoy la información se ha convertido en su activo más estratégico, ya que supone una ventaja a nivel competitivo y favorece la excelencia operativa. Con el boom de las tecnologías móviles, sociales y de la nube, el reto de proteger dicha información es mayor que nunca. Las organizaciones necesitan una estrategia de protección inteligente.

Trend Micro ofrece esa protección inteligente de la información, con soluciones de seguridad innovadoras que resultan sencillas de gestionar e implementar y se adaptan a un ecosistema que no para de cambiar. Las soluciones de Trend Micro proporcionan seguridad de contenidos en capas para dispositivos móviles, puntos de destino, puertas de enlace, servidores y para la nube. Gracias a estas soluciones las organizaciones pueden proteger a su usuario final, sus recursos en los centros de datos y en la nube y su información amenazada por sofisticados ataques dirigidos.

Todas las soluciones funcionan gracias a una infraestructura global de seguridad basada en la nube, la Trend Micro™ Smart Protection Network™, en la que trabajan más de 1200 expertos en amenazas de todo el mundo. Para más información, visita www.trendmicro.com/virtualdummies.

Seguridad para la nube y la virtualización

FOR
DUMMIES®

Edición especial de Trend Micro

Daniel Reis

FOR
DUMMIES®

Seguridad para la nube y la virtualización For Dummies®, Edición especial de Trend Micro

Publicado por

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

Copyright © 2013 by John Wiley & Sons, Inc., Hoboken, New Jersey

No se permite la reproducción total o parcial de este libro, ni su incorporación a un sistema informático de recuperación de datos, ni su transmisión en cualquier forma o por cualquier medio, sea éste electrónico, mecánico, por fotocopia, grabación, escaneado o por otros métodos, con la excepción de lo previsto en las secciones 107 o 108 de la Ley de Derechos de Autor de 1976 de los Estados Unidos, sin el permiso previo y por escrito del editor. Las solicitudes de permiso al editor deben enviarse a Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008/748-6008 o a la dirección de Internet <http://www.wiley.com/go/permissions>.

Marcas registradas: Wiley, For Dummies, el logotipo Dummies Man, The Dummies Way, Dummies.com, Making Everything Easier y la imagen comercial relacionada son marcas registradas de John Wiley & Sons, Inc. y/o sus afiliados en los Estados Unidos y en otros países y no pueden ser utilizados sin permiso escrito. Trend Micro y el logotipo de Trend Micro son marcas registradas de Trend Micro Incorporated. Cualquier otra marca mencionada en el libro pertenece a sus respectivos propietarios. John Wiley & Sons, Inc. no está asociado con producto o fabricante alguno citado en la presente obra.

LIMITACIÓN DE RESPONSABILIDAD/DESCARGA DE RESPONSABILIDAD DE GARANTÍA: EL EDITOR Y EL AUTOR NO REALIZAN MANIFESTACIÓN NI DECLARACIÓN DE GARANTÍA ALGUNA CON RESPECTO A LA EXACTITUD O INTEGRIDAD DE LOS CONTENIDOS DE LA PRESENTE OBRA Y RENUNCIAN EXPRESAMENTE A TODA GARANTÍA, INCLUYENDO, PERO SIN LIMITARSE, LAS GARANTÍAS DE IDONEIDAD PARA UN USO DETERMINADO. NO PODRÁ CREARSE NI PRORROGARSE GARANTÍA ALGUNA POR VENTAS O MATERIALES PROMOCIONALES. LAS RECOMENDACIONES Y ESTRATEGIAS CONTENIDAS EN LA PRESENTE PUEDEN NO SER ADECUADAS PARA TODOS LOS CASOS. LA VENTA DE ESTA OBRA SE REALIZA CON EL CONOCIMIENTO DE QUE EL EDITOR NO ESTA OBLIGADO A PRESTAR NINGUN SERVICIO PROFESIONAL DE TIPO JURIDICO, CONTABLE U OTROS. EN CASO DE QUE SE REQUIERA ASISTENCIA PROFESIONAL, DEBERÁN SOLICITARSE LOS SERVICIOS DE UN PROFESIONAL COMPETENTE. NI EL EDITOR NI EL AUTOR SERÁN RESPONSABLES DE LOS DANOS QUE PUDIERAN DERIVARSE DE LA PRESENTE OBRA. EL HECHO DE QUE EN LA PRESENTE OBRA SE HAGA REFERENCIA A UNA ORGANIZACIÓN O UN SITIO WEB A MODO DE CITA Y/O FUENTE DE INFORMACIÓN ADICIONAL, NO SIGNIFICA QUE EL AUTOR O EL EDITOR AVALEN LA INFORMACIÓN FACILITADA O LAS RECOMENDACIONES REALIZADAS POR DICHA ORGANIZACIÓN O SITIO WEB. ASIMISMO, LOS LECTORES DEBEN TENER PRESENTE QUE LOS SITIOS WEB LISTADOS EN ESTA OBRA PUEDEN HABER CAMBIADO O DESAPARECIDO EN EL TIEMPO TRASCURRIDO ENTRE LA REDACCIÓN Y LA LECTURA DEL LIBRO.

Si desea información general sobre nuestros otros productos y servicios o de cómo crear un libro personalizado de Para Dummies para su negocio u organización, póngase en contacto con Business Development Department, 877-409-4177 (en los Estados Unidos), escriba a info@dummies.biz o visite www.wiley.com/go/custompub. Si desea información sobre la concesión de licencias de la marca For Dummies para productos o servicios, póngase en contacto con BrandedRights&Licenses@Wiley.com.

ISBN 978-1-118-85095-4 (pbk); ISBN 978-1-118-85345-0 (ebk)

Impreso en los Estados Unidos de América

10 9 8 7 6 5 4 3 2 1

Agradecimientos del editor

Éstas son algunas de las personas que ayudaron a sacar este libro al mercado:

Adquisiciones, editorial y sitios web verticales

Editor de producción: Lawrence C. Miller

Editora de proyecto: Jennifer Bingham

Director editorial: Rev Mengle

Representante de desarrollo comercial:

Kimberley Schumacker

Especialista del proyecto de publicaciones

personalizadas: Michael Sullivan

Servicios de redacción

Coordinadora jefe de proyecto: Kristie Rees

Maquetación y artes gráficas: Carrie A. Cesavice, Jennifer Goldsmith, Andrea Hornberger

Correctoras: Lindsay Amones

Colaboración especial de Trend Micro:

Paula Rhea, Monica Niemann

Desarrollo comercial

Lisa Coleman, Director, directora, nuevo mercado y desarrollo de marca

Índice

Introducción	1
Acerca de este libro	2
Suposiciones insensatas.....	2
Cómo está organizado este libro	3
Iconos utilizados en este libro.....	4
¿Por dónde empezar?.....	4
Capítulo 1: Entornos virtuales	5
¿Qué es la virtualización?	5
¿Cuáles son los beneficios de la virtualización?.....	7
Retos de seguridad para empresas en un entorno virtual	8
Agilidad	8
Cumplimiento normativo	10
Nube y virtualización	12
Capítulo 2: Seguridad del servidor virtual	13
Retos de seguridad específicos del entorno virtual.....	13
Comunicaciones entre máquinas virtuales	14
Aprovechamiento de recursos.....	15
VM inactivas	18
Migraciones de VM	19
Cómo abordar los retos de seguridad virtual	
con soluciones compatibles con el entorno virtual.....	20
La protección de datos en la nube.....	22
Capítulo 3: Seguridad de la infraestructura de escritorio virtual (VDI)	23
Los retos de seguridad de la VDI.....	24
Cómo dar con el mejor tipo de seguridad para trabajar	
con la VDI.....	26
Gestión del acceso a datos y la seguridad con la VDI.....	27
Uso de la VDI en la nube.....	28

Capítulo 4: Las soluciones de seguridad de Trend Micro para el entorno virtual.	29
Protección contra amenazas globales.....	29
Un vistazo al paisaje.....	30
Incremento del volumen	30
Mayor sofisticación	30
Una mirada a la red de protección inteligente.....	31
Diseño de la seguridad para entornos virtuales	32
Protección de todos los aspectos del entorno informático	36
Capítulo 5: Diez funciones importantes que hay que buscar en una solución de seguridad consciente del entorno virtual.	41
Apéndice.....	43

Introducción

Las tecnologías de virtualización se están adoptando a una velocidad tremenda hoy en día. Aunque los beneficios de la virtualización superan sus retos, sí que acarrea problemas significativos en el ámbito de la TI.

Puede que el principal problema de la virtualización resida en la creencia de que la tecnología de seguridad tradicional funciona igual en un entorno virtual que en uno físico. En la actualidad, los sistemas virtuales, al igual que los sistemas físicos dedicados, forman parte de la mezcla de entornos informáticos que normalmente encontramos en muchas empresas. Los departamentos de TI han de gestionar entornos informáticos mixtos o híbridos, compuestos de plataformas virtuales y físicas.

A medida que nos volvemos más dependientes de la virtualización, nos vemos obligados a fijarnos (ojalá que sin sorpresas desagradables) en las limitaciones intrínsecas de diseño que tienen las soluciones de seguridad tradicionales a la hora de ser aplicadas a sistemas virtualizados.

Como la aparición de la nube ha acaparado mucha atención durante los últimos años, es necesario que entendamos bien cómo funciona la seguridad en los entornos de la nube. Muchas organizaciones llegan a la peligrosa conclusión de que sus datos están tan seguros en la nube como en su propio centro de datos, y que no tienen que hacer nada especial para garantizar la existencia de un nivel aceptable de seguridad. La realidad puede llegar a ser bastante distinta. El problema no es que el entorno de la nube no esté protegido por el proveedor; lo que pasa es que tus datos, a no ser que ese proveedor y tú hayáis llegado a algún arreglo especial, no están necesariamente protegidos contra la exposición que supone el alojamiento en una nube que comparten multitud de inquilinos. Como usuario, no conoces a los otros inquilinos que manejan sus aplicaciones virtuales en la misma máquina anfitriona que tú, ni sabes si tus datos se almacenan en un dispositivo de almacenamiento compartido con otro grupo de residentes desconocidos. Tampoco sabes a quién pueden estar permitiendo el acceso a sus datos esos otros residentes, justo en

el mismo dispositivo de almacenamiento que comparten contigo. Y la cruda realidad es que no puedes controlar todos esos factores.

Los proveedores de la nube se afanan para que sus entornos sean seguros, pero recuerda que las directivas que establecen (por ejemplo, las reglas de cortafuegos) permiten a miles de clientes acceder a sus sistemas regularmente, por lo que es probable que dichas reglas no respondan a tus preocupaciones sobre seguridad de datos. Así que te corresponde a ti determinar si esas directivas sirven para proteger tus datos de manera satisfactoria. De no ser así, debes asegurarte de que aplicas mecanismos de seguridad que se ajusten a tus necesidades en todo entorno de nube compartido.

Acerca de este libro

Este libro examina los retos de seguridad de la virtualización en el centro de datos, en el puesto de trabajo y en la nube. En él explico por qué es un error utilizar en sistemas virtuales productos de seguridad tradicionales, creados para proteger sistemas físicos. Por último, te muestro cómo las soluciones de seguridad compatibles con el entorno virtual proporcionan seguridad total, sin afectar al rendimiento, en los entornos virtuales, de nube e híbridos, los que incluyen una mezcla de sistemas virtuales y físicos.

Suposiciones insensatas

En primer lugar, doy por hecho que sabes algo sobre la virtualización de servidor y de escritorio y, quizás, también alguna que otra cosa sobre seguridad. Este libro ha sido escrito principalmente para lectores técnicos que están evaluando soluciones de seguridad para un entorno virtual o mixto (físico y virtual).

Aunque muchos de los términos y conceptos presentados en este libro hacen referencia a la tecnología de virtualización en general, doy por sentado que tienes interés principalmente en las soluciones de virtualización de VMware, Microsoft y Citrix, por lo que me centro en dichas soluciones (con mis disculpas a IBM, Oracle y los proveedores de otras muchas soluciones de virtualización disponibles en la actualidad).

