A background image showing a laptop on a desk with a semi-transparent circular gauge overlay. The gauge has numerical markings from 0 to 70 and a white needle pointing towards the 40 mark. The scene is dimly lit, suggesting an office environment.

## Cara a cara frente a los retos de la seguridad de la virtualización

Coordinación de la seguridad 



Defensa de servidor  
para equipos  
virtuales

*Artículo técnico  
de Trend Micro | Agosto de 2009*

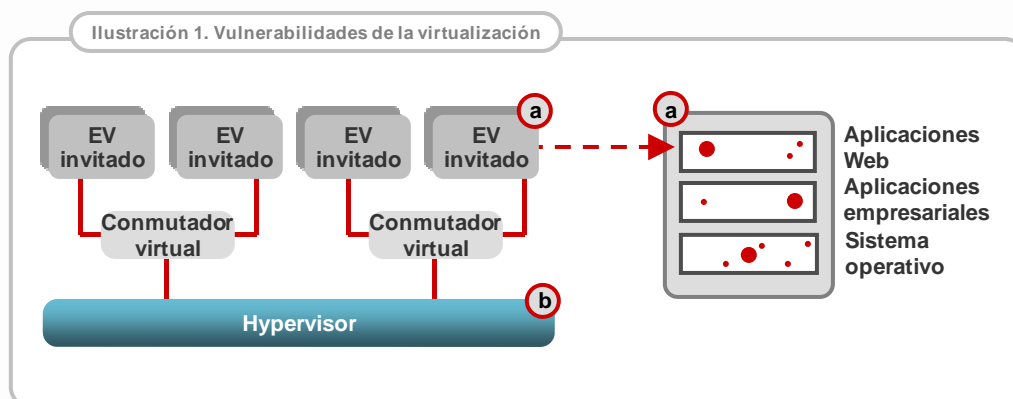
## I. INTRODUCCIÓN

Gracias a la virtualización, las organizaciones pueden lograr grandes resultados en cuanto a eficacia y rentabilidad, así como las ventajas propias de un centro de datos consolidado “más verde”, una mayor escalabilidad y optimización de la gestión de los recursos. Sin embargo, por desgracia las ventajas de la virtualización se ven descompensadas con una mayor exposición a riesgos, dado que los sistemas virtuales del centro de datos deben hacer frente a los mismos retos de seguridad que los servidores físicos, así como a otros riesgos exclusivos a la hora de proteger estos recursos informáticos. Su organización debe estudiar qué mecanismos de seguridad son los más adecuados para proteger los servidores físicos y virtuales, sin olvidar en especial que una arquitectura virtualizada afecta principalmente al modo en que las aplicaciones vitales se diseñan, implementan y gestionan.

Trend Micro ofrece soluciones reales para estos retos. Utilizando las novedosas tecnologías obtenidas por Trend Micro con la adquisición de Third Brigade, y junto con nuestra vasta experiencia en seguridad, hemos desarrollado un enfoque coordinado válido tanto para la defensa del servidor (que incluye detección y prevención de intrusiones, cortafuegos, supervisión de integridad e inspección de registros) como para la protección frente al malware que ya se puede implementar. Su arquitectura está pensada para aprovechar las posibilidades adicionales que los proveedores de virtualización incorporan a sus plataformas, como las incluidas en la VMware vSphere™ 4 lanzada recientemente, que permite el acceso a las API de VMware VMsafe™. Ofrecemos el nivel de protección necesario para mejorar la seguridad de las aplicaciones vitales en entornos virtualizados. Este artículo se centra en el enfoque coordinado de Trend Micro para la defensa del servidor en equipos virtuales.

## II. RETOS DE LA SEGURIDAD DE VIRTUALIZACIÓN

Un sistema virtualizado usa el mismo sistema operativo (y las mismas aplicaciones Web y empresariales) que un sistema físico. La principal amenaza que se cierne sobre estos sistemas virtualizados es la posibilidad de que un malware explote remotamente las vulnerabilidades de estos sistemas y aplicaciones [ver ilustración 1a], aunque también existen vulnerabilidades que se pueden explotar en el hipervisor del sistema [ver ilustración 1b].



