

Trend Micro presenta en Europa Deep Security 8

Según Siemens, uno de sus clientes, los usuarios se "benefician de un mayor nivel de seguridad a un coste significativamente menor"

En el marco de la celebración de VMworld Europe 2011®, Trend Micro Incorporated (TYO: 4704; TSE: 4704), líder global en seguridad cloud, ha anunciado el lanzamiento en Europa de su solución Deep Security 8, consolidando aún más la posición de la solución como la plataforma de seguridad para el servidor más importante de la industria, a través de entornos físicos, virtuales y cloud.

Con nuevas capacidades de monitorización de la integridad sin agente, Trend Micro Deep Security está especialmente diseñada para entornos virtuales VMware vSphere® 5, e incluye comprobación de la integridad hypervisor y otras innovaciones basadas en la nube, Deep Security 8 disminuye las barreras para la adopción de monitorización de la integridad de archivos a través del centro de datos, ayudando a las empresas a alcanzar mayores niveles de protección de los datos y cumplimiento de normativas sin coste añadido ni complejidad.

Deep Security 8

Trend Micro Deep Security ya se ha establecido en el mercado como la oferta de seguridad para virtualización y el servidor líder del mercado. Se trata de una plataforma de seguridad para el servidor que incluye anti-malware, firewall, IDS/IPS, protección de aplicaciones web, monitorización de la integridad e inspección de registros en una solución integrada, Deep Security 8 también aporta las siguientes novedades:

Para servidores físicos:

- Lista blanca automática de eventos basados en cloud y de eventos de confianza configurable con menor complejidad operativa de la monitorización de integridad, y mayor apertura de la tecnología para abarcar a un conjunto mucho más amplio de clientes.
- Anti-malware basado en agente que permite a las organizaciones llevar y ampliar la misma protección de Deep Security a servidores físicos para sistemas operativos Windows y Linux.

Para servidores virtuales:

- Monitorización de la integridad de archivos sin agente, a través del mismo Deep Security Virtual Appliance que ya ofrece anti-malware sin agente y prevención de intrusiones sin agente en entornos virtuales, elimina las tormentas de escaneo de integridad y reduce de forma significativa la complejidad operacional.
- Arquitectura de despliegue flexible que permite seleccionar las máquinas virtuales que se crearán con los agentes opcionales que se coordinarán con el appliance virtual para una mayor defensa en profundidad.
- Monitorización de la integridad del hypervisor que emplea tecnología Intel TPM/TXT, una de las primeras soluciones del mercado disponibles para analizar si el hypervisor está comprometido.
- Soporte para VMware vSphere 5 y VMware vShield™ Manager 5, con VMware vShield Endpoint Security API 2, también permite la compatibilidad con VMware

vSphere 4.1 y con VMware vShield 1.0.

Para desktops virtuales:

- Anti-malware basado en agente para el modo local de VDI que ofrece protección continuamente optimizada de los desktops virtuales a medida que entran y salen del centro de datos.
- Para los entornos de desktop virtual protegidos por Deep Security sin agente anti-malware, Deep Security ahora proporciona la opción End-user Notifier que puede ofrecer notificación del malware en lugar de un de un verdadero agente de anti-malware.

Para servidores cloud:

- Consulte más abajo la integración de Deep Security 8 con SecureCloud 2.

Beneficios adicionales para los usuarios finales

Las empresas sólo necesitan licencia de los componentes de seguridad que requieren actualmente de servidores específicos –para añadir un módulo basta simplemente con cambiar una clave de licencia

Mayores ventajas para los partners de canal

Los partners pueden obtener un portfolio de virtualización diferenciado, así como acuerdos potenciales de mayor envergadura.

Protección cloud total con Deep Security 8 y Trend Micro™ SecureCloud

Trend Micro ha sido el primer fabricante en ofrecer seguridad diseñada para clouds públicas y privadas, y fue pionero en el mercado de seguridad pensada para la virtualización de VMware y de las plataformas de infraestructura cloud. Mientras Deep Security proporciona un contenedor seguro para aplicaciones y servidores en la nube, SecureCloud refuerza a Deep Security mediante la encriptación y protección de datos que utilizan los servidores y las aplicaciones. SecureCloud es una solución de protección de datos en la nube y de gestión de claves de encriptación basada en políticas que facilitan el cifrado de datos y la protección en entornos informáticos físicos, virtualizados y cloud.

