Trend Micro™

DEEP SECURITY 9

Una plataforma de seguridad completa para servidores físicos, virtuales y basados en la nube

La virtualización y la computación en la nube han cambiado la fisionomía del centro de datos actual. A pesar de que las organizaciones están realizando una transición desde entornos físicos hasta una amalgama de elementos físicos, virtuales y basados en la nube, muchas de ellas se están enfrentando al imperante panorama de amenazas con una mezcla obsoleta de soluciones de seguridad heredadas. De hecho, los resultados pueden amenazar las ganancias de rendimiento deseadas y aumentar la complejidad operativa, lo que puede crear agujeros de seguridad inesperados y, en última instancia, frenar la capacidad de la organización para invertir plenamente en la virtualización y en la nube.

Trend Micro Deep Security ofrece una completa plataforma de seguridad para servidores diseñada con el objetivo de proteger los centros de datos virtualizados de las filtraciones de datos y de garantizar la continuidad de la actividad empresarial, permitiendo al mismo tiempo el cumplimiento de los estándares. Esta solución sin agente simplifica las operaciones de seguridad y acelera el retorno de la inversión de los proyectos de virtualización y computación en la nube. Cuenta, además, con módulos integrados a la perfección para ampliar la plataforma y garantizar la seguridad del servidor, las aplicaciones y los datos en servidores físicos, virtuales y basados en la nube así como en equipos de sobremesa virtuales. De este modo, podrá adaptar la seguridad a su medida con posibilidad de elegir una protección basada en agente o sin él y de incluir las características de antimalware, reputación Web, cortafuegos, prevención de intrusiones, supervisión de la integridad e inspección de registros. El resultado es una plataforma de seguridad para servidores adaptable y eficiente que protege las aplicaciones y los datos empresariales de máxima importancia frente a filtraciones e interrupciones comerciales sin tener que aplicar costosos parches de urgencia.

Acelera el retorno de la inversión en virtualización, VDI y la nube

- Ofrece un modo más ligero y fácil de gestionar para proteger los equipos virtuales (VM) con la primera y única plataforma de seguridad sin agente del sector diseñada específicamente para entornos VMware.
- Se basa en una arquitectura de seguridad sin agente que mejora la eficiencia de los recursos gracias a la desduplicación de la exploración del servidor ESX.
- Mejora la eficiencia del uso de los recursos y proporciona el triple de densidades de VM que las soluciones antimalware tradicionales.
- Mejora la facilidad de la gestión de la seguridad en entornos VMware gracias a la reducción de la necesidad de configurar y actualizar los agentes y aplicarles parches continuamente.
- Protege los equipos de sobremesa virtuales VMware View en el modo local con un agente opcional.
- Coordina la protección con un appliance virtual y agentes para permitir una protección continuada y optimizada de los servidores virtuales a medida que se trasladan entre el centro de datos y la nube pública.

CARACTERÍSTICAS PRINCIPALES

Maximiza las reducciones de costes operativos

- Reduce la complejidad al integrarse de forma óptima en las consolas de gestión de Trend Micro, VMware y en los directorios empresariales.
- Ofrece protección frente a vulnerabilidades para priorizar la codificación segura y la implementación rentable de los parches no programados.
- Elimina el coste que supone implementar múltiples clientes de software mediante un agente de software o appliance virtual de varios servicios y gestión centralizada.
- Reduce los costes de gestión al automatizar las tareas de seguridad repetitivas y con gran consumo de recursos, con la consiguiente disminución de alertas de seguridad sobre falsos positivos y el establecimiento de un flujo de trabajo para la respuesta ante incidentes de seguridad.
- Reduce drásticamente la complejidad de la gestión de la supervisión de la integridad mediante listas blancas de sucesos basadas en la nube y sucesos de confianza.

Evita las filtraciones de datos y las interrupciones en la productividad empresarial

- Detecta y elimina el malware en tiempo real con un impacto mínimo en el rendimiento.
- Bloquea el malware que intenta evadir la detección mediante su desinstalación o que interrumpe de otro modo el programa de seguridad.
- Protege de las vulnerabilidades conocidas y no conocidas de las aplicaciones empresariales Web y los sistemas operativos.
- Detecta la actividad sospechosa o maliciosa y envía alertas sobre ella para que puedan realizarse acciones proactivas y preventivas.
- Utiliza las funciones de reputación Web de una de las bases de datos de reputación de dominios más extensa del mundo para rastrear la credibilidad de los sitios Web y evitar que los usuarios visiten sitios infectados.