Los proveedores de virtualización siguen trabajando para simplificar la consola de servicio, tal y como ocurre con VMware ESXi, y poder reducir así la posible superficie de ataque. Prácticamente ninguna de las vulnerabilidades del hipervisor se podrá explotar remotamente (en tanto el hipervisor carece de servicios que finalicen protocolos remotos), de modo que se suelen explotar mediante un malware que pone en peligro un equipo virtual. Por lo tanto, uno de los mejores métodos que existen para proporcionar protección frente a los ataques a las vulnerabilidades del hipervisor consiste, en primer lugar, en impedir que el malware se instale en el entorno virtual.

La naturaleza dinámica de los entornos virtualizados plantea nuevos retos a los sistemas de detección y prevención de intrusiones (IDS/IPS). Dado que los equipos virtuales se pueden revertir rápidamente a instancias anteriores, así como moverse con total facilidad entre servidores físicos, es difícil lograr y mantener una seguridad uniforme.

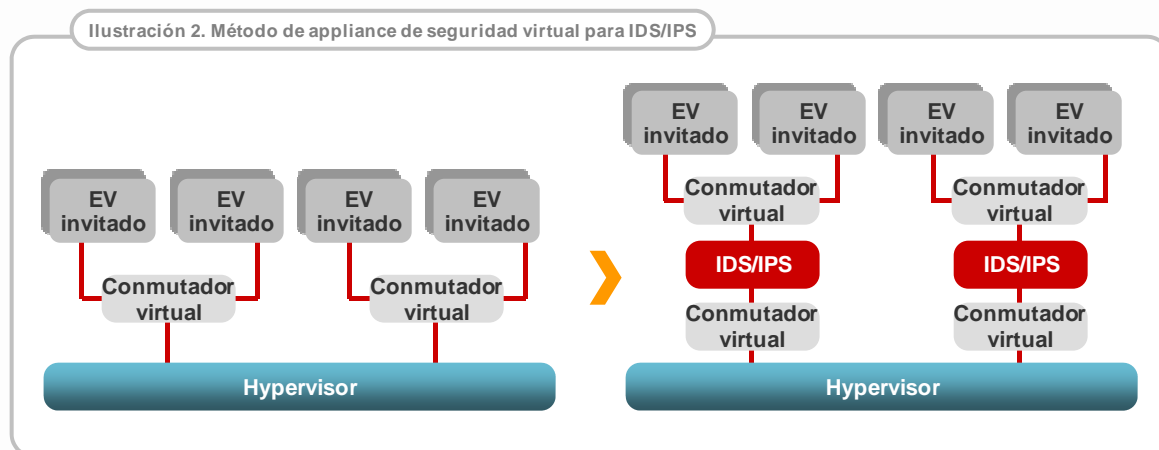
Para crear un enfoque eficaz de la seguridad de virtualización, deberá atenerse a los mismos principios de seguridad que se desarrollaron para proteger los recursos de TI físicos. Uno de ellos es la “defensa exhaustiva”, que constituye un requisito de seguridad fundamental para las organizaciones que han identificado una “desperimetrización” de su infraestructura de TI. Este principio viene respaldado por las mejores prácticas del sector y, en este sentido, organizaciones como Jericho Forum lo incluyen como parte de sus recomendaciones de seguridad. La virtualización ha hecho más patente aún el reto de la “desperimetrización”, así como la necesidad de disponer de una seguridad de vanguardia todavía mayor, habida cuenta de la incapacidad de la seguridad basada en appliances para hacer frente a los ataques entre equipos virtuales en el mismo sistema físico. Por lo tanto, aplicar mejores prácticas de seguridad es algo vital. Entre los otros principios de Forum que se deben seguir encontramos las siguientes reglas:

- El ámbito y el nivel de protección deben ser específicos y adecuados para el activo en peligro.
- El negocio exige que la seguridad permita la agilidad empresarial y que sea rentable.
- Mientras que los cortafuegos fronterizos pueden seguir proporcionando la protección de red básica, los sistemas y datos individuales deberán poder ser capaces de protegerse a sí mismos.
- En general, cuanto más cerca esté la protección de un activo, más fácil será protegerlo.