Por último, supongo que la mayoría de las organizaciones ya han intentado proteger sus sistemas virtuales usando las mismas

herramientas, de manera más o menos parecida, que utilizaron en sus sistemas físicos. Muchos profesionales informáticos dan por sentado, equivocadamente, que los sistemas virtuales son básicamente iguales, o que funcionan de manera bastante parecida a las máquinas físicas, por lo que acaban implementando en sus nuevos entornos virtuales las herramientas de seguridad y gestión que ya poseen, con resultados decepcionantes o incluso catastróficos.

Cómo está organizado este libro

Este libro constituye una fuente de conocimiento virtualmente (¡cómo no!) inagotable. Todo ese saber ha sido embutido en cinco breves capítulos, que te ofrecen solamente la información que necesitas. Echemos un breve vistazo a lo que te espera en las páginas que se avecinan:

- ✓ **Capítulo 1:** Entornos virtuales. Empiezo explicando cómo funciona la tecnología de virtualización, algunos de los principales beneficios que la virtualización ofrece a las organizaciones y algunos retos empresariales relacionados con los entornos virtuales.
- ✓ **Capítulo 2:** Seguridad del servidor virtual. A continuación, te cuento algunos de los retos de seguridad específicos a los que debes enfrentarte en un centro de datos virtualizado.
- ✓ **Capítulo 3:** Seguridad de la infraestructura de escritorio virtual (VDI). En este capítulo, explico algunos de los retos de seguridad de la virtualización de escritorio y cómo la VDI puede ayudarte a proteger datos en el contexto del BYOD.
- ✓ **Capítulo 4:** Las soluciones de seguridad de Trend Micro compatibles con el entorno virtual. Aquí aprenderás algo sobre la solución Deep Security de Trend Micro, compatible con el entorno virtual, que protegerá el tuyo.
- ✓ **Capítulo 5:** Diez funciones importantes que hay que buscar en una solución de seguridad para el entorno virtual. Seguidamente, en el clásico estilo de Para Dummies, te paso una lista de comprobación para cuando tengas que evaluar soluciones de seguridad para tu entorno virtual.
- ✓ **Apéndice:** Glosario. Para terminar, y por si no te sabes todos y cada uno de los acrónimos de los que hace gala la industria informática, he incluido una lista útil con las siglas y los términos que uso en este libro.

Iconos utilizados en este libro

A lo largo del libro, verás iconos que sirven para llamar la atención sobre datos relevantes para el lector. No vas a ver caritas sonrientes guiñándote un ojo u otros bonitos emoticonos del estilo, pero sin duda querrás quedarte con el mensaje. He aquí lo que puedes esperar encontrarte.



Este ícono señala información que, junto con los aniversarios y cumpleaños, sería conveniente que te grabaras en la parte no volátil de tu memoria, es decir, en la materia gris (también conocida como los sesos).



Este ícono explica la jerga que subyace bajo la jerga.



Gracias por tu atención. Espero que te guste el libro. ¡Y trata bien al escritor! En serio, este ícono señala sugerencias e información de utilidad.



Estas convenientes alertas ofrecen consejos prácticos que te ayudarán a evitar errores potencialmente costosos.

¿Por dónde empezar?

Si no sabes por dónde empezar, cualquier capítulo puede valer... Aunque el Capítulo 1 puede ser un buen punto de partida. Sin embargo, si ves algún tema en concreto que te llame la atención, no dudes en saltarte las páginas que sea necesario para leer dicho capítulo. Cada capítulo ha sido confeccionado separadamente (aunque no empaquetado para su venta por separado) y escrito para que pueda leerse de manera independiente, así que tómate la libertad de empezar por donde quieras y saltar libremente de aquí para allá (¡me refiero las páginas del libro, no al mundo físico!). Lee este libro en el orden que quieras (aunque no te recomiendo hacerlo hacia atrás o al revés).

Capítulo 1

Entornos virtuales

En este capítulo

- ▶ Definición de virtualización
- ▶ Beneficios de la virtualización
- ▶ Reconocimiento de los retos de seguridad de la virtualización para las empresas
- ▶ Trabajar en la nube y el entorno virtual

Los beneficios de la virtualización son incuestionables. Organizaciones de todos los tamaños, desde negocios pequeños y medianos hasta grandes empresas globales, están adoptando la tecnología de virtualización –incluyendo la informática en la nube– a una velocidad sin precedentes. En este capítulo aprenderás algunos de los conceptos básicos de las tecnologías de virtualización y sus beneficios, así como el modo en que las tecnologías virtuales están cambiando el panorama de la seguridad.

¿Qué es la virtualización?

La tecnología de *virtualización* emula los recursos de la informática física, tales como los servidores y los ordenadores de sobremesa, en un entorno virtual. El diagrama 1-1 representa un entorno virtual simplificado. La *plataforma de software de infraestructura virtual*, también llamada software de virtualización, es una capa de virtualización instalada en un servidor físico. Estos son algunos ejemplos de software de virtualización: VMware vSphere, Microsoft Hyper-V y Citrix XenServer.

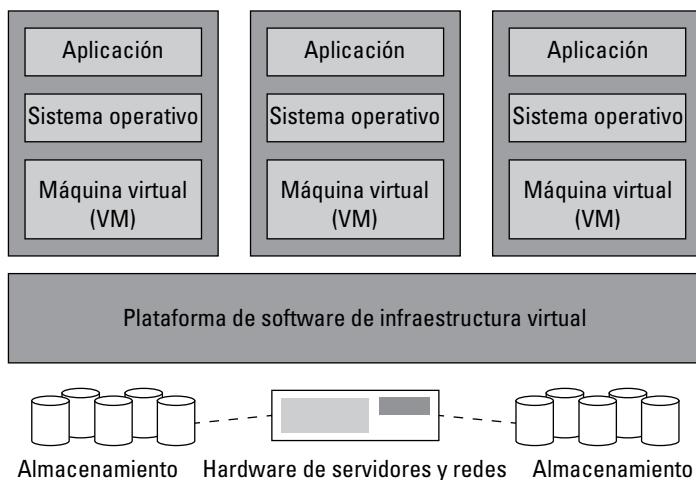


Diagrama 1-1: vista simplificada de un entorno informático virtual.

El software de virtualización se ejecuta en la máquina anfitriona física y proporciona un ecosistema operativo para diversas *instancias virtuales*, o máquinas virtuales (VM, por sus siglas en inglés), que ejecutan aplicaciones específicas. El *hipervisor* es un componente del software de virtualización que funciona entre el núcleo del hardware de la máquina anfitriona física y el sistema operativo de las VM individuales. El hipervisor gestiona las comunicaciones y la asignación de recursos entre las VM, lo cual hace posible que varias VM funcionen en una única máquina anfitriona física.



La tecnología de virtualización tiene su origen en los sistemas de ordenadores centrales. El núcleo de un ordenador central se conoce como *supervisor*. Por tanto, el *hipervisor* es el software que funciona por encima del núcleo de un entorno virtual.

Una VM, en su forma más simple, puede entenderse como una máquina física reducida a un conjunto de entornos de sistemas operativos centrales (ESO): el sistema operativo (SO), una aplicación y el sistema anfitrión o host, que emula a una máquina física (como por ejemplo, un servidor o un ordenador de sobremesa). Cada VM cuenta con su propio sistema operativo (SO), como Windows o Linux, y la máquina anfitriona física le asigna una parte de los recursos totales de procesador, memoria, E/S (entrada/salida) y red, todos ellos son gestionados por el hipervisor del software de virtualización.

En un entorno virtual cada VM funciona a modo de sesión individual dedicada para las aplicaciones específicas que se ejecuten en esa VM. Cada sesión de VM se ejecuta exactamente como lo haría en una

máquina física dedicada, suponiendo que se asignen los recursos adecuados para que sus SO y aplicaciones se ejecuten. El hipervisor hace posible que varias sesiones de VM funcionen a la vez en la infraestructura virtual que alberga dichas sesiones, lo cual permite un aprovechamiento mayor y una asignación más eficiente de los recursos de la máquina anfitriona física.

¿Cuáles son los beneficios de la virtualización?

La virtualización lleva tiempo siendo una de las tendencias tecnológicas más interesantes. Según cálculos de Gartner, Inc., en un centro de datos actual, casi la mitad de los servidores basados en x86 están virtualizados; es de suponer que, para 2015, lo estarán más de las tres cuartas partes.

Las empresas están adoptando la virtualización, entre otras razones, por lo siguiente:

- ✓ **Consolidación del hardware de los servidores.** La virtualización de servidor permite que numerosos sistemas y aplicaciones de varios servidores físicos coexistan en un único servidor físico (o grupo de servidores físicos).
- ✓ **Mejora de la eficiencia operativa.** La virtualización proporciona a las organizaciones la agilidad y flexibilidad necesarias para implementar y mantener los nuevos sistemas y aplicaciones de servidor y escritorio y cubrir sus necesidades empresariales.
- ✓ **Optimización de recursos limitados.** Desde la maximización de CPU, memoria y el aprovechamiento de E/S en los servidores anfitriones físicos hasta la extensión de la vida útil del hardware de los ordenadores personales de sobremesa, la virtualización ayuda a las empresas a sacarle a su equipo informático la mayor rentabilidad sobre la inversión (RSI).
- ✓ **Reducción de gastos de funcionamiento (OPEX).** La virtualización puede simplificar la gestión de sistemas y reducir la huella ecológica de tu centro de datos, lo cual reduce los gastos energéticos e inmobiliarios.

Retos de seguridad para empresas en un entorno virtual

Aunque la virtualización puede reportar importantes beneficios a organizaciones de todos los tamaños, en un entorno virtual es necesario abordar una serie de retos de seguridad. La agilidad y el cumplimiento normativo son algunos de los aspectos que mayor repercusión tienen en la seguridad. Trataré los retos técnicos de seguridad en el Capítulo 2.

Agilidad

La agilidad es uno de los muchos beneficios de la virtualización. Las VM nuevas pueden ser aprovisionadas, retiradas y puestas en estado inactivo con rapidez. Pero la velocidad y comodidad con que se realizan estas tareas pueden incrementar la exposición a diversos problemas de seguridad. He aquí algunas de las importantes cuestiones que conviene tener en cuenta:

- ✓ ¿Se han implementado las nuevas VM usando un perfil de seguridad aprobado y de acuerdo con las directivas establecidas?
- ✓ ¿Se ha instalado la versión adecuada de SO y se le han realizado las revisiones correctas a la hora de implementar nuevas VM?
- ✓ ¿Hay recursos apropiados disponibles para las nuevas VM implementadas en una máquina anfitriona??
- ✓ ¿Se ha llevado a cabo un análisis de capacidad antes de implementar nuevas VM en una máquina anfitriona?
- ✓ ¿Cómo afecta una nueva VM al rendimiento y a la seguridad de otras VM en la misma máquina anfitriona?
- ✓ ¿Son las VM inactivas analizadas con regularidad en busca de vulnerabilidades conocidas y se instalan y actualizan las revisiones de seguridad?
- ✓ ¿Se quitan correctamente de la infraestructura virtual las VM retiradas?
- ✓ ¿Qué tratamiento reciben los datos previamente asociados a una VM retirada?

Aunque muchas de las preguntas anteriores son también válidas para los entornos físicos, es posible que se cree a una cultura de la velocidad, debido a la rapidez con que las VM son implementadas, puestas en línea y retiradas, así como a la constante presión ejercida sobre la TI para que sea flexible y responda a las necesidades empresariales, que deje de lado la prudencia. Por ejemplo, poner en marcha un servidor físico

puede llevarle varias semanas a la típica empresa de informática. Estos son algunos de los pasos que pueden ser necesarios dar para poner en funcionamiento un nuevo servidor físico:

- ✓ Definir las especificaciones de hardware y software para cumplir los requisitos comerciales.
- ✓ Confeccionar una lista de materiales y obtener presupuestos competitivos de varios distribuidores.
- ✓ Conseguir la aprobación del presupuesto y encargar los hardware y software necesarios.
- ✓ Encontrar espacio para el equipo físico en el centro de datos, evaluar los requisitos de alimentación y ventilación y, en caso necesario, procurarse más espacio físico e infraestructura para alimentación y ventilación.
- ✓ Instalar y cablear el hardware nuevo, incluyendo los servidores y los equipos de almacenamiento y redes.
- ✓ Instalar los sistemas operativos de los servidores y las aplicaciones necesarias y configurar los ajustes de sistema apropiados.