En términos generales y de forma sencilla, permite una rápida adopción del cloud, mayor reducción de costes y un mejor cumplimiento de normativas. Con este lanzamiento, los clientes de Deep Security y los partners de canal pueden obtener los beneficios de la integración del cifrado de SecureCloud y las características de gestión de claves basadas en políticas.

Deep Security y SecureCloud trabajan conjuntamente para crear un marco que responda a la constante evolución del estado de los centros de datos dinámicos. Por ejemplo, SecureCloud se comunica con Deep Security utilizando la información del estado de seguridad de Deep Security para asegurarse de que cualquier servidor que solicita acceso a los datos cifrados cuenta con protección actualizada antes de que las claves de cifrado sean liberadas. Si los controles de integridad de Deep Security determinan que una máquina virtual con protección desactualizada o inadecuada está tratando de iniciarse, o que una máquina virtual está comprometida por un ataque, SecureCloud adapta la respuesta y el acceso a los datos de la máquina virtual bloqueándolos mediante la negación de la clave de cifrado, mientras el administrador es avisado de esta acción para tomar medidas de recuperación.

Nuevo y mejorado

SecureCloud 2 también cuenta con nuevas importantes mejoras, entre las que

se incluyen el cifrado de agente completo con certificación FIPS 140-2. Las agencias gubernamentales y empresas están sujetas al cumplimiento de los estándares de seguridad más estrictos, lo que requiere certificación de productos de cifrado FIPS (Estándares de Procesamiento de Información Federal). Además, el nuevo Deep Security Manager (DSM) conecta los puntos que permiten a SecureCloud consultar el DSM y recopilar información sobre los servidores que está protegiendo. Los administradores de SecureCloud pueden crear políticas en torno a esta nueva información y mejorar las reglas por las cuales se rigen los servidores que cuentan con acceso a las claves de cifrado. Esto incrementa la seguridad en general y establece los criterios de validación adicionales solicitados desde el entorno de operación de Deep Security.

SecureCloud se ofrece como una solución SaaS alojada disponible bajo la opción de dos meses de prueba gratuita, o como una aplicación de software on-premise. El proveedor de servicio también suministra alternativas que proporcionan facturación unificada y rápido despliegue. SecureCloud 2 estará disponible a finales de año. Se puede adquirir por separado o como parte del pack Total Cloud Protection con Deep Security 8.

Parag Patel, Vicepresidente de Alianzas Estratégicas Globales de VMware, comenta: "Trend Micro y VMware han continuado colaborando para extender sus esfuerzos mutuos en el suministro de ofertas de seguridad innovadores a los clientes. El trabajo conjunto en las últimas mejoras incorporadas de VMware vSphere® y VMware vShield™, Trend Micro es capaz de proporcionar una amplia protección para entornos virtualizados, incrementar la eficiencia operativa y garantizar el cumplimiento normativo, dando a los clientes la confianza para seguir adelante en su camino hacia el cloud computing".

Trend Micro fue el primer anti-malware sin agente del mercado en entornos VMware. Este enfoque fue bien recibido por las compañías europeas, entre las que se incluyen Siemens Enterprise Communications, por su capacidad para facilitar la implementación y reducir costes.

En un nuevo caso de éxito de Trend Micro, Frank Semmler, Responsable de Soluciones de Gestión de Seguridad en Siemens Enterprise Communications, indica: "Nuestro objetivo para la implementación de soluciones de comunicación unificadas (UC) era proporcionar un alto estándar de seguridad a un coste razonable, pero está claro que no lo íbamos a lograr con el enfoque que teníamos. Pronto nos dimos cuenta de que la única solución disponible que cumplía con todos nuestros requerimientos era Deep Security de Trend Micro".

"Ahora que hemos estandarizado la oferta de seguridad para las soluciones de Comunicación Unificadas de Siemens Enterprise Communications, los clientes se benefician de un mayor nivel de seguridad a un coste significativamente menor comparado con la protección individual de virus que solíamos ofrecer",

Actualmente Deep Security protege 150.000 máquinas virtuales (VM) en EMEA.