Si se aplican estos y otros principios al centro de datos virtualizado, veremos que existe una necesidad ineludible de implementar mecanismos directamente en el servidor físico para proteger estos sistemas virtualizados, enfoque de la seguridad de virtualización que permite que la protección tenga lugar lo más cerca posible del activo pertinente.

## III. ENFOQUES ACTUALES SOBRE LA SEGURIDAD DE VIRTUALIZACIÓN

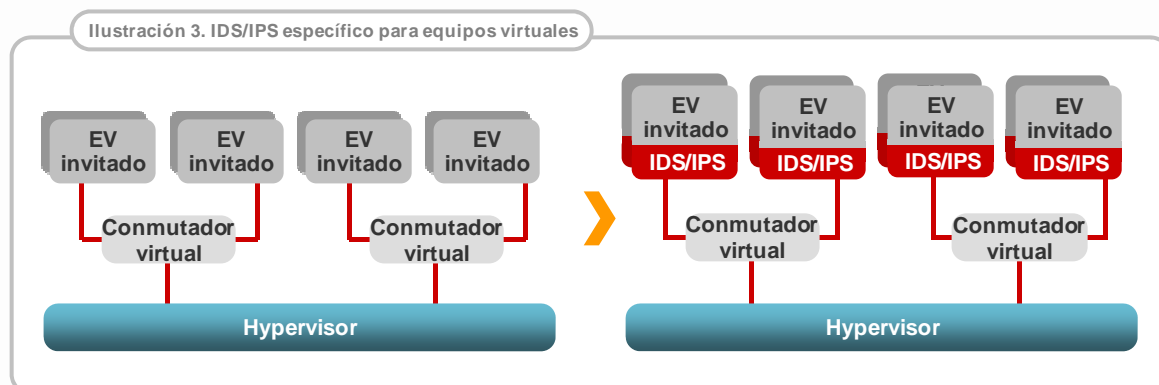
Antes de la disponibilidad generalizada de soluciones de seguridad creadas a propósito para las API de VMware VMsafe, se solían utilizar dos enfoques iniciales con el software de seguridad para proteger los equipos virtuales. Uno de ellos consiste en usar un appliance de seguridad virtual en el entorno informático virtualizado a fin de supervisar el tráfico entre un conmutador virtual (vSwitch) y uno o varios equipos virtuales invitados [ver ilustración 2].



Si bien es cierto que una solución de appliance de seguridad virtual reporta protección de IDS/IPS frente a los ataques que surgen en la red, existen limitaciones muy significativas a este respecto:

- **Tráfico entre equipos virtuales:** los appliances de seguridad virtuales deben situarse frente a un conmutador virtual, de modo que no pueden impedir que se produzcan ataques entre equipos virtuales en el mismo conmutador virtual.
- **Movilidad:** si se usan controles del tipo VMware VMotion™ para trasladar un equipo virtual de un servidor físico a otro, se perderá el contexto de seguridad. Habría que configurar el reagrupamiento de los appliances de seguridad virtuales en cada posible destino en el que un equipo virtual pudiera reubicarse, lo cual repercute desfavorablemente en el rendimiento.
- **No transparencia:** las modificaciones que se deben realizar en la arquitectura de red virtual para implementar los appliances de seguridad virtuales tendrán un impacto negativo en el sistema existente.
- **Cuellos de botella del rendimiento:** el appliance de seguridad virtual debe procesar todo el tráfico entre los equipos virtuales y la red, algo que puede acabar en un cuello de botella del rendimiento.

Con el otro enfoque, se puede implementar la misma funcionalidad de IDS/IPS en cada uno de los equipos virtuales [ver ilustración 3].

