

TREND MICRO SEGURIDAD RENTABLE PARA LA VIRTUALIZACIÓN

La virtualización puede ayudar a su organización a lograr un importante ahorro en las operaciones de los centros de datos: puede reducir los costes de hardware y las demandas de energía y conseguir una mayor flexibilidad a la hora de implementar aplicaciones de software de vital importancia. Las organizaciones se han beneficiado de la consolidación para implementar diez o más equipos virtuales (VM, Virtual Machine) por cada servidor físico en su infraestructura de TI, y su negocio puede utilizar esta tecnología para lograr resultados similares.

El mayor reto al que podría enfrentarse su personal de TI en lo que a virtualización respecta consiste en aplicar mecanismos de seguridad que permitan obtener el máximo rendimiento de la inversión en virtualización. Ello incluye permitir albergar equipos virtuales con distintos niveles de seguridad en el mismo servidor físico, ofrecer una protección continua al tiempo que se usan mecanismos tales como vMotion, proteger los equipos virtuales cuando estén inactivos o sin conexión y ampliar el entorno de virtualización para aprovechar las ventajas de la informática a través de Internet. Trend Micro ofrece soluciones para asegurarle que pueda utilizar de forma total y segura su entorno de virtualización.

Mejoras en la seguridad para la virtualización

Las soluciones Trend Micro™ Virtualization Security ofrecen un software de seguridad avanzado para proteger sistemas operativos, aplicaciones y datos de servidores virtuales y en Internet para ayudar a garantizar el cumplimiento de políticas, al tiempo que permiten una mayor tasa de consolidación de los servidores y maximizan el rendimiento y la flexibilidad de funcionamiento.

Con el software de Trend Micro implementado en los servidores físicos y equipos virtuales, su infraestructura de TI recibe una protección global e integrada, que incluye lo siguiente:

- Cortafuegos
- Sistema de detección y prevención de intrusiones (IDS/IPS)
- Protección de aplicaciones Web
- Control de aplicaciones
- Supervisión de integridad
- Inspección de registros
- Protección frente al malware

La solución ayuda a asegurar el cumplimiento de normativas y estándares tales como PCI DSS, HIPAA, leyes de notificación de infracciones y políticas corporativas.

Componentes de la solución

La solución combinada Virtualization Security consta de dos productos, Trend Micro™ Deep Security y Trend Micro™ Core Protection for Virtual Machines, que ayudan a detener los ataques antes de que afecten a datos, aplicaciones y recursos básicos.

Deep Security ofrece protección para servidores y aplicaciones y permite a los equipos virtuales defenderse por sí solos. Core Protection for Virtual Machines es una solución antimalware en la que se ha tenido en cuenta la virtualización y que aprovecha las API de VMware VMSafe™ para asegurar equipos virtuales tanto activos como inactivos.

- **Deep Security Manager:** un potente sistema de gestión centralizado que permite a los administradores crear perfiles de seguridad y aplicarlos a los servidores. Con una consola centralizada para supervisar alertas y acciones preventivas emprendidas como respuesta a las amenazas, puede configurarse para automatizar o distribuir actualizaciones de seguridad a los servidores bajo petición. También permite generar informes para lograr una óptima visibilidad y cumplimiento de políticas.
- **Deep Security Agent:** pequeño componente de software que se implementa en los equipos virtuales que se van a proteger, con el fin de aplicar las políticas de seguridad y permitir funciones de supervisión de integridad e inspección de registros. Defiende a los equipos virtuales supervisando el tráfico entrante y saliente en busca de desviaciones de los protocolos, contenido que indique un ataque o infracciones de políticas. Cuando es necesario, interviene para neutralizar la amenaza bloqueando el tráfico malicioso.
- **Centro de seguridad:** equipo especializado de expertos en seguridad que ayuda a su empresa a anticiparse a las amenazas más recientes creando y entregando rápidamente actualizaciones de seguridad que solucionan las nuevas vulnerabilidades descubiertas y minimizan el riesgo. También gestiona el portal del cliente que se utiliza para acceder a estas actualizaciones e información sobre seguridad. Las actualizaciones de seguridad pueden entregarse automáticamente o bajo petición a Deep Security Manager para implementarlas en miles de servidores en cuestión de minutos.
- **Core Protection for Virtual Machines** ofrece una exploración dedicada para equipos virtuales, coordinada con agentes en tiempo real situados en cada equipo virtual para protegerlos frente al malware que intente evitar ser detectado mediante la desinstalación, inhibición o implementación fraudulenta de parches de la solución de seguridad antivirus.