Permite conseguir un cumplimiento de políticas rentable

- Satisface los requisitos de las principales normativas de PCI DSS 2.0, así como HIPAA, NIST y SAS 70 con una solución integrada y rentable.
- Proporciona informes detallados y auditables que describen los ataques que se han evitado y el estado de cumplimiento de políticas.
- Reduce el tiempo y el trabajo de preparación de auditorías.
- Admite iniciativas de cumplimiento de normativas internas para aumentar la visibilidad de la actividad de la red interna.
- Hace uso de la probada tecnología certificada para Common Criteria EAL 4+.

MÓDULOS DE LA PLATAFORMA DEEP SECURITY

Antimalware

- Integra las API de VMware vShield Endpoint para proteger los equipos virtuales VMware frente a virus, spyware, troyanos y otros tipos de malware sin impacto en el equipo invitado.
- Proporciona un agente antimalware para ampliar la protección tanto a servidores físicos como a servidores públicos en la nube.
- ¡NOVEDAD! Mejora el rendimiento gracias a los niveles de caché y la desduplicación que ofrece ESX.
- Optimiza las operaciones de seguridad para evitar las tormentas de antivirus que suelen experimentarse en las exploraciones completas del sistema y las actualizaciones de patrones.
- Aísla el malware del antimalware para impedir las modificaciones de la seguridad perpetradas por ataques sofisticados en entornos virtuales.

Supervisión de la integridad

- Supervisa los archivos del sistema operativo y de aplicaciones básicos (directorios, claves de registro, valores, etc.) para detectar en tiempo real cambios maliciosos e inesperados y crear informes al respecto.
- ¡NOVEDAD! Utiliza la tecnología Intel TPM/TXT para ofrecer la supervisión de integridad del hipervisor. Controla los cambios no autorizados que se realizan en el hipervisor, lo que amplía la seguridad y el cumplimiento de normativas de los sistemas virtualizados en el hipervisor.
- Reduce la sobrecarga administrativa gracias al etiquetado de sucesos de confianza que replica automáticamente acciones para sucesos similares en todo el centro de datos.
- Simplifica la administración mediante una reducción drástica del número de sucesos inofensivos conocidos gracias a listas blancas automáticas basadas en la nube de Trend Micro Certified Safe Software Service.

Reputación Web

- Se integra con Trend Micro™ Smart Protection Network™ para utilizar sus funciones de reputación Web y fortalecer así la protección en servidores y equipos de sobremesa virtuales.
- Proporciona reputación Web sin agente en el mismo appliance virtual así como características de antimalware y prevención de intrusiones sin agente para una mayor seguridad del servidor virtual sin carga adicional en el sistema.

Detección y prevención de intrusiones

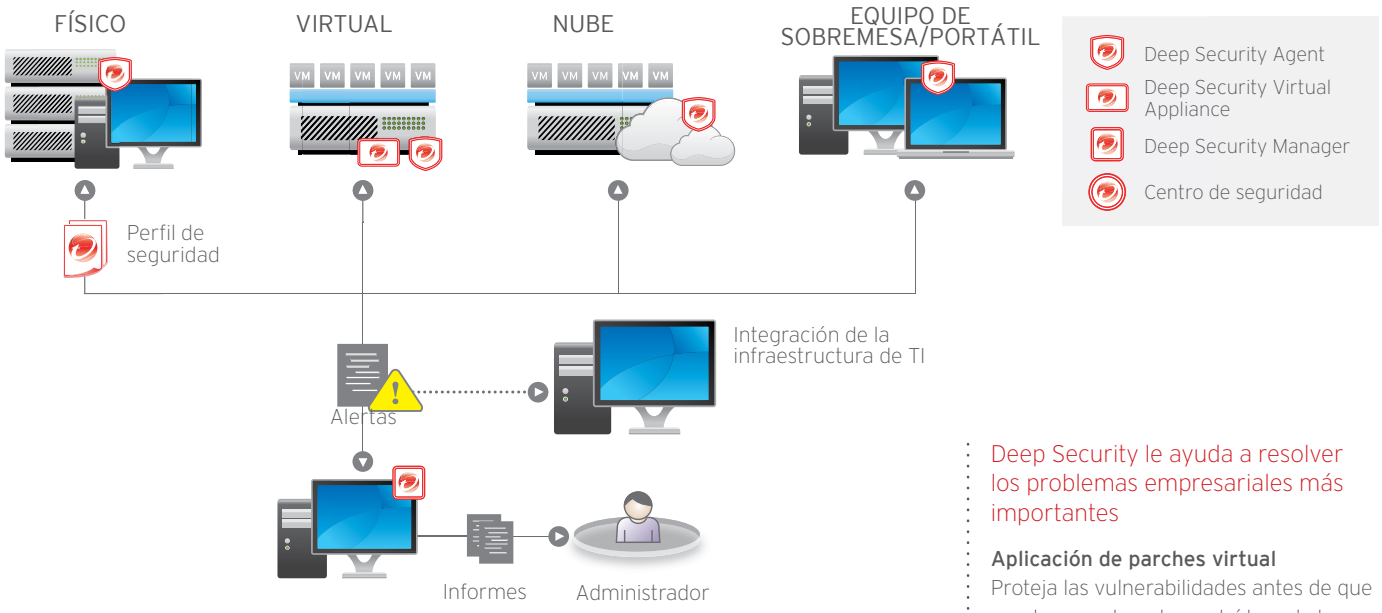
- Protege frente a los ataques conocidos y de día cero ya que evita las vulnerabilidades conocidas de un gran número de ataques.
- Examina todo el tráfico entrante y saliente en busca de desviaciones del protocolo, contenido con signos de ataque o infracciones de las políticas.
- Protege automáticamente de las nuevas vulnerabilidades descubiertas en cuestión de horas, aplicando la protección en miles de servidores en solo unos minutos y sin tener que reiniciar el sistema.
- Ayuda al cumplimiento de normativas (PCI DSS 6.6) para proteger las aplicaciones Web y los datos que procesan.
- Protege frente a SQL Injection, secuencias de comandos de sitios cruzados y otras vulnerabilidades de las aplicaciones Web.
- Ofrece una defensa frente a las vulnerabilidades hasta que se puedan completar las correcciones del código.
- Incluye protección inmediata de vulnerabilidades para los sistemas operativos principales y más de 100 aplicaciones, incluidas bases de datos, sitios Web, correo electrónico y servidores FTP.
- Ofrece una mayor visibilidad o control de las aplicaciones que acceden a la red.