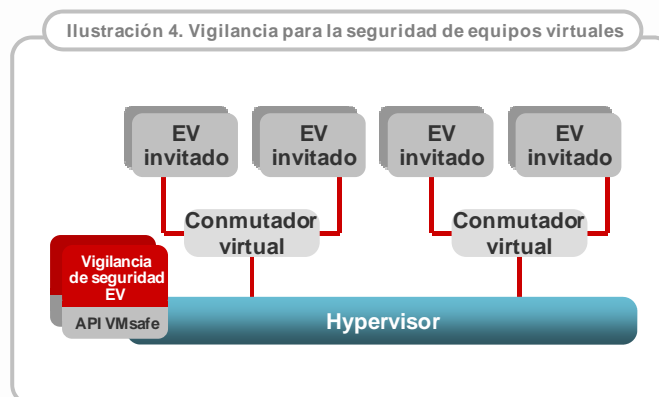


Al contrario de lo que sucede con el método de appliance de seguridad virtual, el enfoque de equipo virtual pone fin a las limitaciones del tráfico entre equipos virtuales y a la escasa visibilidad. Bien es cierto que este enfoque también incide en el rendimiento del sistema, pero se reparte entre los equipos virtuales de la infraestructura de TI. Con todo, una arquitectura de equipos virtuales sigue teniendo que enfrentarse al reto que supone la implementación de un agente de seguridad de IDS/IPS en cada equipo virtual. Esto se minimiza mediante el uso de mecanismos como plantillas (tal y como indica VMware en su tutorial en línea sobre el trabajo con plantillas), con las que se implementa un agente de seguridad común en todos los equipos virtuales. No obstante, la naturaleza dinámica de los entornos virtualizados sigue provocando que se incorporen equipos virtuales en el entorno de producción sin que exista un agente de seguridad.

## IV. EQUIPO VIRTUAL GUARDIÁN DE SEGURIDAD

El programa VMware Vmsafe permite implementar equipos virtuales de seguridad dedicados con acceso privilegiado a las API del hipervisor. Gracias a esto, se puede crear un control de seguridad único, un equipo virtual guardián de la seguridad, tal y como se explica en el informe de Gartner sobre los conceptos de la transformación radical de la seguridad y la gestión en el mundo virtualizado (*Radically Transforming Security and*

*Management in a Virtualized World: Concepts*). Este equipo virtual guardián de la seguridad constituye una nueva forma de implementar controles de seguridad dentro de un entorno virtual [ver ilustración 4].



Las funciones del guardián de seguridad utilizan las API de introspección para tener acceso a la información de estado privilegiada acerca de cada equipo (incluidos la memoria, estado y tráfico de red), de modo que se pone fin a las limitaciones de no transparencia y tráfico entre equipos virtuales del enfoque de appliance de seguridad virtual para el filtrado de IDS/IPS, ya que todo el tráfico de red del servidor estará visible sin necesidad de alterar la configuración de red virtual. Sin embargo, el impacto en la movilidad y el rendimiento siguen siendo aspectos que se deben tener en cuenta al realizar filtrados de IDS/IPS en los equipos virtuales guardianes de seguridad.

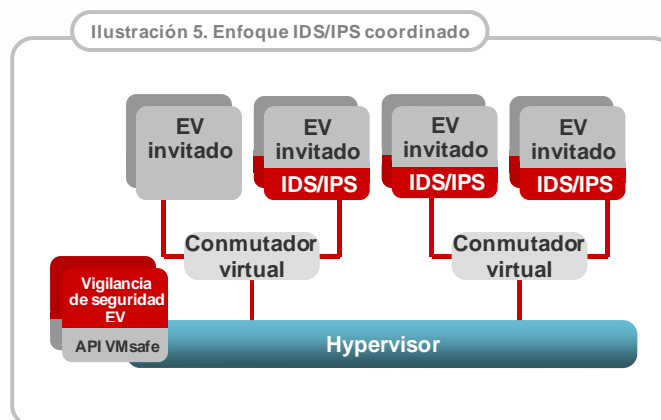
Se puede aplicar una inmensa variedad de funciones de seguridad (como antivirus, cifrado, cortafuegos, IDS/IPS e integridad del sistema) a los equipos virtuales guardianes de seguridad. La finalidad de los appliances de seguridad virtuales se está replanteando para que usen estas API, al tiempo que las tecnologías de agente de equipo virtual también se están rediseñando para que puedan ejecutarse en los equipos virtuales guardianes de seguridad. A pesar de todo esto, es necesario seguir disponiendo de cierta flexibilidad para implementar algunas funciones en un equipo virtual guardián de seguridad y en algunos equipos virtuales mediante agentes de equipo virtual debido a los siguientes aspectos:

- Algunas funciones de seguridad solo se pueden lograr mediante agentes de equipo virtual (por ejemplo, controlar el tráfico cifrado o tener acceso a determinada información de estado en tiempo real).
- Existen compensaciones de rendimiento entre implementar una solución a través del equipo virtual guardián de seguridad e implementar un agente de equipo virtual.
- Las API de introspección que se necesitan se desarrollan y publican por fases, de modo que deberá disponer de mecanismos de seguridad para usarlos durante los periodos transaccionales, hasta que la función del equipo virtual guardián de seguridad esté disponible.

