Trend Micro™

DEEP SECURITY™

Seguridad completa para entornos físicos, virtuales, híbridos y en la nube

La virtualización ya ha transformado los centros de datos y, ahora, las organizaciones están moviendo algunas de sus cargas de trabajo (o todas ellas) a nubes públicas y privadas. Si tiene interés en aprovechar las ventajas de la computación en la nube híbrida, tendrá que garantizar que dispone de seguridad creada para proteger todos sus servidores, ya sean físicos o virtuales, o se encuentren en la nube.

Además, la seguridad no debería poner trabas al rendimiento del host ni a la densidad de máquinas virtuales (VM), ni al retorno de inversión (ROI) de la virtualización y la computación en la nube. Trend Micro™ Deep Security™ proporciona seguridad exhaustiva en una solución creada a propósito para entornos virtualizados y en la nube de modo que no haya brechas en la seguridad ni se vea afectado el rendimiento.

Protección frente a filtraciones de datos e interrupciones en la empresa

Deep Security, disponible como software, como ofertas de Amazon Web Services (AWS) o Microsoft® Azure™ Marketplace, o como servicio, se ha diseñado para proteger su centro de datos y sus cargas de trabajo en la nube frente a filtraciones de datos e interrupciones en la empresa. Deep Security le ayuda a satisfacer los requisitos de cumplimiento al cerrar brechas en la protección de manera eficiente y económica en entornos de nube híbrida.

Varios controles de seguridad gestionados desde un solo panel

Deep Security cuenta con módulos de seguridad integrados, entre los que se incluyen antimalware, machine learning predictivo, reputación de la web, cortafuegos, prevención de intrusiones, supervisión de la integridad, control de aplicaciones e inspección de registros, para garantizar la seguridad de datos, aplicaciones y servidores en entornos virtuales, físicos y en la nube. Deep Security puede implementarse como un único agente multifunción a través de todos los entornos y simplifica las operaciones de seguridad con un único panel de gestión para todas las prestaciones. Puede usar Trend Micro Control Manager como panel, o un sistema de terceros como VMware vRealize Operations, Splunk, HP ArcSight o IBM QRadar.

La perfecta integración se extiende a políticas a través de entornos en la nube.

Deep Security se integra a la perfección con plataformas en la nube entre las que se incluyen cargas de trabajo de AWS, Azure y VMware®, lo que le permite extender las políticas de seguridad de los centros de datos a cargas de trabajo basadas en la nube. Con una amplia variedad de prestaciones optimizadas en distintos entornos, Deep Security permite a las empresas y a los proveedores de servicios ofrecer un entorno multipropiedad en la nube diferenciado y seguro para sus usuarios.

Principales problemas empresariales

Seguridad de los equipos de escritorio virtuales
Preserve los índices de consolidación y rendimiento con una seguridad exhaustiva creada específicamente para maximizar la protección en entornos de VDI

Aplicación virtual de parches
Proteja las vulnerabilidades antes de que puedan aprovecharse y elimine las molestias operativas de la aplicación de parches de emergencia, los ciclos frecuentes de parches y costosos periodos de inactividad del sistema

Cumplimiento
Demuestre el cumplimiento con diversos requisitos normativos como PCI DSS, HIPAA, NIST, SSAE 16, etc.

> "Deep Security también nos permitió eliminar otra solución antivirus en nuestros servidores... Una que había consumido una gran cantidad de memoria y generaba mucha agitación en la CPU debido a las exploraciones. No hemos tenido ninguno de esos problemas con Deep Security."

Blaine Isbelle
Administración de sistemas Tecnología de servicios de información Universidad de California en Berkeley

SEGURIDAD DE CONFIANZA DE LA NUBE HÍBRIDA

Seguridad de la virtualización

Deep Security protege servidores y equipos de escritorio virtuales frente a malware de día cero, incluido ransomware y ataques basados en red, a la vez que minimiza el impacto operativo de ineficiencias de recursos y aplicación de parches de emergencia.

