

Trend Micro™

# Deep Security 7.5

Protección de servidores y aplicaciones para los centros de datos dinámicos

Las grandes empresas optan cada vez más por las operaciones en línea y la centralización de datos, para conectar a partners, personal, proveedores o clientes a las aplicaciones que se enfrentan a un número creciente de ciberataques. Estas amenazas dirigidas son más numerosas y sofisticadas que nunca, y las normativas de protección de datos son cada día más estrictas. Su empresa necesita una seguridad rigurosa que le permita modernizar el centro de datos con la virtualización y la computación basada en Internet, todo ello sin reducir el rendimiento.

**Trend Micro Deep Security** le brinda una seguridad avanzada para servidores físicos, virtuales y de Internet, así como para equipos de sobremesa virtuales. Independientemente de su implementación como software, appliance virtual o en un enfoque híbrido, esta solución minimiza la carga administrativa, agiliza la gestión y ofrece una seguridad eficaz sin agente para equipos virtuales. Asimismo, Deep Security garantiza una amplia variedad de requisitos del cumplimiento de políticas, incluidos siete requisitos de PCI principales con los múltiples módulos de protección unificados en una sola solución.

## ARQUITECTURA

**¡NOVEDAD! Deep Security Virtual Appliance:** aplica las políticas de seguridad de forma transparente en los equipos virtuales VMware vSphere para sistemas de detección y prevención de intrusiones (IDS/IPS) sin agente, protección de las aplicaciones Web, control de aplicaciones y cortafuegos. Puede realizar estas tareas en coordinación con Deep Security Agent para la supervisión de la integridad y la inspección de registros.

**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 (sistema de detección y prevención de intrusiones, protección de las aplicaciones Web, control de aplicaciones, 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 nueva funcionalidad de etiquetado de sucesos acelera la gestión de los sucesos de gran volumen.

**Security Center:** nuestro equipo especializado de expertos en seguridad le ayuda a anticiparse a las amenazas más recientes creando y entregando rápidamente actualizaciones de seguridad que solucionan las nuevas vulnerabilidades descubiertas. Se trata de un portal para clientes que proporciona acceso a las actualizaciones de seguridad que se entregan a Deep Security Manager para su implementación.

**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.

## 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 programa agente se puede implementar fácilmente mediante mecanismos de distribución de software estándar como Microsoft® SMS, Novell Zenworks y Altiris.

## PRINCIPALES BENEFICIOS

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

- Ofrece una línea de defensa en el servidor, ya sea físico, virtual o por Internet.
- Protege de las vulnerabilidades conocidas y no conocidas de las aplicaciones y los sistemas operativos.
- Protege las aplicaciones Web frente a SQL Injection y secuencias de comandos de sitios cruzados.
- Bloquea los ataques a los sistemas empresariales.
- Identifica la actividad y el comportamiento sospechosos, y ofrece medidas proactivas y preventivas.

**Permite el cumplimiento de la normativa PCI y otras normas y estándares**

- Cumple siete principales normativas de seguridad PCI y muchos otros requisitos para el cumplimiento de normativas.
- 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.

**Disminuye los costes operativos**

- Permite una mayor consolidación de los equipos virtuales para optimizar los ahorros en materia de virtualización y computación basada en Internet.
- Ofrece antimalware y otros mecanismos de seguridad en una configuración sin agente para simplificar la gestión de los entornos de servidores y equipos de sobremesa virtuales.
- Automatiza la gestión de los sucesos de seguridad para agilizar la administración en todos los servidores.
- 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.

## MÓDULOS DE DEEP SECURITY

### ¡NOVEDAD! Protección antimalware sin agente para entornos VMware

- Integra la nueva API de VMware vShield Endpoint para puntos finales que protege los equipos virtuales VMware frente a virus, spyware, troyanos y otro tipo de malware sin impacto en el invitado.
- Optimiza las operaciones de seguridad para evitar las interrupciones de la seguridad 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 los ataques sofisticados.

### Inspección profunda de paquetes

- Examina todo el tráfico entrante y saliente en busca de desviaciones del protocolo, contenido con signos de ataque o infracciones de las políticas.
- Funciona en los modos de detección o prevención para proteger los sistemas operativos y las vulnerabilidades de las aplicaciones empresariales.
- Envía notificaciones automáticas sobre quién atacó, cuándo atacó y qué vulnerabilidad intentó aprovechar.