En consecuencia, necesitamos un enfoque coordinado: uno que reporte tanto las ventajas del enfoque de los equipos virtuales como las que ofrecen las API de introspección. Así, podremos disfrutar de opciones inteligentes con las que se minimicen los cuellos de botella y los controles redundantes y, al mismo tiempo, se reduzcan los riesgos de seguridad de manera rentable. Trend Micro tiene una solución que cubre esta necesidad.

## V. UN ENFOQUE DE SEGURIDAD COORDINADO

Nuestro enfoque coordinado para proteger los entornos virtualizados consta de un agente de equipo virtual que se puede implementar en cada uno de los equipos virtuales y de un equipo virtual guardián de seguridad implementado para proteger varios equipos virtuales. Esta arquitectura garantiza que los activos de TI críticos (equipos virtuales) se pueden proteger mediante la implementación de software en los propios activos, mientras que los activos no críticos quedan protegidos mediante el equipo virtual guardián de seguridad [ver ilustración 5].



### ENFOQUE INTEGRADO

Son seis los aspectos de nuestro enfoque coordinado, que examinaremos aquí.

- Coordinación de la detección y prevención de intrusiones
- Integración de la gestión de virtualización
- Gestión empresarial
- Funcionalidad IDS/IPS global
- Varias arquitecturas de virtualización
- Modelos de licencia de software

### COORDINACIÓN DE LA DETECCIÓN Y PREVENCIÓN DE INTRUSIONES

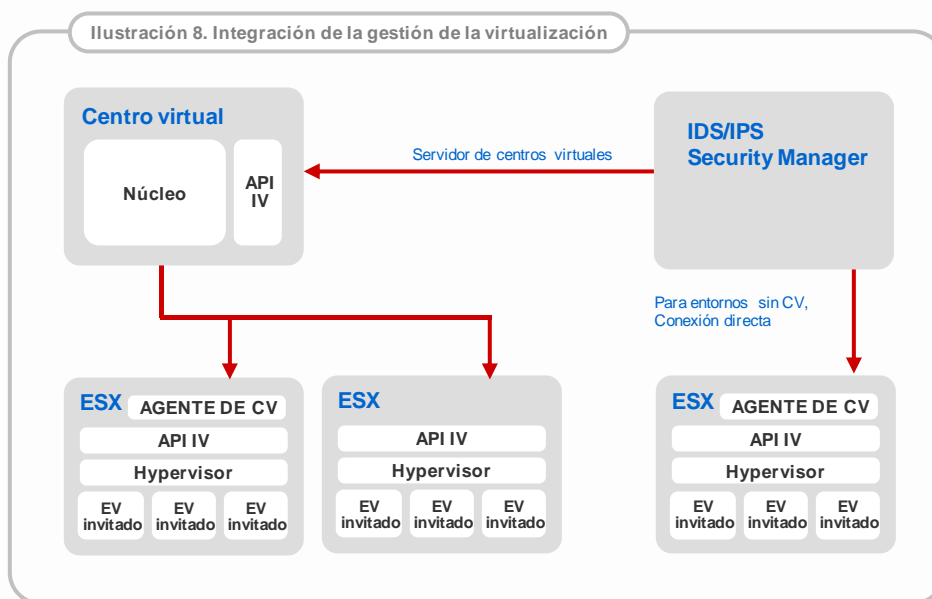
La secuencia de coordinación tiene lugar del siguiente modo:

- El equipo virtual guardián de seguridad recibe una notificación cada vez que un equipo virtual se activa.
- Si el equipo virtual guardián de seguridad detecta un agente de seguridad implementado en el equipo virtual invitado (o bien que debería haber uno implementado), se asegura de que la versión de software y la configuración de seguridad son las adecuadas y actualiza la configuración si procede.
- El resultado es un equipo virtual invitado con una protección al día y que se puede comunicar en la red enviando tráfico directamente del hipervisor al equipo virtual.



