

Trend Micro™

Deep Security 7

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. Además, independientemente de su finalidad (conectar a socios, personal o clientes), las aplicaciones han de enfrentarse 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 infalible que permite la modernización del centro de datos con sistemas virtuales y basados en Internet, sin mermar el rendimiento.

Trend Micro ofrece productos, servicios y soluciones optimizadas e integradas que protegen de forma asequible los datos confidenciales y minimizan los riesgos. Deep Security es una completa solución de protección de servidores y aplicaciones que permite que los entornos físicos, virtuales e informáticos por Internet sean capaces de autoprotgerse. Independientemente de si se implementa como un software, un appliance virtual o en un enfoque híbrido, esta solución reduce al mínimo la sobrecarga, agiliza la gestión y refuerza la seguridad invisible para los equipos virtuales. Deep Security también permite satisfacer una amplia gama de requisitos de cumplimiento, incluidos los seis principales requisitos de cumplimiento de normativas PCI con cortafuegos en la capa de aplicaciones Web, sistema de detección y prevención de intrusiones (IDS/IPS), supervisión de la integridad de los archivos y segmentación de red.

ARQUITECTURA

- **Deep Security Virtual Appliance:** aplica las políticas de seguridad de forma transparente en los equipos virtuales VMware vSphere para los sistemas de detección y prevención de intrusiones, protección de aplicaciones Web, control de aplicaciones y protección del cortafuegos, en combinación con Deep Security Agent, si así lo desea, para la supervisión de integridad e 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 agiliza 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. Un portal para clientes le ofrece acceso a las actualizaciones de seguridad que se entregan a Deep Security Manager para su implementación.

IMPLEMENTACIÓN E INTEGRACIÓN

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

- La integración de VMware con VMware vCenter y ESX Server permite importar información organizativa y operacional en Deep Security Manager, y que se aplique una seguridad pormenorizada en la infraestructura empresarial de VMware.
- La integración con las API VMsafe™ permite la implementación rápida en los servidores de ESX, como un 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.
- La comunicación configurable de la gestión minimiza o elimina los cambios del cortafuegos que suelen ser necesarios en sistemas gestionados centralizadamente gracias a la activación del componente Manager o Agent para iniciar la comunicación.
- El programa agente se puede implementar fácilmente mediante mecanismos de distribución de software estándar como Microsoft® SMS, Novel 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 de SQL Injection y secuencias 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 seis de los principales estándares 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

- Optimiza el ahorro en costes de virtualización o de la informática en Internet al unificar los recursos del servidor.
- Agiliza la administración mediante la gestión automática de los sucesos de seguridad.
- Ofrece protección frente a vulnerabilidades para priorizar la codificación segura e implementar de forma asequible los parches no programados.
- Elimina el coste de implementación de múltiples clientes de software con un agente de software o appliance virtual para diversos usos con administración centralizada.

MÓDULOS DE DEEP SECURITY

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.
- Ofrece una defensa frente a los ataques en la capa de aplicaciones, SQL Injection y secuencias de sitios cruzados.
- Ofrece información valiosa, que indica quién atacó, cuándo atacó y qué vulnerabilidad intentó aprovechar.
- Notifica automáticamente a los administradores cuando se produce un incidente.

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.
- Las reglas inteligentes ofrecen protección de día cero frente a ataques no conocidos que pueden aprovechar una vulnerabilidad no conocida mediante la detección de datos del protocolo no usuales que contienen código malicioso.

Supervisión de integridad

- Supervisa los archivos del sistema operativo y de aplicaciones básicos (directorios, claves de registro, valores, etc.) para detectar cambios maliciosos e inesperados.
- Detecta modificaciones en los sistemas de archivos existentes y las 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.
- Ofrece una supervisión flexible y práctica mediante inclusiones/exclusiones e informes auditables.

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 de ataque de los servidores físicos, por Internet y virtuales.
- Gestiona centralizadamente las políticas del cortafuegos del servidor, incluidas las plantillas de tipos de servidores habituales.
- Cuenta con un filtrado preciso (direcciones IP y MAC, puertos), políticas de diseño para la interfaz de red y reconocimiento de ubicación.
- Evita ataques de denegación de servicios y detecta exploraciones de reconocimiento.
- Cubre todos los protocolos basados en IP (TCP, UDP, ICMP, etc.) y todos los tipos de tramas (IP, ARP, etc.).

Inspección de registros

- Recopila y analiza sistemas operativos y registros de aplicaciones en busca de eventos de seguridad.
- Ayuda al cumplimiento de normativas (PCI DSS 10.6) para optimizar la identificación de eventos 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.
- Detecta el comportamiento sospechoso, recopila sucesos de seguridad y acciones administrativas en el centro de datos, y crea reglas avanzadas usando la sintaxis OSSEC.

PLATAFORMAS PROTEGIDAS

Microsoft® Windows®

- 2000 (32 bits)
- XP (32/64 bits)
- XP Embedded
- Windows 7
- Windows Vista (32/64 bits)
- Windows Server 2003 (32/64 bits)
- Windows Server 2008 (32/64 bits)

Solaris™

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

Linux

- Red Hat® Enterprise 3.0 (32 bits), 4.0, 5.0 (32/64 bits)
- SUSE® Enterprise 9, 10 (32 bits)

UNIX® *

- AIX 5.3
- HP-UX® 10, 11i v2, 11i v3

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

VIRTUALIZACIÓN

- VMware®: VMware ESX Server (SO invitado)
- Citrix®: XenServer Guest VM
- Microsoft®: HyperV Guest VM
- Sun: particiones del SO Solaris 10

CERTIFICACIONES Y ALIANZAS CLAVE

- Common Criteria EAL 3+
- Prueba de idoneidad según la norma PCI para HIPS (NSS Labs)
- Virtualización por VMware
- Programa de protección de aplicaciones de Microsoft
- Socio certificado de Microsoft
- Novell
- Socio de Oracle
- Socio de HP Business
- Certificación Red Hat Ready

MÓDULOS DE DEEP SECURITY						
Requisito del centro de datos	Inspección profunda de paquetes			Cortafuegos	Supervisión de integridad	Inspección de registros
	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	○	●	○	○	●	●

● Esencial ○ Ventajoso



©2009 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. [DS01DeepSecurity7_091019ES]

www.trendmicro.com