Trend Micro

HYBRID CLOUD SECURITY

Entornos físicos, virtuales, híbridos y de la nube seguros de manera fácil y eficaz

INTRODUCCIÓN

Mientras aprovecha las ventajas operativas y económicas de la virtualización y la nube, es fundamental proteger con eficacia sus centros de datos virtualizados, sus implementaciones de la nube y sus contenedores. Si desatiende cualquier aspecto de la seguridad, deja brechas que abren la puerta a amenazas e importantes filtraciones de datos. Y, para cumplir con las normativas de confidencialidad de datos y del sector, necesitará demostrar que cuenta con una seguridad apropiada, con independencia de su entorno informático.

La solución Hybrid Cloud Security de Trend Micro, con tecnología XGen™, protege las aplicaciones y los datos en su servidor, evita las interrupciones y facilita el cumplimiento normativo. Ya se centre en proteger servidores que ejecuten aplicaciones en entornos físicos y virtuales, o cargas de trabajo en la nube o en contenedores, Trend Micro ofrece la seguridad de servidor avanzado que necesita para proteger la nube híbrida a través de **Trend Micro**™ **Deep Security**™.

Trend Micro es el proveedor **n.º 1 de seguridad de servidores para entornos físicos, virtuales y en la nube,**[1] que combina el conjunto más completo de prestaciones de seguridad con gestión automatizada a fin de reducir de manera espectacular tanto los riesgos como los costes.

[1] IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, noviembre de 2016

¿Por qué Trend Micro para la seguridad en la nube híbrida?

- Protege entornos físicos, virtuales, en la nube y en contenedores con control y visibilidad centralizados
- Proporciona el conjunto más completo de prestaciones de seguridad disponibles del líder en cuota de mercado global en cuanto a seguridad de servidores
- Reduce el número de herramientas de seguridad necesarias para proteger su entorno híbrido y satisfacer los requisitos de cumplimiento
- Ahorra recursos y reduce los costes con una seguridad optimizada del entorno y políticas automatizadas
- Disponible como software, como servicio, o a través de los marketplaces de AWS y Microsoft Azure
- Con tecnología de seguridad XGen™, que ofrece un conjunto intergeneracional de controles de seguridad optimizados para entornos líderes

DEEP SECURITY

Al proporcionar varias técnicas de seguridad en un solo producto, Deep Security agiliza y facilita la implementación y la gestión de la seguridad, simplificando la transición de lo físico a lo virtual y a la nube. También incluye compatibilidad con arquitecturas de microservicios y protección de contenedores de anclajes, salvaguardando de manera sistemática la evolución de su centro de datos. Deep Security incluye gestión centralizada, detección automatizada de servidores y protección frente a vulnerabilidades para ahorrarle tiempo y recursos aprovechando la integración con entornos como VMware, AWS y Microsoft Azure optimizada para el máximo rendimiento sin poner en peligro la seguridad.

TREND MICRO HYBRID CLOUD SECURITY

SEGURIDAD DE VIRTUALIZACIÓN DE PROBADA EFICACIA

La solución Trend Micro Hybrid Cloud Security, con tecnología de XGen™, aporta protección y visibilidad a sus entornos virtualizados, incluido VMware Cloud™ en AWS, y elimina la complejidad y el riesgo de gestionar la seguridad a través de varios entornos. Incluye Deep Security, optimizada para el centro de datos virtualizado y que ayuda a los equipos de seguridad y de operaciones a maximizar la seguridad con impactos mínimos sobre el rendimiento. Reduce el riesgo y los costes operativos y brinda una rápida respuesta ante amenazas con una gestión automática de políticas, seguridad basada en hipervisor y control y visibilidad centralizados.

SEGURIDAD AUTOMATIZADA EN LA NUBE

Deep Security le ayuda a defender sus cargas de trabajo en la nube, al abordar la necesidad de proteger lo que se implementa EN la nube como parte de la responsabilidad compartida en cuanto a seguridad para este entorno. Proporciona seguridad elástica para cargas de trabajo dinámicas que se ejecuten en Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud y otras plataformas. Y para las organizaciones que se acojan a los microservicios con contenedores, Deep Security protege los contenedores de anclaje, extendiendo la protección de host sin fricción a través del propio contenedor y haciendo posible un modelo ágil de DevOps.

> “Yo mismo me encargué de implementar Deep Security; el despliegue en 100 máquinas virtuales me llevó menos de un día. De la noche a la mañana, vi como la utilización de nuestros recursos de memoria se redujo en un 27 %.”

Nick Casagrande
Responsable de TI
Southern Waste Systems LLC
Florida (EE. UU.)