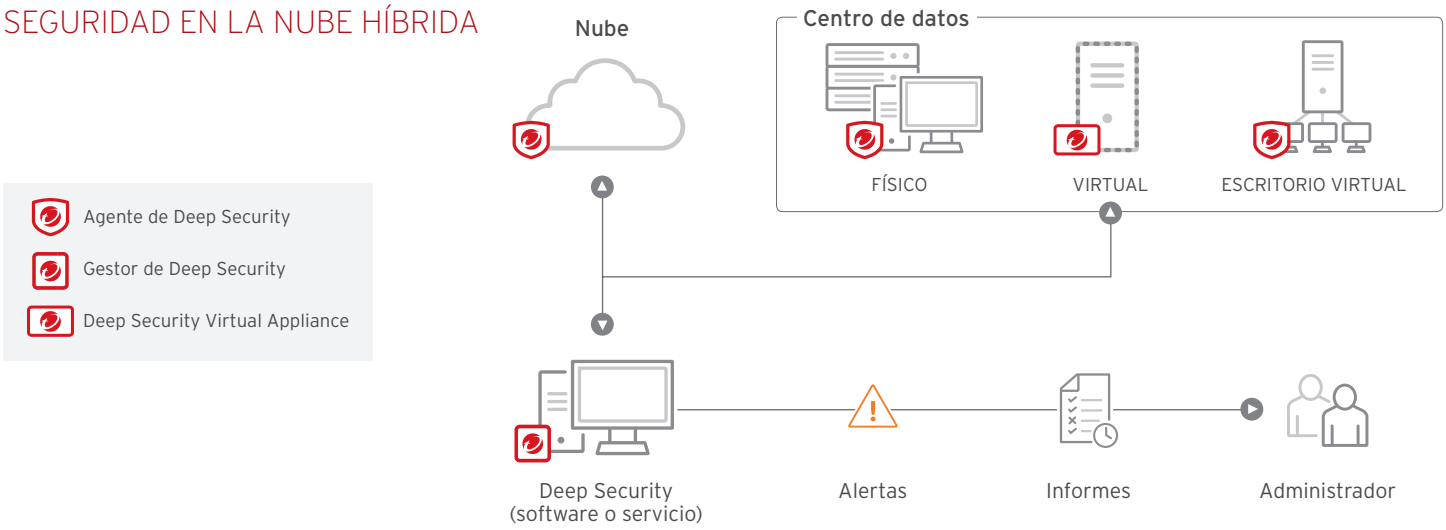
Seguridad en la nube

Deep Security permite a los proveedores de servicios y a los responsables de centros de datos modernos ofrecer un entorno multipropiedad seguro en la nube con políticas de seguridad que pueden extenderse a cargas de trabajo en la nube y gestionarse de forma centralizada con políticas sistemáticas y sensibles al contexto.

Seguridad de servidores integrada

Deep Security consolida todas las funciones de seguridad de servidor en una plataforma exhaustiva, integrada y flexible que optimiza la protección a través de entornos físicos, virtuales, de contenedores y en la nube.

SEGURIDAD EN LA NUBE HÍBRIDA



PRINCIPALES VENTAJAS

Eficacia y eficiencia

- Genera una utilización y gestión de recursos más eficiente con mayores densidades de VM que las soluciones tradicionales antimalware
- Añade prestaciones de flexibilidad y defensa en profundidad como un agente de seguridad multifunción único y fácil de gestionar
- Ofrece un rendimiento sin parangón gracias a la desduplicación de la exploración en el nivel de hipervisor
- Se integra con plataformas en la nube, incluidas AWS, Microsoft Azure y VMware Cloud, permitiendo a las organizaciones la gestión de sus servidores físicos, virtuales y en la nube con políticas de seguridad coherentes y sensibles al contexto
- Permite a los proveedores de servicios ofrecer a los clientes una nube pública segura, aislada de otros inquilinos a través de una arquitectura multipropiedad
- Proporciona adaptación automática, informática de utilidades y autoservicio para respaldar a organizaciones ágiles que hagan funcionar un centro de datos definido por software
- Aprovecha la estrecha integración de Deep Security con VMware para detectar automáticamente nuevas VM y aplicar políticas basadas en contexto para una seguridad sistemática a través del centro de datos y la nube
- Se integra con las últimas versiones de VMware vSphere y NSX™. Deep Security extiende las ventajas de la microsegmentación en el centro de datos definido por software con políticas y prestaciones de seguridad que sigan automáticamente a las VM, no importa a donde estas vayan