TREND MICRO SEGURIDAD RENTABLE PARA LA VIRTUALIZACIÓN

Defensa de servidor para equipos virtuales

Deep Security ofrece a su centro de datos un amplio abanico de funciones y beneficios:

- Flexibilidad de SO: ofrece una protección orientada y basada en software para que el mayor rango de plataformas que se utilizan para ejecutar aplicaciones básicas y almacenar datos confidenciales, como Microsoft Windows, Solaris y Linux, se ejecuten en entornos físicos o en una plataforma virtual tal como VMware, Citrix o Microsoft.
- Revisión virtual: ayuda a detener ataques sobre vulnerabilidades de software que se suelen encontrar en sistemas operativos y aplicaciones empresariales basadas en Web en las que se basan las organizaciones. Como resultado, las revisiones pueden implementarse de forma más eficaz y regular, con un impacto mínimo en los recursos de TI o el equipo host.
- Detección y prevención de ataques: detecta e impide ataques dirigidos contra datos confidenciales, avisando inmediatamente al personal del intento de ataque.
- Respuesta de seguridad coordinada: la solución coordinará la respuesta de seguridad entre el software Deep Security Agent de un equipo virtual amenazado y Deep Security Virtual Appliance, mediante API de VMsafe que se conectan en Hypervisor, lo que maximiza la eficacia y efectividad de la seguridad.
- Estrecha integración con VMware vCenter Server y ESX Server: esta íntima coordinación permite importar información organizativa y de funcionamiento de nodos vCenter y ESX a Deep Security Manager, así como aplicar seguridad detallada a la infraestructura VMware de una empresa.
- Gestión centralizada basada en Web: este método optimizado permite al personal de TI crear y gestionar políticas de seguridad, así como controlar amenazas y acciones preventivas emprendidas en respuesta a éstas, desde una interfaz familiar, similar a la de Explorer.
- Recomendaciones de protección proactivas: la solución recomienda, de forma proactiva, medidas de protección apropiadas para servidores, basadas en las políticas y aplicaciones implementadas, para asegurarse de forma más rápida y sencilla de que se están siguiendo los pasos adecuados.
- Implementación basada en plantilla: la solución puede integrarse en plantillas virtuales para simplificar la implementación y aumentar fácilmente la actitud de seguridad.

- Implementación automática: la solución garantiza que las configuraciones de seguridad estándar se apliquen de forma coherente y automática a todos los sistemas apropiados, lo que reduce los riesgos.
- Registros: la solución notifica automáticamente al personal de TI cuando se produce un incidente y ofrece un registro detallado sobre quién ha atacado, cuándo lo ha hecho y qué intentó aprovechar.
- Creación de informes: la solución genera y emite una amplia variedad de informes detallados, de forma programada o *ad hoc*, para documentar los intentos de ataques y ofrecer un historial auditable de configuraciones y cambios de seguridad.
- Actualizaciones automáticas: la solución ofrece actualizaciones periódicas de seguridad para impedir el aprovechamiento de vulnerabilidades recientemente descubiertas.

Protección antimalware líder mundial

Trend Micro™ Core Protection for Virtual Machines está diseñado específicamente para entornos VMware ESX/ESXi y:

- Garantiza la seguridad de los equipos virtuales cuando están en estado de inactividad y la protección mediante las actualizaciones de patrones más recientes cuando se activan.
- Protege frente al malware que evita ser detectado mediante la desinstalación, inhibición o implementación fraudulenta de parches de la seguridad antivirus.
- Ofrece una capa de seguridad adicional mediante la ejecución del agente de exploración en un equipo virtual distinto al equipo que se está explorando.
- Se sincroniza continuamente con la consola de gestión de VMware vCenter para liderar las dinámicas de equipos virtuales y reducir la complejidad que implica gestionar entornos virtuales.
- Configura automáticamente nuevos equipos virtuales de exploración de la seguridad para gestionar mejor la expansión de los equipos virtuales.
- Optimiza las exploraciones de todo el sistema que requieren un elevado rendimiento sin necesidad de volver a configurar.
- Funciona a la perfección en implementaciones de Trend Micro OfficeScan™ Client Server Suite.

Para obtener más información, puede visitarnos en:

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