

Trend Micro™

# Deep Security 7

La alternativa a CSA recomendada por Cisco

Si su empresa utiliza Cisco CSA, entonces sabrá hasta qué punto es importante defender los servidores, equipos de sobremesa y portátiles (puntos finales) frente al malware y los ataques de día cero caracterizados por su elevado nivel de sofisticación. Hasta ahora, ha dependido de CSA para minimizar los parches de emergencia, prevenir las filtraciones de datos e, incluso, aplicar el cumplimiento de normativas. Sin embargo, ¿dónde va a encontrar una protección ininterrumpida de día cero cuando CSA se retire del mercado?

Cisco recomienda Trend Micro Deep Security como una alternativa realmente atractiva que ofrece todas las facilidades de migración a los clientes actuales de CSA. Deep Security brinda la misma vigilancia del sistema y protección de día cero a la que está acostumbrado. Además, proporciona características avanzadas que superan a CSA, tales como la protección de los entornos informáticos virtualizados y basados en Internet, mayor compatibilidad de plataformas y una eficaz consola de gestión centralizada. La protección de Deep Security a nivel de red garantiza una implementación inmediata, sin necesidad de largas definiciones de reglas o fases de ajuste, junto con herramientas y servicios opcionales de migración de Trend Micro que pueden facilitar aún más la transición de CSA a Deep Security. Independientemente de si se implementa como software, appliance virtual o en un enfoque híbrido, Deep Security minimiza la carga administrativa, agiliza la gestión y refuerza la seguridad empresarial.

## ARQUITECTURA

- **Deep Security Manager:** permite a los administradores crear perfiles de seguridad y aplicarlos en puntos finales, supervisar alertas y acciones preventivas, distribuir actualizaciones de seguridad entre los puntos finales y generar informes, todo ello mediante una eficaz gestión centralizada. También ofrece una funcionalidad de etiquetado de sucesos que acelera la gestión de los sucesos de gran volumen.
- **Deep Security Agent:** se implementa en el punto final o equipo virtual protegido a modo de pequeño componente de software para aplicar la política de seguridad de la organización (IDS/IPS), la protección de aplicaciones Web, el control de aplicaciones y el cortafuegos.
- **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), protección de las aplicaciones Web, control de aplicaciones y cortafuegos. Puede realizar estas tareas en coordinación con Deep Security Agent, si así lo desea.
- **Centro de seguridad:** realiza actualizaciones de seguridad constantes para que los clientes estén por delante de las últimas amenazas. El portal de clientes ofrece acceso a las actualizaciones de seguridad que se envían para la implementación en Deep Security Manager.

## IMPLEMENTACIÓN E INTEGRACIÓN

### Aprovecha las inversiones existentes en TI y seguridad

- La integración de VMware® con VMware vCenter y ESX Server permite importar información organizativa y operacional a Deep Security Manager, y que se aplique una seguridad pormenorizada en la infraestructura empresarial de VMware.
- La integración con la API de VMsafe™ permite la rápida implementación en los servidores ESX como appliance virtual para proteger los equipos virtuales vSphere de forma inmediata y transparente.
- Ofrece sucesos de seguridad detallados del servidor para 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 los cambios del cortafuegos que suelen ser necesarios en sistemas gestionados centralizadamente.
- El programa agente se implementa fácilmente mediante mecanismos de distribución de software como Microsoft SMS, Novell ZENworks y Altiris.

## PRINCIPALES BENEFICIOS

### Minimiza los parches de emergencias y las infecciones

- Protege de las vulnerabilidades conocidas y no conocidas de las aplicaciones y los sistemas operativos.
- Amplía la seguridad a los servidores críticos que no pueden interrumpir el servicio para la aplicación de parches de vulnerabilidades.
- Identifica la actividad y el comportamiento sospechosos, y ofrece medidas proactivas y preventivas.

### Evita las filtraciones de datos

- Ofrece una línea de defensa en el punto final, ya sea físico, virtual o por Internet.
- Protege las aplicaciones Web frente a SQL Injection, secuencias de comandos de sitios cruzados y otros ataques.
- Bloquea los ataques a los sistemas empresariales.

### Ayuda en el cumplimiento de normativas

- Cumple seis de las principales normativas de seguridad PCI, incluidos 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.

### Reduce los costes operacionales

- Consolida los recursos del servidor para optimizar los ahorros en materia de virtualización y computación basada en Internet.
- Automatiza la gestión de los sucesos de seguridad para agilizar la administración.
- Prioriza la codificación segura y la implementación rentable de parches no programada.
- 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

### 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.
- Notifica automáticamente a los administradores cuando se produce un incidente.
- Identifica quién atacó, en qué momento y qué vulnerabilidad se quiso explotar.

### 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 puntos finales 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.
- Detecta los datos de protocolo inusuales que contienen código malicioso para ofrecer protección de día cero.

### 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 puntos finales, tanto físicos como 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.).

Protección ofrecida	Cisco CSA	Trend Micro Deep Security
IDS/IPS	✓	✓ • Modos de detección y prevención, o solo de detección
Cortafuegos	✓	✓ • Cortafuegos de inspección de estado bidireccional para la red
Protección de aplicaciones Web	✓	✓
Control de aplicaciones	✓	✓ • Bloqueo de las conexiones entrantes/salientes, sin control de aplicaciones local • Introducción del control de aplicaciones local en una versión futura
Conocimiento de ubicación	✓	✓
Supervisión de integridad	✓	✓
Inspección de registros		✓
Prevención frente a la pérdida de datos	✓	✓ • Disponible en otras soluciones de Trend Micro
Antivirus	✓	✓ • Solo entornos virtualizados (también disponible para puntos finales físicos en otras soluciones de Trend Micro)

## 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 R2 (32/64 bits)

### Solaris™

- SO: 8, 9, 10 (SPARC de bits, x86) 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® 11i v3

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

## VIRTUALIZACIÓN

- **Appliance virtual:** VMware vCenter 4 y ESX 4 o ESXi4
- **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
- Partner certificado de Microsoft
- Novell
- Partner de Oracle
- Partner de HP Business
- Certificación Red Hat Ready



© 2010 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 o empresas pueden ser marcas comerciales o registradas de sus respectivos propietarios. [DS01DeepSec\_Cisco\_100518ES]

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