Cortafuegos de inspección de estado bidireccional

- Disminuye la superficie del ataque de los servidores físicos, virtuales y basados en la nube mediante un filtrado avanzado, el diseño de políticas por red y la notificación de la ubicación para los protocolos basados en IP y tipos de tramas.
- Gestiona centralizadamente las políticas del cortafuegos del servidor, incluidas las plantillas de tipos de servidores habituales.
- Evita ataques de denegación de servicios y detecta exploraciones de reconocimiento.

Inspección de registros

- Recopila y analiza sistemas operativos y registros de aplicaciones en busca de comportamiento sospechoso, sucesos de seguridad y sucesos administrativos en todo el centro de datos.
- Contribuye al cumplimiento de políticas (PCI DSS 10.6) para optimizar la identificación de sucesos de seguridad importantes ocultos en múltiples entradas del registro.
- Reenvía los sucesos al sistema SIEM o el servidor de registro centralizado para las tareas de correlación, documentación y archivado.



DISEÑADO PARA ENTORNOS VIRTUALES VMWARE Y BASADOS EN LA NUBE

Deep Security está específicamente diseñado para entornos virtuales. Su arquitectura sin agente soluciona las tormentas antivirus, minimiza la complejidad operacional de la seguridad y permite a las organizaciones aumentar las densidades de VM y acelerar la adopción de infraestructuras virtuales y basadas en la nube. Desarrollado en estrecha colaboración con VMware, Deep Security es el primer producto de su categoría en ofrecer compatibilidad con VMware vSphere 5.1 y VMware vShield Endpoint 5.1. Deep Security también ofrece total compatibilidad con versiones anteriores de entornos vSphere 4.1 y 5.0. Por su parte, Deep Security 9 Manager también es compatible con entornos VMware del modo mixto que admitan tanto vSphere 5.1 como vSphere 5.0 protegidos por appliances virtuales de Deep Security 9 o 8.

ARQUITECTURA DE LA PLATAFORMA

Deep Security Virtual Appliance. Aplica las políticas de seguridad de forma transparente en los equipos virtuales VMware vSphere para las características sin agente de antimalware, reputación Web, prevención de intrusiones, supervisión de integridad, protección de cortafuegos. Si se desea, pueden realizarse estas tareas en coordinación con Deep Security Agent para garantizar la inspección de registros y una defensa exhaustiva.

Deep Security Agent. Este pequeño componente de software instalado en el servidor o equipo virtual que se desea proteger aplica la política de seguridad del centro de datos (antimalware, reputación Web, prevención de intrusiones, cortafuegos, supervisión de integridad e inspección de registros).

Deep Security Manager. Una gestión centralizada y eficaz permite a los administradores crear perfiles de seguridad y aplicarlos en servidores, supervisar alertas y acciones preventivas realizadas en respuesta a las amenazas, distribuir actualizaciones de seguridad entre los servidores y generar informes. La funcionalidad de etiquetado de sucesos acelera la gestión de los sucesos de gran volumen.

Smart Protection Network. Deep Security se integra en esta infraestructura Cloud-Client de última generación para ofrecer una protección en tiempo real frente a las amenazas emergentes, mediante la evaluación y correlación continuas de las amenazas y la información sobre la reputación de sitios Web, recursos de correo electrónico y archivos.