SEGURIDAD PARA EL CENTRO DE DATOS MODERNO

La seguridad líder en el mercado de Trend Micro protege servidores y equipos de escritorio virtuales, cargas de trabajo en la nube, contenedores de anclaje y arquitecturas híbridas frente a malware de día cero, incluido ransomware, y amenazas avanzadas, a la vez que minimiza el impacto operativo sobre la seguridad y la aplicación de parches de emergencia.

Proporciona automáticamente prestaciones de seguridad completa en el centro de datos

Para ver las ventajas de la virtualización y ser eficiente, una solución de seguridad creada para entornos virtuales debe automatizarse como parte del proceso de aprovisionamiento del centro de datos. Trend Micro no solo garantiza la protección de servidores físicos y máquinas virtuales (VM) en el momento en que se aprovisionan; también recomienda y aplica únicamente las políticas pertinentes. Deep Security se adapta a entornos dinámicos con cargas de trabajo virtuales y en la nube siguiendo a las VM a medida que estas se ponen en marcha o se retiran y aplicando la seguridad apropiada.

Entre las prestaciones de Deep Security se incluyen:

- Prevención de malware con reputación de la web, machine learning preventivo e integración de análisis en recinto aislado para proteger frente a ataques de malware, incluidos ransomware y ataques como WannaCry y Erebus
- Seguridad en la red, incluida detección y prevención de intrusiones (IDS/IPS) para proteger frente a vulnerabilidades para las que no existe parche, así como un cortafuegos de inspección de estado que sirva de perímetro personalizable alrededor de cada servidor
- Seguridad del sistema, incluida supervisión de la integridad de sistemas y archivos con fines de cumplimiento, control de aplicaciones multiplataforma para bloqueo de servidores y prevención de ransomware, así como inspección de registros para identificar y documentar importantes sucesos de seguridad

Optimiza los recursos del centro de datos

El enfoque con el que Deep Security aborda la seguridad de la virtualización es mejor gracias a la integración en el nivel de hipervisor a través de VMware NSX. Al implementarse automáticamente sin periodos de inactividad, elimina la necesidad de instalar y gestionar un agente separado en cada VM. Esto también implica que los servidores y VM individuales no presentan un exceso de bibliotecas de firmas y motores de detección, lo que lleva a tremendas mejoras en la gestión, el uso de la red, la velocidad de los análisis, el uso de memoria y CPU en todo el host, operaciones de entrada/salida por segundo (IOPS) y uso global del almacenamiento.

Este enfoque centralizado permite el uso de una caché de exploración de malware altamente eficiente. La caché de exploración elimina la duplicación en la exploración a través de VM similares, lo que mejora el rendimiento de forma espectacular. Las exploraciones completas finalizan hasta 20 veces más rápido, el análisis en tiempo real hasta cinco veces más rápido, e incluso los inicios de sesión para VDI son más rápidos.

Para simplificar aún más el aprovisionamiento, las soluciones de Trend Micro aprovechan las últimas innovaciones en plataformas de VMware, como NSX y VMware Cloud en AWS. La integración de VMware NSX permite la protección automática de nuevas máquinas virtuales a medida que se ponen en marcha, a la vez que aprovisionan automáticamente las políticas de seguridad apropiadas y garantizan que no haya brechas de seguridad. Y nuestra integración exclusiva con vRealize Operations Management permite a las organizaciones contar con una vista única de operaciones de centros de datos y seguridad, racionalizando aún más cómo se gestiona la seguridad en un centro de datos virtual.

Gestiona la seguridad de manera eficiente, incluso durante la transición a nuevos entornos

La gestión de la seguridad es fácil gracias a un único panel que permite la supervisión continua de varios controles por los entornos físicos, virtuales y en la nube. Las sólidas funciones de generación de informes y alertas ayudan a concentrarse en lo importante para poder identificar rápidamente problemas y responder en consecuencia. La fácil integración con otros sistemas, como Security Information and Event Management (SIEM), ayuda a incorporar la gestión de seguridad como parte de otras operaciones de centros de datos. Y con la seguridad gestionada a través de un punto de integración central con NSX, no hay necesidad de mantener manualmente los agentes actualizados, una tarea especialmente difícil cuando se adaptan rápidamente las operaciones. El panel también incluye información de entornos en la nube como AWS, Microsoft Azure o Google Cloud, entre otros, lo que elimina las complicaciones de gestionar todos sus servidores, independientemente de su ubicación, desde una herramienta centralizada. Y con el respaldo de contenedores y arquitecturas de microservicios, puede hacer evolucionar con seguridad el modo en que funciona su centro de datos.