Al estar acostumbrados los clientes y usuarios internos a tener que esperar varias semanas antes de que los nuevos sistemas y aplicaciones sean puestos en línea, los departamentos de informática ganan tiempo para realizar muchas actividades importantes. Por ejemplo, tras definir las especificaciones de hardware y software de un nuevo sistema o aplicación, se puede analizar la capacidad y el rendimiento de referencia e identificar las dependencias del sistema con la infraestructura del momento para así determinar si es posible instalar el nuevo sistema o aplicación en sistemas ya existentes. Entonces, tras pasarse varias horas instalando un sistema operativo base, los administradores del sistema casi siempre dedican el tiempo necesario para descargar e instalar los últimos paquetes de servicio y revisiones de seguridad y de software.

Sin embargo, en un entorno virtual los usuarios finales pueden acostumbrarse con rapidez a la situación ‘en el momento en que se pida’ según la cual, desde que alguien solicita una nueva VM con carácter inmediato hasta que es puesta en marcha sólo transcurren unos minutos. En un entorno tan vertiginoso es posible que se pasen por alto etapas importantes de planificación y análisis, incluyendo las configuraciones de seguridad. Usa siempre herramientas de seguridad que hayan sido diseñadas para trabajar con los aspectos dinámicos del entorno virtual y puedan detectar los problemas automáticamente y proteger las VM al instante.

Cumplimiento normativo

Movidos por la necesidad de proteger los datos privados (tales como la información personal identificable, los datos financieros y los informes médicos) de la ciudadanía frente a ciberdelincuentes y ladrones de identidades, gobiernos de todo el mundo han hallado agujeros normativos en todos los niveles. Las prácticas recomendables de la seguridad de la información están siendo codificadas con rapidez mediante mandatos legales que buscan garantizar que la política corporativa, los controles internos, los procesos comerciales y las operaciones empresariales de los distintos sectores se encuentren a salvo.



Con más de 400 normas y más de 10 000 controles solapados en más de 50 países de todo el mundo, el cumplimiento normativo se ha convertido en todo un reto y un mandato complejo para cada organización.

Estas normas a menudo requieren de controles específicos, programas corporativos de cumplimiento normativo, auditorías y procesos de divulgación pública, e imponen severas sanciones por incumplimiento. Éstas son algunas de las normas más relevantes sobre la seguridad de la información y los datos:

- ✓ **FISMA (ley federal sobre gestión de la seguridad de la información):** aplicable a las agencias y contratistas del gobierno de los EE. UU. Exige la aplicación de los procesos de seguridad de la información de acuerdo con los FIPS (normas federales de procesamiento de la información) y el NIST (instituto nacional de normas y tecnología).
- ✓ **HIPAA (ley de transferibilidad y responsabilidad de los seguros médicos):** estas reglas de seguridad y privacidad son aplicables a las “entidades afectadas” y sus socios comerciales de la industria sanitaria.
- ✓ **HITECH (ley de tecnología de la información sanitaria para la salud económica y clínica):** proporciona, entre otras cosas, fondos para la financiación de historias clínicas digitales(HCE) y exclusión de responsabilidad ante peticiones de divulgación relacionadas con la violación de información cifrada.
- ✓ **PCI DSS (norma de seguridad de datos de la industria de las tarjetas de pago):** mandato industrial que establece los requisitos de seguridad de la información para organizaciones que procesan transacciones con tarjeta (tales como las tarjetas de crédito y débito).
- ✓ **SOX (Sarbanes-Oxley):** las empresas de capital abierto deben poner en práctica un sistema de control informático. Algunos mandatos no pueden ser llevados a cabo sin el uso prudente de la seguridad para la tecnología y la información.

El rápido ritmo y constante evolución propios de la tecnología hacen que alcanzar y mantener el cumplimiento normativo sea muy difícil. Además, los requisitos normativos a menudo se quedan atrás con respecto a tecnologías concretas y sus repercusiones en la seguridad. Aunque la mayor parte de los requisitos normativos no van dirigidos a tecnologías concretas (de éstas, el cifrado es una destacada excepción), algunos organismos reguladores han comenzado a aceptar la realidad de que la virtualización se ha convertido en una práctica importante en los centros de datos de todo el mundo.

Por ejemplo, el *PCI Security Standards Council* (SSC, consejo de normas de seguridad de la industria de tarjetas de pago) ha publicado directrices para la virtualización. Estas directrices no son requisitos normativos adicionales, sino que proporcionan definiciones estándar de conceptos y tecnologías de virtualización, abordan peligros específicos de los entornos virtualizados y realizan recomendaciones para remediar los riesgos de seguridad de un entorno virtual o en la nube.

Las directrices de virtualización PCI DSS (de junio de 2011) presentan cuatro principios aplicables a la virtualización en los entornos de datos de titulares de tarjetas. Dichos principios, en síntesis, son los siguientes:

- ✓ Los requisitos de la PCI son aplicables a las tecnologías de virtualización empleadas en los entornos de titulares de tarjetas.
- ✓ La virtualización entraña riesgos exclusivos que deben ser evaluados.
- ✓ A la hora de implementar la virtualización, es necesario llevar a cabo detección, identificación y documentación minuciosas del entorno.
- ✓ No existen soluciones universales para la seguridad en un entorno virtualizado.

Algunos de los peligros abordados en las directrices de virtualización PCI, de los cuales hablaré con más detalle a lo largo de este libro, son los siguientes:

- ✓ Las vulnerabilidades de los entornos físicos son también aplicables a los entornos virtuales.
- ✓ Los hipervisores crean una nueva superficie susceptible de ataque.
- ✓ Los entornos virtuales presentan una mayor complejidad.
- ✓ La virtualización acaba con el modelo de implementación según el cual cada servidor físico cumple una sola función.
- ✓ Coexisten en el mismo anfitrión físico varias máquinas virtuales (VM) con distintos niveles de confianza (por ejemplo, las aplicaciones orientadas al interior y al exterior y las distintas directivas de seguridad).

- ✓ No hay separación de tareas entre los administradores del sistema, pues todos necesitan tener acceso a los entornos virtuales.
- ✓ Revisiones y actualizaciones para las VM inactivas.
- ✓ Información confidencial contenida en imágenes e instantáneas de las VM.
- ✓ Registro y seguimiento insuficientes en el entorno virtual.
- ✓ Filtración de información entre los segmentos y los componentes de las redes virtuales.

Aunque las diferencias entre los entornos físicos y virtuales puedan parecer obvias, es esencial que conozcas los detalles para poder así realizar una evaluación y diseño correctos de las soluciones de seguridad que implementas en tu entorno virtual. En el Capítulo 2 explicaré algunos de los retos específicos de seguridad técnica en un entorno virtual.

Nube y virtualización

El crecimiento de la informática en la nube ha sido propiciado por la virtualización y su menor coste en cuanto a recursos informáticos, al permitir que varias entidades no relacionadas comparten dichos recursos. Gracias a la alta densidad de VM y a un aprovechamiento del hardware aún mayor en la infraestructura de la nube, los proveedores de la nube pueden ofrecer sus productos con una buena relación calidad-precio y permitir un fácil acceso a empresas de todos los tamaños. La capacidad de aumentar y reducir la potencia de procesamiento en un instante permite proporcionar la flexibilidad necesaria para mejorar el equilibrio entre los requisitos informáticos y la demanda de los usuarios y del mercado. Actualmente, muchas empresas incluyen los recursos de la nube en la mezcla informática que usan a diario, lo cual ha dado lugar a un nuevo modelo de entornos híbridos que combina sistemas físicos y virtuales para la implementación individual o de servidor (tanto en los lugares de las empresas como en centros de datos corporativos) e incorpora de modo transparente la computación en la nube a la mezcla. Los beneficios son obvios, ya que las empresas pueden proveer con mayor facilidad infraestructuras basadas en una serie de variables (como las necesidades según la temporada), funciones individuales o pueden usar el mejor tipo de recurso informático para cumplir con las normativas.

Capítulo 2

Seguridad del servidor virtual

En este capítulo

- ▶ Retos de seguridad de un entorno virtual
- ▶ Uso de la solución de seguridad adecuada para tu entorno
- ▶ Protección de datos en la red

Las herramientas de seguridad diseñadas para sistemas físicos poseen limitaciones que restringen su eficacia en entornos virtuales. Estas limitaciones pueden también reducir o eliminar muchos de los beneficios de la virtualización cuando las herramientas de seguridad diseñadas para sistemas físicos se implementan o asignan a los entornos virtuales. En este capítulo explicaré esos retos y el modo en que afectan negativamente a los entornos de servidores virtuales, así como la manera en que las soluciones de seguridad compatibles con el entorno virtual pueden ayudar a abordar dichos retos.

Retos de seguridad específicos del entorno virtual

Una plataforma para software de infraestructura virtual es en esencia un entorno de alojamiento virtual expuesto a los mismos problemas de seguridad que los entornos físicos y que tiene además algunos retos adicionales exclusivos de los sistemas virtuales. El hipervisor de un entorno virtual es, de alguna manera, análogo al router de red de un entorno físico. Cada máquina virtual (VM) y aplicación hacen pasar su tráfico de red a través del hipervisor de camino a otros sistemas virtuales o físicos o a dispositivos del cliente. Dado que el hipervisor es parte de un sistema cerrado dentro de la infraestructura virtual, muchos productos de seguridad (por ejemplo, los cortafuegos y los sistemas de detección de intrusiones/sistemas de prevención de intrusiones (IDS/IPS) en

la red) no pueden ver el tráfico del hipervisor y crean, por tanto, una importante zona de exposición y un vector de ataques muy atrayente, especialmente debido a la variada mezcla de aplicaciones que pueden instalarse a modo de VM en una máquina anfitriona física.

La imposibilidad de visualizar el tráfico entre máquinas virtuales genera un riesgo inaceptable debido a la existencia de posibles amenazas desconocidas circulando por el hipervisor. Es además la causa de potenciales problemas de rendimiento que son en realidad provocados por agentes de seguridad tradicionales, tales como el software de antimalware instalado en VM individuales que descarga, de manera programada, archivos de firmas actualizados. Estas condiciones afectan negativamente a la seguridad y al rendimiento de un entorno virtual, así como a sus potenciales beneficios, debido a la menor densidad de VM por anfitrión físico.

Por último, las VM inactivas y las migraciones de VM también pueden dar lugar a retos de seguridad propios del entorno virtual.

Comunicaciones entre máquinas virtuales

La implementación de un entorno virtual no cambia el modo en que uno debería diseñar el entorno de su sistema. Al igual que sucede en un entorno físico, tus sistemas y aplicaciones privados o internos deben estar separados de tus sistemas y aplicaciones públicos u orientados al exterior. Evita siempre poner los sistemas y aplicaciones orientados al interior y al exterior en el mismo hardware físico. Si mezclas aplicaciones orientadas al interior (por ejemplo, el sistema de nóminas de una empresa) y al exterior (por ejemplo, una aplicación web para socios), puedes estar exponiendo al mundo exterior, sin necesidad alguna, las aplicaciones internas que contienen información confidencial. Una VM orientada al exterior proporciona una puerta de entrada a todas las demás VM de la misma máquina anfitriona a través del hipervisor (ver diagrama 2-1).

Según investigaciones realizadas en el sector, hasta un 70 por ciento de las VM está orientada al exterior, lo que significa que hay muchas probabilidades de que haya usuarios que no conoces o en los que no confías y que no puedes controlar su acceso a al menos una de aplicaciones que se ejecutan en la máquina anfitriona de tu VM.