Deep Security le ayuda a resolver los problemas empresariales más importantes

Aplicación de parches virtual
Proteja las vulnerabilidades antes de que puedan ser atacadas y olvídese de los problemas operativos que comporta la aplicación de parches de urgencia, los ciclos frecuentes de parches y los costosos periodos de inactividad del sistema.

Seguridad para equipos de sobremesa y servidores virtuales
Proteja los equipos de sobremesa y los servidores virtuales del malware de día cero a la vez que minimiza el impacto operativo derivado del bloqueo de recursos y la aplicación de parches de urgencia.

Cumplimiento de normativas
Podrá conseguir y probar el cumplimiento de una gran cantidad de requisitos normativos como PCI DSS 2.0, HIPAA, FISMA/NIST, NERC. SAS 70 y muchos otros.

Seguridad para servidores integrada
Consolide todos los productos puntuales de seguridad para servidores en una sola plataforma flexible, integrada y completa que optimiza la protección de servidores físicos, virtuales y basados en la nube.

Seguridad en la nube
Aplique las políticas de seguridad de su centro de datos a las cargas de trabajo públicas e híbridas de Internet y gestione tanto los centros de datos como las cargas de trabajo en la nube mediante un solo panel de vidrio. Deep Security combina tecnologías avanzadas como la prevención de intrusiones y la supervisión de la integridad con la tecnología de gestión de claves basada en políticas, disponible si se integra con SecureCloud. Todo ello garantiza la seguridad del servidor, las aplicaciones y los datos de Internet.

IMPLEMENTACIÓN E INTEGRACIÓN

Una implementación rápida que usa las inversiones existentes en TI y seguridad

- La integración con las API de vShield Endpoint y VMsafe™, así como VMware vCenter, permite la rápida implementación en los servidores ESX como appliance virtual para proteger los equipos virtuales vSphere de forma inmediata y transparente.
- Los sucesos de seguridad detallados del servidor están disponibles en un sistema SIEM, incluidos ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic y otros sistemas mediante numerosas opciones de integración.
- Permite la integración con directorios empresariales como Microsoft Active Directory.
- El software con agente se puede implementar fácilmente mediante mecanismos de distribución de software estándar como Microsoft® SMS, Novel Zenworks y Altiris.

Certificaciones y alianzas principales

- Common Criteria EAL 4+
- Prueba de idoneidad según la norma PCI para HIPS (NSS Labs)
- Virtualización por VMware
- Programa de protección de aplicaciones de Microsoft
- Partner certificado de Microsoft
- Partner de Oracle
- Partner de HP Business
- Certificación Red Hat Ready

REQUISITOS DEL SISTEMA

Microsoft® Windows®

- XP (32/64 bits)
- XP Embedded
- Windows 7 (32/64 bits)
- Windows Vista (32/64 bits)
- Windows Server 2003 (32/64 bits)
- Windows Server 2008 R2 (64 bits)

Linux

- Red Hat® Enterprise 5, 6 (32/64 bits)[1]
- SUSE® Enterprise 10, 11 (32/64 bits)[1]

Solaris™

- Sistema operativo: 8, 9, 10 (SPARC de 64 bits), 10 (x86 de 64 bits)[1]

UNIX

- AIX 5.3, 6.1 en IBM Power Systems[2]
- HP-UX 11i v3 (11.31)[2]

VIRTUAL

- **VMware®:** ESX/ESXi 3.x[3], vSphere 4.0[4], vSphere 4.1/5.0[5], View 4.5/5.0[5]
- **Citrix®:** XenServer[3]
- **Microsoft®:** HyperV[3]

[1] Antimalware no disponible.

[2] En esta plataforma solo están disponibles la supervisión de la integridad y la inspección de registros.

[3] Protección solo a través de Deep Security Agent.

[4] Protección a través de Deep Security Agent y Virtual Appliance para cortafuegos, IDS/IPS y protección de las aplicaciones Web; a través del agente solo para otros módulos.

[5] Protección a través de Deep Security Agent únicamente para la inspección de registros, a través del agente y el appliance virtual para el resto de módulos. Se requiere una licencia independiente para vShield Endpoint.

TREND MICRO™

Securing Your Journey to the Cloud.

©2012 por Trend Micro Incorporated. Reservados todos los derechos. Trend Micro, el logotipo en forma de pelota de Trend Micro, OfficeScan y Trend Micro Control Manager son marcas registradas o marcas comerciales de Trend Micro Incorporated. El resto de los nombres de productos y empresas pueden ser marcas comerciales o marcas registradas de sus respectivos propietarios. La información del presente documento puede modificarse sin previo aviso. [DS01_DeepSecurity9_120812ES]