Evite filtraciones de datos e interrupciones en la empresa

- Evita que se ejecuten aplicaciones desconocidas en sus servidores más importantes
- Detecta y elimina malware de servidores virtuales en tiempo real con un mínimo impacto en el rendimiento
- Detecta y bloquea software no autorizado con control de aplicaciones multiplataforma
- Resguarda vulnerabilidades conocidas y desconocidas en aplicaciones y sistemas operativos de la web y empresariales
- Proporciona detección de amenazas avanzada y reparación de objetos sospechosos mediante el análisis en un recinto aislado
- Envía alertas y desencadena prevención proactiva tras detectar actividad sospechosa o malintencionada
- Rastrea la credibilidad del sitio web y protege a los usuarios frente a sitios infectados con inteligencia de reputación de la web frente a amenazas procedente de la base de datos de reputación de dominios global de Trend Micro
- Identifica y bloquea ataques de robots y ataques dirigidos a las comunicaciones de comandos y controles (C&C) mediante inteligencia unificada frente a amenazas de la base de datos de reputación de dominios global de Trend Micro

Reduzca al máximo los costes operativos

- Elimina el coste de implementar varios clientes de software con un dispositivo virtual o un agente de software multifunción gestionado centralmente
- Reduce la complejidad gracias a integraciones estrechas con consolas de gestión de Trend Micro, VMware y directorios empresariales como VMware vRealize Operations, Splunk, HP ArcSight e IBM QRadar
- Protege hosts y contenedores de anclaje con análisis antimalware y protección frente a intrusiones
- Reduce los costes de gestión al automatizar tareas de seguridad repetitivas y con gran consumo de recursos, reduciendo los falsos positivos en alertas de seguridad y permitiendo el flujo de trabajo de respuestas ante incidencias de seguridad
- Reduce significativamente la complejidad de gestionar la supervisión de la integridad de archivos con listas blancas de sucesos basados en la nube y sucesos de confianza
- Detecta vulnerabilidades y software a través de la exploración de recomendaciones para detectar cambios y proteger frente a vulnerabilidades
- Garantiza una mejor eficiencia operativa con un agente inteligente más ligero y dinámico que facilita la implementación para maximizar la asignación de recursos por el centro de datos y la nube
- Combina la seguridad con sus necesidades de políticas de manera que es preciso dedicar menos recursos a controles de seguridad específicos
- Simplifica la administración con la gestión centralizada a través de productos de seguridad de Trend Micro. La generación centralizada de informes de varios controles de seguridad reduce el reto de crear informes para productos individuales

Consiga un cumplimiento rentable

- Aborda los principales requisitos de cumplimiento para PCI DSS, así como HIPAA, SSAE 16 y otras normativas con una solución rentable e integrada
- Brinda informes de auditoría que documentan los ataques evitados y el estado de cumplimiento de las políticas
- Reduce el tiempo y el esfuerzo de preparación necesarios para respaldar auditorías
- Respalda iniciativas internas de cumplimiento a fin de aumentar la visibilidad de la actividad de red interna
- Aprovecha tecnología de probada eficacia certificada según Common Criteria EAL

PRESTACIONES DE DEEP SECURITY

Prevención de malware con supervisión del comportamiento y machine learning predictivo