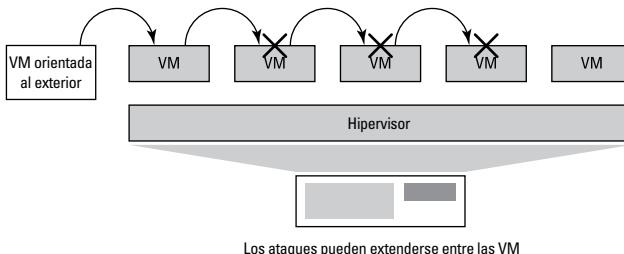


Diagrama 2-1: una VM orientada al exterior puede usarse como trampolín para atacar otras VM de la misma máquina anfitriona a través del hipervisor.

Las VM se comunican por medio del hipervisor en el caso de las operaciones habituales entre clientes y servidores (tráfico de norte a sur) y de las comunicaciones entre servidores de VM (comunicaciones entre máquinas virtuales o tráfico de este a oeste). Las comunicaciones entre máquinas virtuales pueden exponer a las VM a tráfico imprevisto (por ejemplo, a una mezcla de diferentes tipos de aplicaciones). Las herramientas de seguridad tradicionales, tales como los cortafuegos y los IDS/IPS utilizados para gestionar y proteger los sistemas físicos que funcionan en un segmento de red física, no pueden supervisar las comunicaciones entre máquinas virtuales dentro de un entorno virtual. Esto significa que tus cortafuegos y IDS/IPS tradicionales no pueden proteger tus VM de muchos tipos de ataques porque sólo pueden ver el tráfico entre sistemas físicos. Para supervisar y proteger el tráfico entre las VM, se necesitan soluciones de seguridad diseñadas para funcionar en un entorno virtual y que puedan tanto supervisar y proteger las comunicaciones entre máquinas virtuales.

Aprovechamiento de recursos

Otro de los principales beneficios de la tecnología de virtualización es que maximiza el uso eficiente de los recursos del servidor físico. Muchas de las aplicaciones típicas para servidores aprovechan como mucho un 5 por ciento de la capacidad total de una CPU y sólo entre un 30 y un 40 por ciento de la memoria disponible en el servidor físico.

Debido a este bajo nivel de aprovechamiento y al exceso de capacidad disponible en los servidores físicos, el software de seguridad tradicional que se ejecuta en el hardware de servidores dedicados tiene normalmente todos los recursos de CPU, memoria y E/S que necesita para llevar a cabo sus operaciones de seguridad

y raramente tiene que competir con otras aplicaciones de software por dichos recursos. Por ejemplo, el software antimalware tradicional emplea tantos recursos disponibles del servidor como le son precisos para desempeñar funciones tales como analizar y poner en cuarentena los archivos infectados. El software de seguridad también suele experimentar fuertes altibajos en cuanto a demanda de recursos se refiere: a veces le basta con un mínimo de recursos para supervisar ciertas actividades del servidor o desencadenar eventos y otras veces necesita numerosos recursos para analizar y proteger rápidamente el servidor frente a una nueva amenaza.

En un servidor físico dedicado, este modelo de asignación de recursos funciona relativamente bien, ya que todos los recursos del servidor físico están disponibles para el sistema operativo (SO), sus aplicaciones instaladas y el software de seguridad. El SO gestiona todos los recursos disponibles y garantiza que las tareas de seguridad reciban la prioridad adecuada, de modo que el SO y todas las aplicaciones que se estén ejecutando funcionen correctamente y estén protegidas de manera apropiada.

En el diagrama 2-2 se muestra la implementación típica de las aplicaciones individuales instaladas en servidores físicos separados. En cada uno de los servidores físicos se instala un agente de seguridad para analizar y proteger el SO y las aplicaciones. Los agentes de seguridad individuales se comunican con el sitio externo para actualizar la información sobre amenazas que posee.

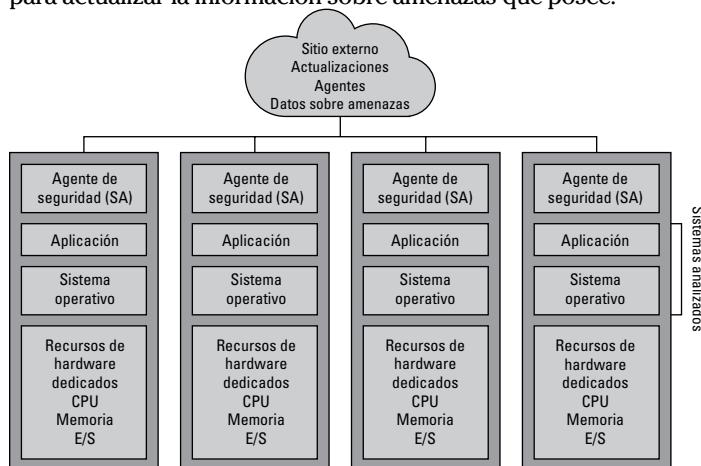


Diagrama 2-2: servidores físicos tradicionales con aplicaciones individuales y agentes de seguridad instalados.

Comparativamente, en un entorno virtual el aprovechamiento de los recursos informáticos de una máquina anfitriona física tenderá a ser muy superior a la media. En un entorno virtualizado, el hipervisor (ver el Capítulo 1) gestiona la asignación de los recursos de la máquina anfitriona física entre todas las VM que se ejecutan en ese anfitrión. Pero por muy grande que sea el servidor físico que se utilice para hacer funcionar este ecosistema virtual, sigue habiendo una cantidad fija de recursos de hardware (tales como la CPU, la memoria o la E/S).

El software de seguridad diseñado para los sistemas físicos no es eficaz en el entorno virtual, esto es, no cuenta con mecanismos para detectar que está instalado en un entorno virtualizado, en el que tiene que compartir los recursos del servidor con las muchas VM de la misma máquina virtual física. Aunque el hipervisor está diseñado para manejar los fuertes altibajos de demanda de recursos, cuando el software tradicional de seguridad se ejecuta en un entorno virtual puede causar problemas a todas las VM implementadas en ese anfitrión físico. Por ejemplo, si hay varias VM instaladas en un único anfitrión físico y cada VM ejecuta un agente de seguridad antimalware tradicional, el desencadenamiento de un sólo evento puede hacer que todas las VM realicen simultáneamente un análisis de sistema completo. Esto puede causar que los recursos del sistema disponibles en el anfitrión físico se agoten de inmediato y las aplicaciones alojadas dejen de funcionar.

El diagrama 2-3 muestra el software tradicional de seguridad antivirus/antimalware basado en un agente diseñado para un sistema físico, pero que se ha implementado en un entorno virtual. Como en el modelo de implementación física, los agentes de seguridad instalados analizarán los archivos individualmente en busca de amenazas dentro de cada VM y realizarán periódicamente análisis parciales o completos del sistema, las aplicaciones y los archivos de cada VM. Los agentes de seguridad individuales se comunicarán también regularmente con un sitio externo para actualizar su información sobre amenazas, lo que puede hacer que el sistema anfitrión físico y a la red se ralenticen.

Estos conflictos de recursos pueden llevar a las empresas de informática a realizar prácticas poco recomendables, como asignar recursos excesivos para cubrir actividades y análisis de seguridad dinámicos, de alto consumo de recursos en ciertas ocasiones y garantizar así que sus aplicaciones virtualizadas alcancen un rendimiento aceptable. Por desgracia, tener que considerar la naturaleza intermitente de dichos agentes de seguridad puede reducir significativamente el número de VM que pueden instalarse en una plataforma anfitriona.

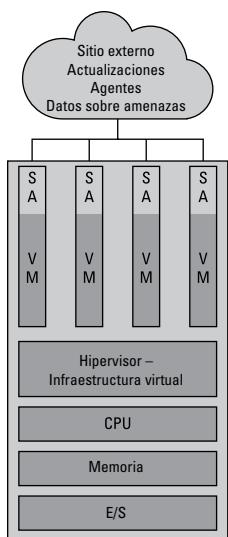


Diagrama 2-3: agentes de seguridad tradicionales diseñados para los sistemas físicos instalados en un entorno virtual.

VM inactivas

Los *servidores inactivos*, es decir, los servidores que han sido desconectados o no han funcionado durante largo tiempo, presentan retos de seguridad en todos los entornos de centros de datos, ya sean físicos o virtuales. Los servidores inactivos (o VM inactivas en un entorno virtual) suelen pasar desapercibidos cuando se aplican como parte del ciclo normal de mantenimiento actualizaciones del sistema operativo, parches de seguridad y actualizaciones o archivos de firmas contra amenazas. Cuando estos servidores inactivos son conectados y puestos en funcionamiento, pueden ser más vulnerables a amenazas contra las que previamente se han aplicado parches o actualizaciones en otros sistemas de producción. Así, un servidor inactivo puede poner todo tu centro de datos en peligro al facilitar un punto de entrada a tu red.

En un entorno de servidores físicos, los servidores inactivos son normalmente menos predominantes que en los entornos virtuales. Muchas empresas de informática carecen de herramientas de gestión para conectar o desconectar con facilidad el hardware de los servidores físicos de un centro de datos remoto. El hardware físico es también relativamente caro. Por tanto, la mayor parte de las organizaciones normalmente sólo adquiere nuevo hardware para

servidores cuando es necesario y prefieren no tenerlo inactivo y ocupando el valioso espacio de las estanterías del centro de datos. De hecho, la ausencia de “lucecitas parpadeantes” en una estantería haría que la mayoría de los administradores informáticos sufriesen un breve ataque de pánico, temiendo que un sistema de producción se hubiese apagado inesperadamente o hubiese empezado a funcionar mal.

En cambio, una VM inactiva en un entorno virtual es una cuestión completamente distinta. La facilidad con que las VM pueden ser creadas y conectadas o desconectadas (como se muestra en el Capítulo 1) y la falta en general de costes adicionales reales asociados con VM inactivas conduce a la proliferación de servidores en el centro de datos.

Otros muchos sistemas y tecnologías del centro de datos pueden también aprovechar la capacidad del entorno virtual de crear o conectar las VM de modo dinámico, como ocurre cuando un servidor se bloquea o se alcanza un umbral de carga. Por ejemplo, los equilibradores de carga pueden conectar automáticamente más servidores web virtuales durante períodos de máxima actividad para así mantener el nivel de rendimiento requerido por un sitio web con muchas visitas. Un servidor web con VM inactivas al que no se le hayan aplicado los parches adecuados podría poner en peligro casi al instante toda la infraestructura de una empresa si se conecta automáticamente mediante un equilibrador de carga.



Las herramientas de gestión centralizadas (como, por ejemplo vCenter y VMware) pueden ayudar a los administradores informáticos a controlar todas las VM de un entorno virtual (incluyendo las inactivas). No obstante, la aplicación de parches y actualizaciones a las VM inactivas sigue siendo en gran medida una tarea de seguridad manual, aunque importante, en la mayoría de los casos.

Migraciones de VM

Otra característica importante de los entornos virtuales es la capacidad de trasladar las VM entre anfitriones físicos para gestionar de modo dinámico los recursos o cargas de los servidores o con fines de recuperación ante desastres. Una VM puede ser trasladada de un anfitrión físico a otro dentro del mismo centro de datos o a otros centros ubicados en cualquier lugar del mundo.

Las migraciones de VM conllevan complejos retos de seguridad entre los que se incluyen los siguientes:

- ✓ ¿Cómo garantizar que se aplican las directivas de seguridad adecuadas al trasladar VM individuales de un anfitrión físico o centro de datos a otro?
- ✓ ¿Qué sucede cuando una VM es trasladada a una máquina anfitriona física con un nivel distinto de protección de seguridad?
- ✓ ¿Cómo se protege una VM al migrarla de un anfitrión físico a otro?

Los cortafuegos e IDS/IPS tradicionales están instalados en segmentos de redes físicas y, por ello, no pueden proteger las VM de manera adecuada ya que éstas migran de un anfitrión físico a otro o de un centro de datos a otro.



Tener una solución de seguridad *adherente* (es decir, aquella que se desplaza junto con una VM determinada), tanto si es sin agente como basada en un agente, te permite tener distintos ajustes de seguridad para cada VM de tu entorno virtual, independientemente de la máquina anfitriona física en la que esté ubicada una VM determinada en un momento dado.