Optimizado para:

vmware®

amazon web services

Microsoft Azure

> “Deep Security ha encajado a las mil maravillas en nuestro centro de datos y proporciona una protección excelente para nuestros servidores y equipos de escritorio virtualizados, así como para nuestro entorno en continuo cambio. Me encanta.”

Orinzal Williams
Director ejecutivo
United Way of Atlanta
Georgia (EE. UU.)

SEGURIDAD AUTOMATIZADA PARA LA NUBE

La nube se está adoptando con gran rapidez, impulsada por los ahorros de costes, la agilidad y otras ventajas que ofrece. En su transición a la nube, el modelo de responsabilidad compartida en cuanto a la seguridad implica que usted debe proteger lo que pone EN la nube, y que su solución de seguridad debe obedecer a normas de cumplimiento interno y normativo.

Deep Security está optimizada para proveedores líderes de servicios en la nube (CSP), incluidos, entre otros AWS, Microsoft Azure o Google Cloud. Facilita la utilización de herramientas de orquestación como Chef, Puppet, SaltStack, Ansible y AWS Opworks, proporcionando ejemplos de implementación y generación automatizada de secuencias de comando de políticas que permiten la gestión de la seguridad como parte de las operaciones en la nube.

Evita filtraciones de datos e interrupciones en la empresa

Las prestaciones de seguridad líderes en el mercado de Trend Micro, por las que ya han optado miles de clientes globales para proteger millones de servidores, ayudan a las organizaciones a:

- Defenderse frente a amenazas de las aplicaciones y la red, aprovechando controles de seguridad de red de probada eficacia basados en host como la detección y la protección frente a intrusiones (IDS/IPS)
- Protegerse frente a vulnerabilidades, resguardando al instante aplicaciones y servidores vulnerables con un 'parche virtual' hasta poder sustituir una carga de trabajo
- Bloquear servidores para que solo pueden ejecutarse procesos autorizados con control de aplicaciones para Windows y Linux
- Mantener malware como ransomware lejos de las cargas de trabajo, garantizando la protección de servidores y aplicaciones
- Identificar cambios sospechosos en servidores, incluidas configuración de registros, carpetas de sistema y archivos de aplicación que no deberían cambiar

Reduce los costes operativos

Trend Micro proporciona seguridad avanzada de servidor para cargas de trabajo en la nube a la vez que gestiona simultáneamente la seguridad en servidores físicos y virtuales en el centro de datos.

La consola administrativa integrada ofrece una vista única y actualizada de la postura de seguridad para todo su entorno en la nube, reduciendo los costes de tiempo y recursos al hacer más eficiente la gestión de la seguridad. La protección automatizada frente a vulnerabilidades evita interrumpir la aplicación de parches de emergencia.

Además, la estrecha integración de Deep Security con AWS y Azure permite la detección de cargas de trabajo y la implementación de seguridad, incluidas plantillas de políticas personalizables que pueden aplicarse basándose en los metadatos de instancias, garantizando que se apliquen las políticas adecuadas a los servidores adecuados de forma automática.

ACELERE EL CUMPLIMIENTO EN TODA LA NUBE HÍBRIDA

El cumplimiento con importantes normativas como PCI DSS, HIPAA, NIST, SSAE-16 y GDPR abarca al centro de datos y la nube. Deep Security ayuda con:

- **Informes detallados y auditables** que documentan las vulnerabilidades evitadas, los ataques detectados y el estado de cumplimiento de las políticas
- **Menores tiempo y esfuerzo de preparación** necesarios para respaldar auditorías mediante controles centralizados de seguridad y generación consolidada de informes
- **Respaldo para iniciativas internas de cumplimiento** a fin de aumentar la visibilidad de la actividad de red interna
- **Tecnología de probada eficacia** certificada según Common Criteria EAL2

Para obtener más información sobre nuestras prestaciones de seguridad en la nube híbrida o realizar una prueba, visite trendmicro.com/hybridcloud

Disponible en awsmarketplace Microsoft Azure

La solución Trend Micro Hybrid Cloud Security, con tecnología XGen™, es un método de seguridad inteligente, optimizado y conectado.

POWERED BY XGen™ SECURITY

> "Las empresas se enfrentan a unas amenazas en Internet en continuo crecimiento y cambio. Al bloquear amenazas, Deep Security protege las experiencias en línea de nuestros clientes. Esto mantiene nuestra reputación y la de ellos."

Todd Redfoot
Responsable de seguridad de la información en Go Daddy

TREND MICRO™

Protegemos su transición a la nube