- Integra API de VMware vShield Endpoint para proteger máquinas virtuales VMware frente a virus, spyware, troyanos, ransomware y otro malware
- Proporciona un agente antimalware para extender la protección a servidores físicos, virtuales y en la nube, incluidos entornos AWS, Microsoft y VMware
- Incluye mejor rendimiento a través de desduplicación y almacenamiento en caché sin agente de nivel VMware ESX
- Optimiza operaciones de seguridad para evitar tormentas de antivirus vistas habitualmente en exploraciones de sistema completo y actualizaciones de patrones de prestaciones de seguridad tradicionales
- Protege frente a ataques sofisticados en entornos virtuales aislando malware de componentes de seguridad y sistemas operativos críticos
- Utiliza tecnología avanzada de machine learning para correlacionar la información sobre amenazas y realizar un análisis de archivos en profundidad a fin de detectar riesgos de seguridad desconocidos emergentes
- Detecta actividad sospechosa o cambios no autorizados y brinda la capacidad de poner en cuarentena y recuperarse rápidamente
- Identifica y analiza objetos sospechosos a través del análisis en recinto aislado
- Se integra con la inteligencia frente a amenazas globales Trend Micro™ Smart Protection Network™ para ofrecer prestaciones de reputación de la web que refuercen la protección para servidores y equipos de escritorio virtuales

Inspección de registros

- Recopila y analiza registros de aplicaciones y de sistemas operativos en más de 100 formatos de archivos de registro, identificando comportamiento sospechoso, sucesos de seguridad y sucesos administrativos en todo el centro de datos
- Ayuda con el cumplimiento (PCI DSS sección 10.6) para optimizar la identificación de importantes sucesos de seguridad enterrados en múltiples entradas de registro
- Reenvía sucesos al sistema SIEM o al servidor de registro centralizado para las tareas de correlación, documentación y archivado

Prevención de intrusiones

- Examina todo el tráfico entrante y saliente en busca de desviaciones de protocolo, infracciones de políticas o contenido que haga sospechar de un ataque
- Protege automáticamente frente a vulnerabilidades conocidas pero sin parche al aplicar parches virtuales (resguardarlas) frente a distintos aprovechamientos de vulnerabilidades, insertando la protección en miles de servidores en cuestión de minutos sin necesidad de reiniciar el sistema
- Ayuda con el cumplimiento (PCI DSS sección 6.6) para proteger a las aplicaciones web y a los datos que procesan
- Defiende frente a ataques SQL injection, de secuencias de sitios cruzados y otras vulnerabilidades de aplicaciones web
- Incluye protección frente a vulnerabilidades desde el principio para todos los principales sistemas operativos y más de 100 aplicaciones, como bases de datos, web, correo electrónico y servidores FTP
- Proporciona una mayor visibilidad y control sobre aplicaciones que acceden a la red, incluidos conjuntos de reglas para bloquear software no deseado y evitar que se ejecute en un nivel de sistema

Cortafuegos basado en host bidireccional

- Disminuye la superficie de ataque de servidores físicos, virtuales y en la nube con filtrado preciso, políticas por red y la notificación de la ubicación para todos los protocolos basados en IP y tipos de tramas
- Gestiona de forma centralizada la política de cortafuegos del servidor, incluidas plantillas para tipos de servidor habituales
- Evita ataques de denegación de servicio y detecta exploraciones de reconocimiento
- Registra los sucesos de cortafuegos en el host, permitiendo el cumplimiento y la generación de informes de auditoría, especialmente críticos para implementaciones de la nube pública

Supervisión de la integridad

- Supervisa archivos de aplicaciones y sistemas operativos críticos, como directorios, claves de registro y valores, para detectar cambios maliciosos e imprevistos en tiempo real e informar de ellos
- Utiliza tecnología Intel TPM/TXT para supervisar la integridad de hipervisor en busca de cualquier cambio no autorizado en este, por tanto extendiendo la seguridad y el cumplimiento a la capa del hipervisor
- Reduce los gastos administrativos con etiquetado de sucesos de confianza que replica automáticamente acciones para eventos similares a través de todo el centro de datos
- Simplifica la administración reduciendo en gran medida el número de buenos sucesos conocidos mediante la inclusión automática en listas blancas basadas en la nube de Trend Micro™ Certified Safe Software Service