### 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.
- Protege automáticamente de las vulnerabilidades recientemente descubiertas en cuestión de horas, aplicando la protección en miles de servidores en solo unos minutos y sin tener que reiniciar el sistema.
- Incluye protección inmediata de vulnerabilidades para más de 100 aplicaciones, incluidas bases de datos, sitios Web, correo electrónico y servidores FTP.

### Protección de aplicaciones Web

- 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.

### Control de aplicaciones

- Ofrece una mayor visibilidad o control de las aplicaciones que acceden a la red.
- Usa reglas de control de aplicaciones para identificar el software malicioso que accede a la red.
- Reduce la exposición de los servidores a las vulnerabilidades.

### Cortafuegos de inspección de estado bidireccional

- Disminuye la superficie del ataque de los servidores físicos, virtuales y de Internet 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.

### Supervisión de integridad

- Supervisa los archivos del sistema operativo y de aplicaciones básicas (directorios, claves de registro, valores, etc.) para detectar cambios maliciosos e inesperados.
- Detecta las modificaciones en los sistemas de archivos existentes así como las nuevas creaciones de archivos, y lo notifica en tiempo real.
- Permite realizar detecciones bajo petición, programadas o en tiempo real. Comprueba las propiedades de los archivos (PCI 10.5.5) y supervisa directorios específicos.

### 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.
- Ayuda al cumplimiento de políticas (PCI DSS 10.6) para optimizar la identificación de sucesos de seguridad importantes escondidos 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.

## PLATAFORMAS PROTEGIDAS

### Microsoft® Windows®

- 2000 (32 bits)
- 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 (32/64 bits)
- Windows Server 2008 R2 (64 bits)

### Solaris™

- SO: 8, 9, 10 (SPARC de 64 bits), 10 (x86 de 64 bits)

### Linux

- Red Hat® Enterprise 4.0, 5.0 (32/64 bits)
- SUSE® Enterprise 10, 11 (32/64 bits)

### UNIX®\*

- AIX 5.3, 6.1
- HP-UX® 10, 11i v2/v3

\* Solo disponibles los módulos de supervisión de integridad e inspección de registros

## VIRTUALIZACIÓN

- **Appliance virtual:** VMware vSphere 4.1
- **VMware®:** VMware ESX 4.1 Server (SO invitado)
- **Citrix®:** XenServer
- **Microsoft®:** HyperV
- **Sun:** contenedores Solaris 10

## CERTIFICACIONES Y ALIANZAS CLAVE

- Common Criteria EAL 3+ (EAL 4 en curso)
- 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
- Novell
- Partner de Oracle
- Partner de HP Business
- Certificación Red Hat Ready

| Requisito del centro de datos                | Inspección profunda de paquetes |                                |                         | Cortafuegos | Supervisión de integridad | Inspección de registros | ¡NOVEDAD! Antimalware |
|--|---------------------------------|--------------------------------|-------------------------|-------------|---------------------------|-------------------------|-----------------------|
|  | IDS/IPS                         | Protección de aplicaciones Web | Control de aplicaciones |             |                           |                         |                       |
| Protección de servidores                     | ●                               |                                |                         | ●           | ●                         | ○                       | ●                     |
| Seguridad de las aplicaciones Web            | ●                               | ●                              |                         |             | ○                         | ●                       |                       |
| Seguridad de virtualización                  | ●                               | ○                              |                         | ●           | ●                         | ○                       | ●                     |
| Detección de comportamiento sospechoso       | ○                               |                                | ●                       | ●           | ●                         | ●                       |                       |
| Seguridad de sistemas basados en Internet    | ●                               | ○                              |                         | ●           | ●                         | ●                       | ●                     |
| Informes sobre el cumplimiento de normativas | ○                               | ●                              | ○                       | ○           | ●                         | ●                       |                       |
| Basado en agente                             | ●                               | ●                              | ●                       | ●           | ●                         | ●                       |                       |
| Consola unificada                            | ●                               | ●                              | ●                       | ●           |                           |                         | ●                     |

● Básico ○ Ventajoso



©2010 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. [DS03DeepSecurity7.5\_100721ES]

[www.trendmicro.com](http://www.trendmicro.com)