## INTEGRACIÓN DE LA GESTIÓN DE VIRTUALIZACIÓN

Las plataformas de virtualización suelen incluir un sistema de gestión centralizada para gestionar la implementación de hosts físicos y equipos virtuales, como VMware vCenter Server. La función de gestión de la seguridad del sistema de IDS/IPS se conecta con este sistema de gestión de virtualización para obtener la configuración de los hosts y los equipos virtuales [ver ilustración 8].



Así, la disposición de los sistemas se puede mostrar mediante una estructura similar dentro del gestor de seguridad de IDS/IPS para poder gestionar eficazmente el host físico y los equipos virtuales [ver ilustración 9].

## GESTIÓN EMPRESARIAL

Los sistemas de IDS/IPS de clase empresarial proporcionan una gestión de la seguridad centralizada que se integra en la propia gestión de virtualización. Esta función define y distribuye la política a los componentes de cumplimiento de IDS/IPS y recopila eventos de las acciones que el componente de cumplimiento lleva a cabo, como los ataques detectados o impedidos. Otros elementos indispensables de la gestión de la seguridad centralizada en un sistema de IDS/IPS distribuido incluyen los siguientes:

- Escalabilidad de la gestión: el mismo componente de gestión debe tener capacidades de virtualización en varios equipos virtuales a fin de permitir una implementación escalable y una disponibilidad elevada.

Ilustración 9. Hosts y equipos virtuales



- Puntos de integración (como syslog y servicios Web), para que IDS/IPS se pueda integrar en otros elementos de seguridad de la empresa, como los sistemas de gestión de información de seguridad y eventos (SIEM).
- Funciones de seguridad compatibles: esto incluye el control del acceso basado en roles y un historial de auditoría de las acciones realizadas por el administrador.
- Evaluaciones de otros fabricantes: estas evaluaciones, como los denominados *Common Criteria for Information Technology Security Evaluation*, ayudan a garantizar que se ha alcanzado un conjunto de parámetros de seguridad específico.

## **FUNCIONALIDAD IDS/IPS GLOBAL**

Si bien el análisis de la red es habitual tanto en los appliances de seguridad virtuales como en los agentes de equipo virtual, la guía NIST para sistemas de detección y prevención de intrusiones establece que la detección y prevención de intrusiones basadas en host incluyen los siguientes elementos:

- Análisis de código
- Análisis del tráfico de red (inspección profunda de paquetes e inspección de protocolo de aplicación)
- Filtrado del tráfico de red (cortafuegos)
- Supervisión del sistema de archivos
- Análisis de registros
- Supervisión de la configuración de la red

Cada una de estas áreas de funcionalidad precisa de coordinación entre los agentes de equipo virtual y los equipos virtuales guardianes de seguridad a fin de garantizar una seguridad uniforme.

## **VARIAS PLATAFORMAS DE VIRTUALIZACIÓN**

VMware es líder de virtualización del sector, pero existen otros muchos proveedores que desarrollan plataformas de virtualización (entre otras, Microsoft Windows Server Virtualization y Citrix XenServer). Si bien la profundidad de funcionalidad de un equipo virtual guardián de seguridad será distinta según la plataforma, el enfoque coordinado de Trend Micro para la seguridad de virtualización será aplicable a todas ellas.

## **MODELOS DE LICENCIA DE SOFTWARE**

La transición a entornos virtualizados ha captado una atención cada vez mayor hacia las licencias de software, dado que la virtualización ha tenido un impacto considerable en el software, del mismo modo que ha revolucionado el uso del hardware. Las organizaciones esperan que con las licencias aumente el uso de software, dado que ofrecen una serie de opciones idóneas sin que esto suponga un incremento en los costes de software. A medida que las organizaciones adoptan el enfoque coordinado a IDS/IPS, se requieren opciones de licencia flexibles y "a prueba de futuro" que se ajusten adecuadamente a entornos tanto físicos como virtuales. Esto incluye la posibilidad de usar una licencia por cada agente de IDS/IPS de un equipo virtual, así como de tener una licencia de la funcionalidad de IDS/IPS para un número ilimitado de equipos virtuales en un servidor físico. Los mecanismos de gestión de licencias deben garantizar que las organizaciones realizan un seguimiento del uso que se hace de ellas en un entorno virtualizado dinámico sin añadir complejidad alguna.