Cómo abordar los retos de seguridad virtual con soluciones compatibles con el entorno virtual

Una solución de seguridad compatible con el entorno virtual está diseñada tanto para entornos virtuales como físicos. Con este tipo de solución se pueden instalar agentes de seguridad individuales en servidores físicos dedicados cuando se requiera. En el entorno virtual se puede implementar un aparato virtual (ver diagrama 2-4) que desempeñe todas las funciones de una solución de seguridad como si fuera una sola VM. El aparato virtual supervisa todos las VM a través del hipervisor. De ese modo, no se necesita agente en las VM individuales y el aparato puede ver todo el tráfico entre máquinas virtuales en el hipervisor. El aparato virtual se comunica directamente con un sitio externo para descargar información actualizada sobre amenazas, la cual se usa para proteger todas las VM a la vez, incluyendo las VM inactivas. Este diseño reduce considerablemente el tráfico de red y el uso de los recursos del anfitrión físico. En un entorno virtual con muchos recursos concurrentes, la seguridad sin agente es el modo más eficaz de

proporcionar protección consistente y maximizar la densidad de las VM por anfitrión.

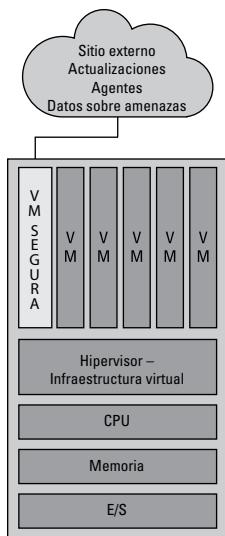


Diagrama 2-4: aparato de seguridad (VM segura) compatible con el entorno virtual instalado en un entorno virtual.

Además de un aparato virtual sin agente, una solución de seguridad completa, compatible con el entorno virtual, proporciona herramientas basadas en agente que son asimismo aptas para el entorno virtual ante diferentes casos de implementación y necesidades comerciales. Por ejemplo, puede que necesites utilizar un agente al trasladar una de tus VM a un proveedor de servicios en la nube. Puedes instalar un agente en la VM y seguirlo hasta la nube, lo que te proporciona el mismo nivel de protección que si la VM estuviese aún en tu centro de datos y te permite gestionar la seguridad de la VM remotamente desde tu consola local.

Las herramientas de seguridad tanto sin agente como basadas en agente tienen usos apropiados en entornos físicos, virtuales, en la nube e híbridos. Para obtener la máxima flexibilidad, necesitas una solución de seguridad compatible con el entorno virtual, sin agente y basada en agente, que te permita seleccionar el tipo de implementación que mejor se adapte a tu caso sin que afecte de manera negativa al rendimiento.



La protección de datos en la nube

El uso de la informática en la nube ha aumentado enormemente y ha generado todo un nuevo modelo empresarial. Ofrece a las empresas la posibilidad de modificar la disponibilidad de sus recursos informáticos de manera rápida, fácil y barata y de adaptarse a las exigencias de los recursos informáticos dinámicos. De modo que ¿cómo se protegen las empresas frente a los peligros específicos de la nube? ¿Cómo se asegura una empresa de que sus datos en la nube tengan el mismo nivel de protección que cuando se accede a ellos y se almacenan en su propio centro de datos?

Los proveedores de servicios en la nube quieren que tus datos estén seguros. Les interesa que emplees las herramientas apropiadas para proteger tus aplicaciones virtuales en la VM de las VM de otras organizaciones que se ejecutan en la misma máquina anfitriona o están almacenadas en el mismo espacio. Estas funciones (como se muestra en el Capítulo 4) han de permitirte supervisar y bloquear las amenazas que puedan surgir de otras aplicaciones virtuales. También debería ser posible proteger aplicaciones específicas o archivos y directorios confidenciales.

En el mundo compartido de la nube, tus datos están más expuestos porque circulan por redes compartidas y se guardan en dispositivos de almacenamiento compartidos con los datos de otros clientes de la nube. Además, la ubicación de tus datos almacenados puede cambiar en base a muchos factores que se hallan fuera de tu control. El hecho es que un proveedor de servicios en la nube puede trasladar, y trasladará, tus aplicaciones virtuales entre anfitriones físicos y tus datos de un entorno de almacenamiento a otro.



Es posible que el movimiento de datos dé lugar a problemas puesto que pueden quedar restos legibles de tus datos en una antigua ubicación de almacenamiento. Para proteger los datos que viajan por redes compartidas y son almacenados de manera compartida, es necesario adoptar un enfoque que se centre más en los datos. Trata de emplear un componente de seguridad que te permita establecer directivas de acceso y almacenamiento de datos en la nube (esto también puede funcionar en tu propio centro de datos). Asimismo, sírvete del cifrado para garantizar que los datos no puedan ser leídos cuando circulen o sean almacenados en la nube. Este sistema te permite establecer y hacer cumplir directivas para la protección de datos mediante un servidor de directivas que te pertenece y el cual controlas. Se trata en parte de utilizar claves para cifrar y descifrar datos, con derechos definidos de acceso a las claves y los datos de acuerdo con las directivas de tu empresa.

Capítulo 3

Seguridad de la infraestructura de escritorio virtual (VDI)

En este capítulo

- ▶ Reconocimiento de los problemas con productos de seguridad tradicionales en las implementaciones de la VDI
- ▶ Cómo dar con la mejor seguridad para la VDI
- ▶ Gestión del acceso a datos y la seguridad con la VDI
- ▶ Trabajo con la VDI y la nube

La virtualización de escritorio se ha ido extendiendo durante los últimos cinco años. Constituye un paso lógico para las empresas de informática que ya han adoptado la virtualización del servidor en sus centros de datos. Dichas empresas han adquirido los conocimientos y la experiencia necesarios para llevar a cabo la expansión requerida para la virtualización de escritorio. La virtualización de escritorio es coherente con la tendencia actual del BYOD (“trae tu propio dispositivo”, por sus siglas en inglés), que ha llevado a la proliferación del número y el tipo de dispositivos que los usuarios llevan al trabajo.

En este capítulo aprenderás por qué los productos tradicionales de seguridad para escritorio y las infraestructuras de escritorio virtual (VDI) no casan bien y cómo la VDI misma puede proporcionar un mayor control sobre el acceso y la seguridad de datos.

Los retos de seguridad de la VDI

A medida que el BYOD va ganando aceptación, empresas de todos los tamaños se ven en la necesidad de dar con distintas maneras de enfocar la seguridad del punto de destino. Cada vez es más habitual no tener ni la propiedad ni el control de los dispositivos que acceden a tus sistemas e información, por lo que las soluciones de seguridad para el punto de destino, tales como el software antimalware y los cortafuegos personales, son mucho menos prácticos. Por ejemplo, una empresa pequeña puede usar un servicio de facturación de terceros para introducir la información de un cliente en sus sistemas o un profesional sanitario puede trabajar en su despacho o en el hospital y usar sus dispositivos personales (como teléfonos inteligentes y tabletas) en ambos lugares para acceder al historial de sus pacientes. En ambos ejemplos la cuestión gira entorno a cómo hacer lo siguiente:

- ✓ Proteger tus sistemas e información sin poder controlar directamente los dispositivos del usuario final.
- ✓ Permitir el acceso únicamente a las aplicaciones necesarias para realizar una labor específica.
- ✓ Asegurarte de que tus sistemas e información no se vean amenazados por un dispositivo que haya sido infectado con malware.



El *malware* es software o código malicioso que normalmente daña o inutiliza un sistema informático o toma control o roba información del mismo. El malware incluye generalmente virus, gusanos, troyanos, bombas lógicas, rootkits, bootkits, puertas traseras, spyware y adware.

En una infraestructura de escritorio virtual (VDI, por sus siglas en inglés) se alojan varios sistemas operativos para escritorio y/o aplicaciones a modo de máquinas virtuales (VM) en un servidor físico que ejecuta un hipervisor (ver diagrama 3-1). Al ejecutar productos de seguridad tradicionales tanto en un entorno de VDI como en un entorno de servidor virtual surgen algunos problemas importantes (ver Capítulo 2). Los productos tradicionales de seguridad de servidores se ejecutan en la máquina anfitriona, no en los escritorios virtuales, por lo que no pueden llevar a cabo análisis o gestionar recursos entre los escritorios virtuales. Estas limitaciones pueden hacer que la aplicación del anfitrión se ralentice e incluso deje de responder a las peticiones del cliente del escritorio virtual.



Diagrama 3-1: escritorio virtual ejecutándose en un entorno de VDI.



La VDI no es la única tecnología de virtualización de escritorio disponible, pero se está convirtiendo rápidamente en una de las implementaciones de escritorios virtuales más populares. Otras tecnologías de virtualización de escritorio incluyen: la virtualización de aplicaciones para servicios de escritorio remoto, la virtualización de usuario, la disposición en capas, *Desktop as a Service* (DaaS, escritorio según demanda) y la virtualización de escritorio local.

Los problemas son aún peores en el caso de los productos tradicionales de seguridad para escritorio instalados en escritorios virtuales individuales. Por ejemplo, cuando muchos usuarios inician sesión en su escritorio virtual más o menos simultáneamente, como por ejemplo al inicio de la jornada laboral, los métodos de análisis tradicionales pueden paralizar todo un entorno de VDI. Un producto tradicional de seguridad para escritorio normalmente analiza un sistema de escritorio entero cuando un usuario inicia sesión, ya sea porque está programado para realizar el análisis tras iniciarse correctamente la sesión o porque el último análisis programado (quizá un análisis nocturno a las 3 de la mañana) no ha podido llevarse a cabo debido a que el escritorio virtual estaba inactivo en ese momento.

A medida que los usuarios individuales acceden a las distintas aplicaciones y datos a lo largo de la jornada, se realizan más análisis de acuerdo con las directivas normalmente establecidas en base a un modelo de “un solo usuario por cada escritorio físico”. En cambio, en un entorno de VDI muchos escritorios virtuales comparten los mismos procesadores y la misma memoria de un único servidor físico. Debido al hecho de que estas directivas de análisis se aplican sin tener en cuenta la disponibilidad de recursos y de que los productos tradicionales

de seguridad para escritorio no son capaces de detectar los problemas de conflicto de recursos que puedan surgir, el impacto en el rendimiento de los escritorios virtuales puede ser frustrante para los usuarios finales.

Además, los productos tradicionales de seguridad para escritorio suelen analizar todo lo que hay en un ordenador de sobremesa, sin tener en cuenta si ha habido cambios desde el último análisis en los directorios, archivos, perfiles de usuario o en cualquier otro elemento. Los análisis en masa suponen un gran esfuerzo de uso de recursos (al contrario que los análisis inteligentes, que sólo se ejecutan cuando hay cambios) sin que ello tenga necesariamente ningún beneficio real en la seguridad.



En un entorno de VDI las limitaciones de los productos tradicionales de seguridad para escritorio pueden afectar significativamente al número de usuarios que tengan la posibilidad de acceder a cualquiera de los escritorios o aplicaciones de anfitriones de VDI lo que, a su vez, limita los beneficios que se obtendrán de la virtualización de escritorio.

Cómo dar con el mejor tipo de seguridad para trabajar con la VDI

La conclusión es que las soluciones de seguridad tienen que ser capaces de adaptarse a los distintos entornos virtuales que encontramos en las empresas actuales. Con la VDI tu software de seguridad debe poder adaptarse a tu entorno informático, sea éste físico o virtual. Ello incluye la capacidad de hacer lo siguiente:

- ✓ Analizar y proteger frente a las amenazas que se presentan con mecanismos de análisis inteligentes para evitar así que el acceso de los usuarios de la VDI sufra retrasos.
- ✓ Analizar sólo aquello que ha cambiado, o únicamente archivos en vez de todo el sistema de escritorio, para reducir la demanda de recursos compartidos y permitir una mayor densidad de VDI por máquina anfitriona.
- ✓ Emplear protección inteligente que mantenga automáticamente el rendimiento y el acceso al sistema y al escritorio.
- ✓ Analizar los escritorios virtuales inactivos de la máquina anfitriona de la VDI.
- ✓ Proteger el hipervisor de la máquina anfitriona de la VDI.

Estas funciones pueden marcar una enorme diferencia en lo que respecta a las posibilidades de uso de un entorno de VDI y, por tanto, permitir que tu empresa conecte un número mayor de usuarios a un escritorio o aplicación anfitriona de VDI. Lee el texto del cuadro “Trend Micro Deep Security protege los entornos de VDI y reduce costes” a modo de ejemplo de cómo una gran organización puede lograr una mayor densidad de VDI por máquina anfitriona y ahorrar considerablemente en costes.

Gestión del acceso a datos y la seguridad con la VDI

En un entorno de VDI los datos de tu empresa se alojan en tus servidores internos, lo cual reduce la exposición a numerosas amenazas. Por ejemplo, tus datos sólo pueden verse durante una sesión de usuario y no pueden ser descargados o guardados en el escritorio local de un usuario. Estas características pueden por sí solas mitigar considerablemente muchos de los peligros asociados con el BYOD ya que evitan de hecho que se pierdan datos debido al extravío de un dispositivo o a la intrusión de terceros en el mismo, lo que reduce en gran medida el riesgo la sustracción de información importante. En el caso, ya comentado anteriormente en este capítulo, del empleado de hospital que accede al historial de un paciente desde una tableta, crear una sesión de VDI garantizaría que nunca se almacenase información en dicho dispositivo. El empleado puede acceder directa y fácilmente a la información desde una aplicación del servidor en el que dicha información estará alojada y protegida por los distintos sistemas de seguridad del hospital.

La VDI ayuda a las organizaciones a cumplir con los diferentes requisitos normativos, en especial con las disposiciones que requieran estrictos controles de acceso y mecanismos para la prevención de pérdida de datos y así proteger determinada información. La VDI también hace más fácil probar el cumplimiento normativo en auditorías internas y externas. Por último, la VDI puede reducir en gran medida el alcance y el coste de las solicitudes de pedido de presentación de pruebas electrónicas asociadas a citaciones o peticiones legales de conservación de documentos; ello se debe a que se tiene constancia del número de máquinas anfitrionas de la VDI en las que está alojada la información y pueden encontrarse con relativa facilidad, al no estar dispersas por cientos o miles de escritorios en las numerosas ubicaciones geográficas de la organización.

Uso de la VDI en la nube

Muchas empresas que ya usan una mezcla informática híbrida pueden valerse de la infraestructura de la nube para implementar una VDI. Por ejemplo, cuando se necesita contratar personal temporal en periodos de aumento de la actividad. La VDI en la nube puede ayudarte a añadir recursos para eventuales de modo rápido a la vez que proteges tus datos. Puedes facilitar el acceso de los trabajadores temporales de manera sencilla y rentable y no permitir que usen aplicaciones específicas, con lo que garantizas el almacenamiento seguro de tus datos y les impides explorar tu red o guardar y almacenar tus datos localmente.

Trend Micro Deep Security protege los entornos de VDI y reduce costes

La VDI es la categoría de virtualización que crece con mayor rapidez. Las organizaciones que adoptan la VDI buscan una sólida seguridad de escritorio y la máxima densidad de servidor. Esto puede lograrse mediante soluciones de seguridad sin agente, en las que se ha observado que las densidades de servidor son entre un 60 y un 200 por ciento superiores a sus equivalentes basadas en agente.

Por ejemplo, una organización con 1000 escritorios provistos de VDI, en cada uno de los cuales se ha instalado un sistema de seguridad heredado basado en agente, sólo puede instalar unos 50 escritorios con VDI por cada servidor físico (según el informe oficial de marzo de 2012 de Osterman Research). Con Trend Micro Deep

Security, una organización puede tener unos 80 escritorios con VDI por cada servidor físico.

De tal modo que, usando Trend Micro Deep Security, el dinero que ahorraría una organización en servidores físicos, costes de licencia de VMware, costes de centros de datos por cada servidor físico cada año y costes de mantenimiento regular, sería del 30 por ciento de la inversión inicial en servidores físicos, software de virtualización y soluciones de seguridad.

Así, usando Trend Micro Deep Security para proteger sus entornos de VDI la organización se ahorra una cantidad considerable de dinero a lo largo de tres años.

Capítulo 4

Las soluciones de seguridad de Trend Micro para el entorno virtual

En este capítulo

- ▶ Cómo hacer frente al volumen y la sofisticación de las amenazas de malware
- ▶ Conocer la solución Trend Micro Deep Security
- ▶ Protección de entornos físicos, virtuales, en la nube e híbridos

Una práctica recomendable en el ámbito de la seguridad es usar herramientas de seguridad diseñadas al entorno que se desea proteger adecuado que sean adecuadas. Con todo, según el Instituto de Seguridad Informática en su estudio 2010–2011 Computer Crime and Security Survey, sólo el 20 por ciento de las herramientas de seguridad empleadas actualmente en entornos virtuales han sido diseñadas para dichos entornos. En este capítulo aprenderás sobre las amenazas globales y las soluciones de seguridad compatibles con el entorno virtual que Trend Micro ha diseñado para proteger entornos informáticos virtuales, en la nube e híbridos.

Protección contra amenazas globales

Hoy en día, las amenazas llegan desde todos los rincones del planeta. Tu organización debe implementar soluciones de seguridad que tengan la capacidad de responder eficazmente a las amenazas, sin importar su origen. Una solución de seguridad completa ha de tener un alcance global para recabar información sobre amenazas de cualquier lugar y, después, analizarla y responder con rapidez, así como ofrecerte la posibilidad de tomar las medidas necesarias y adecuadas para proteger tus sistemas y tu red.

Un vistazo al paisaje

Se han dado cambios en el paisaje de las amenazas en dos importantes áreas: el volumen y la sofisticación. Para proteger tus redes y sistemas de todas esas amenazas necesitas recursos de protección más inteligentes y sólidos de lo que los productos de seguridad tradicionales pueden proporcionarte. Una solución de seguridad eficaz no sólo debe tratar de bloquear las amenazas en los límites de la red y sus varios puntos de acceso; también ha de posibilitar el seguimiento constante y continuo de todos los sistemas informáticos de tu organización.

Incremento del volumen

En la actualidad, se descubren más de 1500 variantes de amenazas de malware cada hora. Eso significa que, posiblemente, los archivos de firma y modelo del software antimalware tradicional, a pesar de actualizarse con regularidad, se quedan desfasados con rapidez y el peligro para servidores y puestos de trabajo aumenta paulatinamente.



Independientemente del tipo de sistema de seguridad que uses para proteger tus plataformas informáticas físicas o virtuales, si dichos sistemas no son capaces de obtener información sobre nuevas amenazas a tiempo, todo tu entorno informático se encontrará en peligro.

El volumen de malware se incrementa en gran medida debido a la acción de hackers de poca pericia (conocidos como *script kiddies*) que lo que hacen es comprar o alquilar kits de malware prefabricado, tales como código fuente de virus y botnets, para promover la creación de variantes de malware o para lanzar rápidos ataques de fuerza bruta contra las redes.

Mayor sofisticación

También la sofisticación de las amenazas modernas se ha incrementado. Ahora las amenazas de malware pueden ir dirigidas contra entornos operativos concretos, incluyendo sistemas virtuales y en la nube. Las amenazas actuales muestran características avanzadas como las siguientes:

- ✓ **Nuevos métodos de infección:** la infección se sirve cada vez más de técnicas como la suplantación de identidad (phishing), los sitios de redes sociales y las descargas automáticas o no seguras. La infección emplea métodos como el cifrado SSL para eludir las soluciones de seguridad tradicionales.
- ✓ **Mecanismos de persistencia:** los rootkits, los bootkits, las puertas traseras y el software contra programas antivirus son ejemplos del malware normalmente usado para garantizar que el atacante pueda seguir infiltrándose en un sistema o red durante más tiempo una vez se ha producido la infección.

- ✓ **Técnicas de comunicación sigilosa:** el cifrado, los proxies, el salto entre puertos y la tunelización son técnicas empleadas para mantener la comunicación con otros sistemas infectados, permitir el comando y control del malware y la extracción de información valiosa de un sistema o red bajo ataque.
- ✓ **Función de comando y control:** esta función permite al atacante controlar, gestionar y actualizar malware para procurarse objetivos de ataque específicos.

Las amenazas modernas resultan aún más inquietantes! Por ejemplo, una *amenaza persistente avanzada* (APT, por sus siglas en inglés) es un tipo de ataque sofisticado dirigido contra una organización que tiene lugar durante un periodo de tiempo prolongado, a veces varios años, con el fin de robar información valiosa y confidencial. Estos tipos de ataques normalmente los realizan organizaciones ilegales o estados-nación corruptos con vastos recursos de piratería informática. Por ello, debes defenderte no sólo contra los script kiddies, sino también frente a ciberdelincuentes profesionales y ciberterroristas.

Una mirada a la red de protección inteligente

Consciente de que el paisaje de las amenazas ha evolucionado rápidamente durante la pasada década, Trend Micro ha desarrollado recursos de protección proactivos y dinámicos.

En 2008 Trend Micro creó un Sistema de Información Global (SIG) denominado Smart Protection Network (SPN, red de protección inteligente) para hacer frente con mayor eficacia al volumen y la sofisticación de las nuevas amenazas en constante evolución. La SPN está formada por más de una docena de centros globales, lo que permite a Trend Micro descubrir información sobre amenazas y compartirlo con sus soluciones de seguridad y, a través de las mismas, difundirla, independientemente de su procedencia.

Eso significa que Trend Micro puede compartir, de manera instantánea y global, información sobre el ataque de un nuevo malware descubierto en cualquier lugar del mundo, sin tener que transferir a los dispositivos protegidos ningún archivo de firma actualizado. Esta técnica reduce considerablemente el tamaño y el número de los archivos que tus dispositivos necesitan. Asimismo, si se descubre una nueva amenaza en uno de los más de 160 millones de dispositivos protegidos por las soluciones de Trend Micro, la información crítica sobre dicha amenaza estará a disposición, casi al instante, de los clientes de Trend Micro de todo el mundo, con lo que se proporcionará protección antes de que los sistemas y dispositivos se encuentren en peligro. Olvídate de la protección de día cero. ¡Esto es protección de minuto cero!



La SPN guarda una base de datos de gran reputación con fuentes de correo electrónico, sitios web y uso compartido de archivos. Si un mensaje electrónico, un sitio web o un archivo proceden de una fuente maliciosa sospechosa o conocida, la SPN puede evitar el acceso al mismo, así como su descarga o apertura, y bloquear la fuente. Igualmente, la SPN busca activamente y registra todo tipo de vulnerabilidades y analiza la reputación de las aplicaciones móviles, ya que cada vez más malware es enviado mediante estas aplicaciones. Además, Trend Micro cuenta con más de 1200 investigadores que analizan activamente las amenazas, las rastrean y comprueban qué es lo que tratan de hacer. Dicha información es compartida con los usuarios finales a través de la SPN. Trend Micro también responde a las peticiones de asistencia de organizaciones que hayan descubierto o sospechen de la existencia de una nueva amenaza en su red. Tras analizar la amenaza, Trend Micro puede desarrollar un archivo de firma para detectarla y bloquearla, lo cual beneficia a la organización y a toda la base global de clientes de Trend Micro, a través de la SPN (ver diagrama 4-1).