## VI. CONCLUSIÓN

Si bien una infraestructura de TI virtualizada comparte muchos de los desafíos a los que deben hacer frente los entornos de servidores físicos, se puede aprovechar la inversión en arquitecturas con varios núcleos y procesadores y software de virtualización para proporcionar los mecanismos necesarios para protegerlos. Además, los recursos de TI virtualizados pueden recibir protección para hoy y para mañana con las mejoras de seguridad creadas como funciones de introspección, tales como las API de VMsafe, que continúan evolucionando en las plataformas de virtualización. La adopción del enfoque coordinado con software de seguridad que Trend Micro proporciona permite una protección optimizada y una implementación de soluciones instantánea, al tiempo que garantiza una línea base de seguridad para todos los equipos virtuales sin generar cuellos de botella o controles redundantes. Trend Micro permite ampliar la implementación de virtualización para que abarque a todos los sistemas críticos.

## VII. POR QUÉ TREND MICRO

Desde su nacimiento, hace ya 20 años, Trend Micro ha centrado todos sus esfuerzos en la seguridad del contenido. Con más de mil millones de dólares estadounidenses en ingresos anuales, más de 1.000 investigadores de amenazas y más de 4.000 empleados en todo el mundo, Trend Micro dispone del tamaño, la velocidad y la infraestructura de tecnología única para Internet necesarios para tratar la seguridad de contenido empresarial de hoy día. Ningún otro proveedor de seguridad puede igualar el potencial que Trend Micro ofrece a las empresas. Este es el motivo por el que miles de empresas de todo el mundo continúan confiando en Trend Micro.

A medida que aumenta la velocidad de las amenazas, también lo hacen los riesgos y costes. Las empresas quieren una seguridad escalable, que se pueda gestionar y que sea capaz de adelantarse a las nuevas amenazas con total fiabilidad. Solamente Trend Micro ofrece la combinación exclusiva de una protección inmediata con una menor dificultad. Con la innovadora tecnología Smart Protection Network, Trend Micro Enterprise Security ofrece una protección inmediata que mejora de forma automática y que cierra la ventana hacia las vulnerabilidades antes de que sea demasiado tarde. Además, Trend Micro reduce increíblemente el tiempo necesario para adquirir, implementar y gestionar la seguridad. Gracias a Trend Micro Enterprise Security, las empresas reducirán el tiempo invertido en protección, lo cual supondrá a su vez una disminución de los riesgos y costes.

Para obtener más información, puede llamarnos o visitarnos en:

<http://es.trendmicro.com/es/solutions/enterprise/security-solutions/virtualization/>

## VIII. REFERENCIAS

- Gartner, Radically Transforming Security and Management in a Virtualized World: Concepts, Neil MacDonald, 14 de marzo de 2008
- Common Criteria for Information Technology Security Evaluation, [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)
- Jericho Forum, [www.jerichoforum.org/](http://www.jerichoforum.org/)
- NIST Guide to Intrusion Detection and Prevention Systems, <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>
- VMware, [www.vmware.com/overview/security/vmsafe.html](http://www.vmware.com/overview/security/vmsafe.html)
- Tutorial de VMware: "Working with Templates," [www.vmware.com/support/vc13/doc/c13templateintro.html](http://www.vmware.com/support/vc13/doc/c13templateintro.html)
- VM World News, [www.vmware.com/vmworldnews/esx.html](http://www.vmware.com/vmworldnews/esx.html)

© 2009 Trend Micro, Incorporated. Reservados todos los derechos. Trend Micro y el logotipo en forma de pelota son marcas registradas o marcas comerciales de Trend Micro Incorporated. El resto de los nombres de productos o empresas pueden ser marcas comerciales o registradas de sus respectivos propietarios. La información del presente documento puede modificarse sin previo aviso. (WP04\_VirtSec\_100524ES)