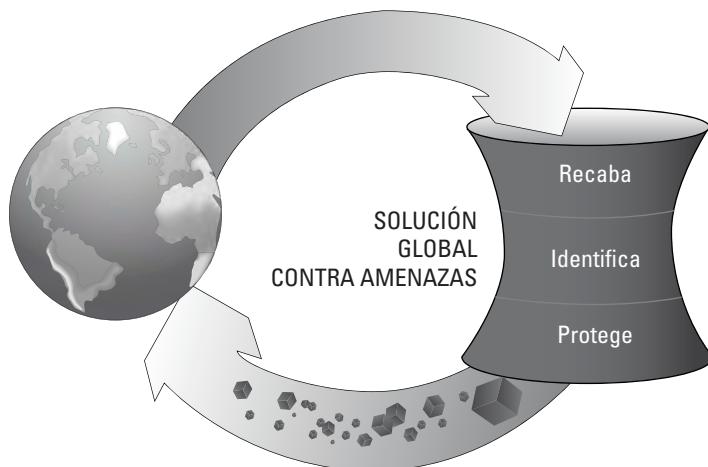


Diagrama 4-1: la SPN de Trend Micro proporciona soluciones globales contra amenazas de malware nuevas y ya existentes.

Diseño de la seguridad para entornos virtuales

Los productos de seguridad tradicionales diseñados sólo para los entornos físicos tienen una eficacia limitada en entornos virtuales, en la nube y en los *híbridos* (una mezcla de entorno físico, virtual y/o en la nube). Dichos productos de seguridad normalmente no pueden manejar un gran volumen de amenazas o, en el caso de las herramientas de seguridad que han de implementarse en un segmento

de red física, puede que simplemente se desvíen. Además, debido a problemas de conflicto de recursos (explicados en el Capítulo 2), los productos de seguridad tradicionales no compatibles con el entorno virtual pueden originar lo que básicamente constituye un ataque auto dirigido por denegación de servicio al superar la capacidad de una aplicación virtual, o basada en la nube, para responder a las peticiones de un usuario u otro sistema. El recurso de cargar los sistemas individuales (ya sean puestos de trabajo o servidores, físicos o virtuales) con grandes archivos de firma es simple y llanamente ineficaz contra las amenazas actuales que se hayan en rápida y constante evolución.



Para proteger por completo tu entorno informático, una solución de seguridad debe proteger tanto tus sistemas como tus datos.

Trend Micro Deep Security es una solución de seguridad compatible con el entorno virtual (ver diagrama 4-2), sin agente o basada en agente, que protege los sistemas y los datos. Deep Security tiene un diseño modular con una serie de componentes clave que proporcionan recursos de protección para entornos virtuales y en la nube, así como para entornos físicos tradicionales y mixtos. El diseño modular de Deep Security ofrece al cliente la posibilidad de añadir componentes individuales, según sea necesario, para cumplir con los requisitos corporativos y normativos. Entre dichos componentes se incluyen los siguientes:

- ✓ **Antimalware:** protección, sin agente o basada en agente, contra malware que emplea la SPN de Trend Micro (como se explica en la sección “Una mirada a la red de protección inteligente”) para proporcionar protección en tiempo real frente a amenazas de malware conocidas y de día cero sin que haya que descargar grandes archivos de firma o realizar análisis intensivos del sistema.
- ✓ **Cortafuegos para aplicaciones:** este módulo ayuda a reducir la superficie de ataque de una aplicación virtual, supervisa la VM en busca de ataques por denegación de servicio (DoS) y realiza análisis de reconocimiento. El cortafuegos para aplicaciones puede también proteger una VM recién creada (o una VM inactiva que está poniéndose en funcionamiento).
- ✓ **Supervisión de integridad:** el seguimiento de integridad de archivos ofrece la posibilidad de gestionar el acceso a directorios y archivos determinados y detectar cambios maliciosos o no autorizados en los directorios, archivos o incluso las claves del registro. El seguimiento de integridad puede ser implementado en una única aplicación virtual, quizás para proteger datos específicos, tales como información financiera confidencial, de titulares de tarjetas de pago o información sanitaria privada.

- ✓ **Sistemas de detección y prevención de intrusiones (IDS/IPS):** los IDS/IPS pueden detectar y bloquear los ataques conocidos y de día cero que se dirijan contra las vulnerabilidades del sistema y el software. Deep Security se vale de la SPN de Trend Micro para obtener actualizaciones dinámicas e instantáneas sobre la reputación de determinadas direcciones URL, como por ejemplo un enlace en un mensaje electrónico o documento.
- ✓ **Registro:** este componente (solamente disponible como agente instalado en VM individuales) ofrece recursos exclusivos para recoger, alertar y registrar el tráfico específico de seguridad y optimizar la identificación de problemas de seguridad importantes que a menudo quedarían soterrados en un sistema de registro tradicional.
- ✓ **Cifrado:** el cifrado puede proporcionar protección total a los datos, sea cual sea su ubicación. También ofrece un servidor de directivas para establecer reglas de acceso a información específica y alertar sobre actividad no autorizada. Estas funciones se ubican en un sistema bajo tu control que también alberga las claves para cifrar o descifrar datos, con completos recursos de auditoría para ayudar a tu organización a cumplir con una variedad de reglas. Estas funciones te permiten utilizar la informática en la nube de forma segura, ya que tienes control total del estado de tus datos y del acceso a los mismos.

Cada uno de estos componentes de Deep Security puede ejecutarse en las VM individuales, a modo de agente, en una variedad de infraestructuras virtuales entre las que se incluyen VMware, Microsoft y Citrix, por nombrar algunas.

En un entorno de VMware, Deep Security puede ejecutarse como una solución basada en agente instalado en VM individuales o a modo de aparato virtual sin agente que se ejecuta directamente en las máquinas anfitrionas físicas del entorno virtual. Trend Micro Y VMware colaboraron en el desarrollo de un conjunto de APIs en el ecosistema de VMware. Usando los enlaces de esas APIs, el aparato virtual de Deep Security puede ver todo el tráfico que circula en el hipervisor y entre las máquinas virtuales de la máquina anfitriona física, lo que por norma general te permite lograr una densidad de VM por máquina anfitriona física mayor que la que puede lograrse con una solución basada en agente.

Los agentes de Trend Micro Deep Security son compatibles con el entorno virtual, por lo que no colapsan los recursos informáticos de dichos entornos y no impiden a las aplicaciones acceder a esos recursos.



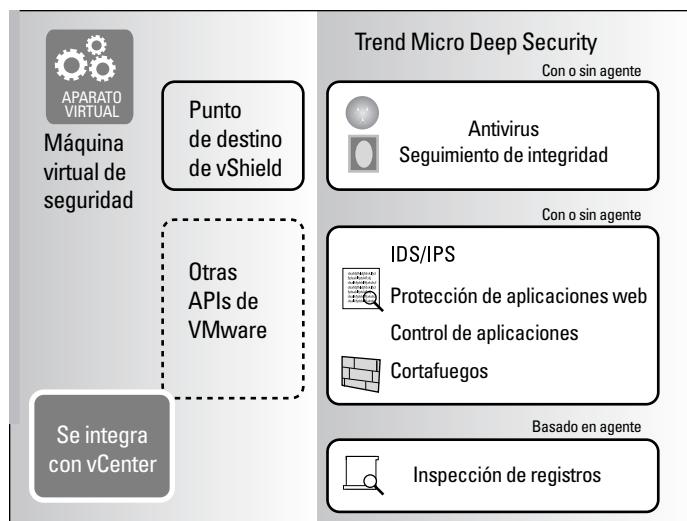


Diagrama 4-2: soluciones compatibles con el entorno virtual, sin agente y basadas en agente, de Trend Micro Deep Security.

En un entorno virtual, el hipervisor es la red de una máquina anfitriona física: cada una de las VM de la máquina anfitriona y sus aplicaciones se comunican con el hipervisor y a través del mismo. La comunicación entre máquinas virtuales permite a las VM comunicarse con otras VM (tráfico de este a oeste), así como con el mundo exterior (tráfico de norte a sur). La inspección exhaustiva de paquetes te permite buscar comportamientos anómalos que pueden ser indicativos de una nueva amenaza o ataque. Por ejemplo, un ataque DoS (por denegación de servicio) dirigido contra aplicaciones específicas –quizá una aplicación orientada al exterior– puede paralizar todas las demás VM y aplicaciones de la máquina anfitriona física.

Es fundamental poder supervisar e inspeccionar el tráfico entre máquinas virtuales para bloquear las amenazas que una VM afectada pueda dirigir contra otras VM de su mismo anfitrión físico. Para supervisar las amenazas de un entorno virtual, se debe supervisar el tráfico que llega a cada VM a través del hipervisor.



La única manera de supervisar eficazmente el tráfico entre máquinas virtuales y reaccionar ante las amenazas (ya sea individualmente con cada VM o tomando el anfitrión físico en su conjunto) es a través de un aparato de seguridad virtual, sin agente o basado en agente, que también esté alojado en la máquina anfitriona.

Protección de todos los aspectos del entorno informático

Es fundamental contar con soluciones de seguridad diseñadas específicamente para proteger tus entornos virtuales y en la nube, pero también hay que proteger los entornos físicos, como servidores, puestos de trabajo (ordenadores de sobremesa y portátiles, tabletas y teléfonos inteligentes) y ciertas aplicaciones. Hoy en día, todas las actividades de un ecosistema informático se extienden a plataformas de todo tipo, viajan por sendas desconocidas y necesitan una seguridad que sea adecuada para todos esos dispositivos, aplicaciones y actividades. En el entorno informático moderno actual hay que protegerlo todo (aplicaciones, sistemas o información), aunque no necesariamente al mismo nivel.

Un plan de clasificación de datos ayuda a las organizaciones a asignar valores a sus activos de información según lo sensibles que sean a la pérdida o a la divulgación de datos. Un plan de ese tipo puede también determinar el nivel de protección adecuado. Los planes de clasificación de datos pueden ser obligatorios para cumplir con normativas u otro tipo de requisitos. No es práctico ni deseable aplicar una única protección estándar a toda la información de tu organización.

La solución Trend Micro Deep Security protege los entornos de los centros de datos físicos y virtuales, así como los modelos de nube públicos y privados y los entornos mixtos físicos/virtuales/en la nube (ver diagrama 4-3). Trend Micro también ofrece Deep Security como un servicio que proporciona la opción de un modelo de seguridad “según demanda” para aquellas organizaciones que usan la nube pública para todos o algunos de sus sistemas y aplicaciones.



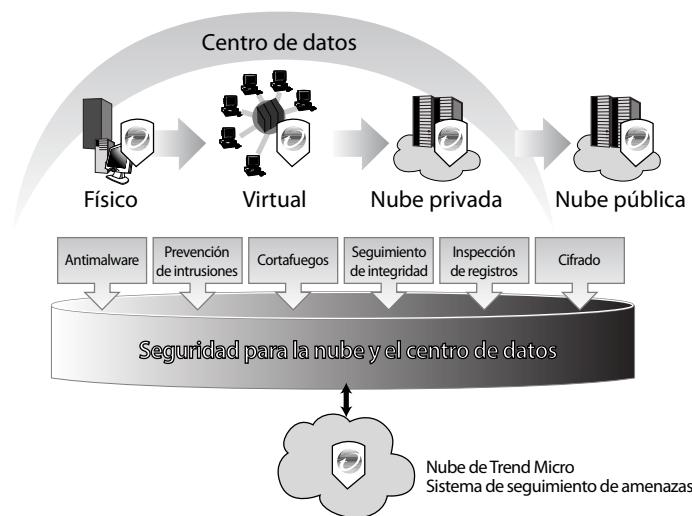


Diagrama 4-3: Trend Micro Deep Security protege los entornos físicos, virtuales, privados y públicos, así como aquellos híbridos.

Ahorro y seguridad reales con soluciones compatibles con el entorno virtual

Cuando utilizas soluciones de seguridad que han sido especialmente diseñadas para un entorno determinado, como el virtual, los beneficios (calculados en términos de aprovechamiento y eficiencia operativa) pueden superar con creces el coste de dicha solución. Los siguientes son algunos ejemplos de ese ahorro:

- ✓ **Licencias:** una solución de seguridad compatible con el entorno virtual emplea funciones de la infraestructura virtual, tales como la gestión de recursos, que te permiten incrementar la densidad de las máquinas virtuales (VM) en cada

máquina anfitriona y reducir potencialmente los costes de las licencias (por ejemplo, las de los preprocesadores de Windows Server Datacenter Edition y VMware).

- ✓ **Hardware, espacio físico, energía:** poner en marcha más VM en cada máquina anfitriona puede reducir la necesidad de más hardware para servidores y la huella ecológica de tu centro de datos. Si se gestiona adecuadamente, una infraestructura virtual puede reducir también el gasto de recursos energéticos como la electricidad y la ventilación.

(continuación)

(continuación)

- ✓ **Gestión:** a menos servidores físicos, menos trabajo de gestión. Incluso en situaciones que requieren usar una sola VM en una máquina anfitriona, al poder gestionar tus VM y tus servidores físicos con las mismas herramientas de seguridad compatibles con el entorno virtual, se simplifica enormemente la gestión de tu centro de datos. También se reduce el peligro de nuevas amenazas o vulnerabilidades debido a errores de configuración derivados de la complejidad.
- ✓ **Nube:** Ya que cada vez más organizaciones trasladan sus sistemas y aplicaciones empresariales importantes a la nube, se deben hacer frente los retos de la seguridad en la nube. No es posible hacer funcionar aparatos de seguridad físicos en la nube, por lo que muchas organizaciones deben confiar en su proveedor de servicios de nube para cubrir sus necesidades de seguridad. Este hecho por sí solo conduce a muchas organizaciones a retrasar el traslado a la nube o a renunciar por completo a cualquier iniciativa en la misma.

Sin embargo, las soluciones de seguridad diseñadas para el entorno virtual que, por su naturaleza, son en sí mismas virtuales, pueden ser usadas en la nube. En otras palabras, los sistemas y aplicaciones de la nube pueden ser gestionados con las mismas soluciones de seguridad empleadas a para gestionar los sistemas y aplicaciones virtuales del centro de datos.

Cuando las organizaciones utilizan soluciones de seguridad compatibles con el entorno virtual, normalmente las densidades de consolidación de las VM o los escritorios de VDI pueden ser hasta tres veces mayores que las que se logran con herramientas de seguridad tradicionales.

Obviamente, esto puede calcularse de manera sencilla con un análisis de ahorro de costes. Al ser más eficaces que las herramientas de seguridad tradicionales y estar diseñadas para protegerse automáticamente, las soluciones de seguridad para el entorno virtual eliminan las vulnerabilidades exclusivas de los entornos virtuales a las que los productos tradicionales de seguridad no pueden hacer frente.

Capítulo 5

Diez funciones importantes que hay que buscar en una solución de seguridad consciente del entorno virtual

En este capítulo

- Evaluación de las soluciones de seguridad para el entorno virtual

Proteger los entornos virtuales y en la nube no es tan simple como dar un retoque a los ajustes de análisis y actualización de los programas antivirus/antimalware tradicionales. Si actúas así, no estás teniendo en cuenta el hecho de que los entornos virtuales son muy diferentes a los físicos. Para tratar esas diferencias de modo eficaz has de utilizar soluciones de seguridad diseñadas para funcionar en entornos virtuales; no debes tratar de reasignar los programas de seguridad que ya tienes, pues no resultan eficaces en el mundo virtual.

Aquí tienes una lista de las principales funciones que hay que buscar en una solución de seguridad para el entorno virtual:

- ✓ **Funciona en entornos mixtos.** Opera en entornos físicos, virtuales y en la nube, usando instalaciones sin agente y basadas en agente.
- ✓ **Gestiona servidores y escritorios mediante una interfaz única.** Gestiona los servidores y los escritorios, ya sean físicos o virtuales, por medio de una única consola de control.
- ✓ **Ajusta automáticamente el uso de recursos.** Se ajusta automáticamente al entorno en el cual es implementada

(especialmente si es virtual) para que los niveles de rendimiento no se vean afectados por la solución de seguridad.

- ✓ **Migra con sistemas virtuales.** Las protecciones de seguridad migran de forma dinámica junto a las VM entre máquinas anfitrionas físicas o en la nube.
- ✓ **Ofrece las funciones complementarias necesarias.** Utiliza sólo las funciones requeridas por tu entorno y agrega otras nuevas a medida que tus requisitos de seguridad evolucionan, sin tener que volver a implementar o configurar la solución de seguridad completa.
- ✓ **Protege las VM inactivas.** Las VM inactivas pueden ser iniciadas con rapidez en un entorno virtual. Si no es analizada y protegida adecuadamente antes de ser puesta en línea, una VM inactiva puede exponer a todo tu entorno virtual ante amenazas de seguridad.
- ✓ **Registra la información de seguridad relevante.** Un sistema de registro específico para operaciones de seguridad (ya sea en un entorno físico, virtual o en la nube) ofrece la posibilidad de recabar información relevante sobre actividades que puedan estar asociadas a una amenaza, gracias a lo cual el análisis puede centrarse en una menor cantidad de contenidos.
- ✓ **Filtre los sistemas a los que no se han aplicado parches.** Protege mediante un filtro aquellos sistemas a los que no se han aplicado parches contra vulnerabilidades conocidas. Filtra también sistemas más antiguos que puede que ya no reciban asistencia por parte del fabricante o sistemas y aplicaciones personalizados, valiéndose de filtros que puedes crear para protegerlos frente a vulnerabilidades conocidas.
- ✓ **Aplica reglas y perfiles de gestión de la configuración mínima de seguridad.** Extiende automáticamente las reglas y los perfiles de gestión de la configuración de seguridad a nuevos anfitriones y sus VM, sin tener que volver a configurar los sistemas a cada inicio. Con el establecimiento de una configuración de seguridad de referencia, los sistemas que requieran medidas de seguridad adicionales pueden ser tratados más eficazmente, en función de las necesidades..
- ✓ **Cumple con los requisitos normativos.** Proporciona módulos de seguridad complementarios diseñados para cumplir con requisitos normativos específicos, tales como el PCI, en un entorno virtual

Apéndice

adware: software malicioso que publicita programas, a menudo por medio de pancartas y ventanas emergentes.

agente de seguridad (SA): componente de software que se instala en un servidor u ordenador de sobremesa y desempeña una función de seguridad específica, como la protección contra malware o la detección de intrusos.

amenazas: eventos y condiciones que en caso de darse suponen un peligro para sistemas y datos.

APT (amenaza persistente avanzada): ataque prolongado que se lanza desde Internet normalmente por parte de un grupo con importantes recursos, como delincuentes organizados o naciones-estado corruptos.

autenticación: el proceso de verificación de la identidad de un usuario, ordenador o servicio.

bomba lógica: software que realiza una acción maliciosa al cumplirse una condición predeterminada, como una fecha o una cálculo específico.

bootkit: software malicioso, variante del rootkit, que se usa a menudo para atacar un disco duro cifrado.

bot: máquina a la que se le ataca e infecta con malware y forma parte de un botnet (se conoce también como zombi).

botnet: red amplia de bots que funcionan conjuntamente.

Bring Your Own Device (BYOD): la tendencia “trae tu propio dispositivo” permite a los empleados usar sus teléfonos inteligentes, tabletas y otros dispositivos informáticos en el centro de trabajo para su uso tanto personal como laboral.

consumerización: tendencia actual según la cual los usuarios pueden encontrar cada vez más productos tecnológicos y aplicaciones personales que resultan más potentes o capaces, más prácticos, menos caros, más rápidos de instalar y más fáciles de usar que las soluciones informáticas corporativas. Ver también *BYOD*.

defensa a fondo: estrategia para proteger la información mediante múltiples capas de defensa.

entorno de sistema operativo (OSE): sistema operativo de servidor o de escritorio que constituye un sistema informático completo y se ejecuta en un entorno virtual o físico.

gusano: software malicioso que se reproduce con rapidez de un ordenador a otro a través de redes, sin que el usuario final necesite que realizar acción alguna.

hipervisor: componente principal de una capa de la plataforma de una infraestructura virtual que permite comunicarse a dos máquinas virtuales y gestiona el uso de recursos entre las máquinas virtuales y la máquina anfitriona física.

infraestructura de escritorio virtual (VDI): sistema operativo de escritorio situado en una máquina virtual que proporciona un escritorio virtual a los usuarios finales desde un servidor físico centralizado.

integridad de datos: exactitud y coherencia de la información durante su creación, transmisión y almacenamiento.

malware: software o código malicioso que generalmente daña o inutiliza un sistema informático, se hace con el control del mismo o le roba información. Ver también: adware, puerta trasera, bootkit, bomba lógica, rootkit, spyware, troyano, virus y gusano.

máquina virtual (VM): simulación mediante software de un ordenador físico (por ejemplo, un servidor o un ordenador de sobremesa) que incluye un sistema operativo y aplicaciones. Se conoce también como máquina invitada.

phishing: utilización de técnicas de ingeniería social a través del correo electrónico para hacer que los usuarios faciliten información personal.

puerta trasera: software malicioso que permite a un atacante saltarse los mecanismos de autenticación para acceder sin autorización a un sistema o una aplicación.

rootkit: software malicioso que facilita el acceso privilegiado a un ordenador (por ejemplo, mediante el uso de permisos de administrador o de nivel de raíz).

seguridad compatible con el entorno virtual: software de seguridad con capacidad de detectar si está ejecutándose en un entorno virtual y adaptar su funcionamiento de tal modo que el resto de aplicaciones de una máquina virtual cuente con los recursos suficientes para rendir como se espera.

sistema de detección de intrusiones (IDS): aparato de hardware o agente de software que detecta y notifica las presuntas intrusiones en redes o anfitriones.

sistema de prevención de intrusiones (IPS): aparato de hardware o agente de software que detecta y bloquea las presuntas intrusiones en redes o anfitriones.

spyware: también conocido en español como programa espía, es un software malicioso que recopila información sobre el uso de Internet o los datos privados de un usuario.

troyano: Se trata de un malware que se hace pasar por un programa de confianza, pero que en realidad desempeña otras funciones.

virus: software malicioso que se incrusta en otro programa (por ejemplo, al archivo adjunto de un mensaje electrónico) y requiere de una acción por parte de un usuario final (como abrir un archivo adjunto) para reproducirse.

vulnerabilidad: ausencia o debilidad de protección de un sistema o aplicación que hace que una amenaza sea potencialmente más dañina o costosa, que haya más posibilidades de que ocurra o que ocurra con mayor frecuencia.

Seguridad que optimiza el rendimiento

- Virtualización de vía rápida
- Autenticación del cumplimiento normativo
- Del puesto de trabajo a la nube

Más información en:
TrendMicro.com/VirtualDummies

¡Aprende a mantener protegido tu entorno virtual!

Los productos de seguridad tradicionales creados para proteger sistemas físicos no funcionan con los sistemas virtuales. En este libro se examinan los retos de seguridad de la virtualización en el centro de datos, en el puesto de trabajo y en la nube. Se muestra cómo las soluciones de seguridad compatibles con el entorno virtual proporcionan seguridad total sin afectar al rendimiento.

- **Virtualización 101 – averigua cómo funciona la tecnología de virtualización y los retos de seguridad asociados con todo entorno virtualizado**
- **Protege tu centro de datos privado o público – descubre los retos de seguridad específicos a los que debes enfrentarte en la virtualización del centro de datos y de la nube**
- **Usa la infraestructura de escritorio virtual (VDI) – entérate de los retos de seguridad de la virtualización de escritorio y de cómo la VDI puede ayudarte a proteger tus datos**
- **Explora la seguridad de Trend Micro – entiende mejor el modo en que las soluciones de Trend Micro abordan la virtualización de tu actividad informática privada y pública (en la nube)**

Daniel Reis ha trabajado en el ámbito de la seguridad durante más de 12 años y lleva 20 dedicándose a las altas tecnologías. Éste es su primer libro en la colección *Para Dummies*.



Abre este libro
y encontrarás:

- Una explicación sencilla de lo que es la virtualización
- Un glosario útil de términos
- El modo de dar con el modelo de seguridad adecuado que se ajuste a tus necesidades
- Una explicación sobre las ventajas de la virtualización
- La razón por la que la seguridad de la virtualización constituye un reto

Visita **Dummies.com®**
para ver vídeos, ejemplos paso a paso, artículos how-to o para realizar compras

WILEY

ISBN: 978-1-118-85095-4
No destinado para la venta