Control de aplicaciones multiplataforma

- Detecta y bloquea automáticamente software no autorizado en servidores Windows y Linux
- Analiza una máquina y determina qué aplicaciones hay actualmente en ella
- Bloquea el sistema una vez creado el inventario, evitando que nuevas aplicaciones se ejecuten sin estar permitidas
- Se integra en un entorno DevOps para respaldar cambios continuos a pilas de aplicaciones, a la vez que mantiene la protección del control de aplicaciones mediante API

ARQUITECTURA

Deep Security Virtual Appliance. Aplica de forma transparente políticas de seguridad en máquinas virtuales VMware vSphere. En el caso de entornos VMware NSX, esto proporciona antimalware sin agentes, reputación de la web, prevención de intrusiones, supervisión de la integridad y protección mediante cortafuegos. El modo combinado puede usarse donde se emplea el dispositivo virtual para la supervisión de integridad y antimalware sin agente y un agente para la prevención de intrusiones, el control de aplicaciones, cortafuegos, la reputación de la web y la inspección de registro.

Agente de Deep Security. Aplica la política de seguridad del centro de datos (control de aplicaciones, antimalware, prevención de intrusiones, cortafuegos, supervisión de la integridad e inspección de registros) mediante un pequeño componente de software implementado en el servidor o la máquina virtual que se estén protegiendo (puede implementarse automáticamente con herramientas de gestión operativa líderes como Chef, Puppet y AWS OpsWorks).

Gestor de Deep Security. Potente consola de gestión centralizada: la administración basada en funciones y la herencia de políticas multinivel permiten el control granular. Las funciones de automatización de tareas como la exploración de recomendaciones y el etiquetado de sucesos y tareas basadas en sucesos simplifican la administración de seguridad continua. La arquitectura multipropiedad permite el aislamiento de políticas de inquilinos individuales y la delegación de gestión de seguridad a administradores de inquilinos.

Información sobre amenazas global. Deep Security se integra con Smart Protection Network para proteger en tiempo real frente a amenazas emergentes al evaluar y correlacionar de forma continua inteligencia global de reputación y amenazas para sitios web, fuentes de correo electrónico y archivos.

Deep Security Scanner es un módulo que se integra con sistemas SAP y los protege al integrarse con los sistemas de interfaz NetWeaver Virus Scan.

SAP Partner

Certificación para proveedores de servicios en la nube

Trend Ready for Cloud Service Providers es un programa global de pruebas de validación diseñado para proveedores de servicios en la nube (CSP) a fin de probar la interoperabilidad con soluciones de seguridad en la nube líderes en el sector de Trend Micro.

IMPLEMENTACIÓN E INTEGRACIÓN

Rápida implementación: aproveche inversiones en seguridad y TI existentes

- El software de agente puede implementarse fácilmente a través de mecanismos estándar de distribución de software como Chef, Puppet, AWS OpsWorks, Microsoft System Center Configuration Manager (SCCM), Novell ZENworks y Symantec Deployment Solution
- Se proporcionan sucesos de seguridad detallados de nivel de servidor a un sistema SIEM, incluidos HP ArcSight, Intellitactics, IBM QRadar, NetIQ, RSA Envision, Q1Labs, Loglogic, Splunk, Sumologic y otros sistemas a través de múltiples opciones de integración
- La integración de directorios con directorios empresariales, incluido Microsoft Active Directory

Deep Security se ha desarrollado usando ágiles prácticas para la innovación y el desarrollo continuos. Nos enorgullece presentar los **lanzamientos de funciones**, que publican nuevas funciones a medida que están disponibles, antes de la próxima versión con funcionalidad completa. Esto le aporta la flexibilidad y la opción de aprovechar nuevas funciones a medida que se incorporan al producto, en lugar de esperar hasta la próxima versión con funcionalidad completa.

	VERSIÓN DE DEEP SECURITY		
Prestaciones y herramientas de seguridad	**10.0**	**Lanzamiento de funciones 10.1***	**Lanzamiento de funciones 10.2***
Control de aplicaciones	✓ Linux	✓ + Windows	✓
- Listas negras globales			✓
- Actualizaciones de confianza de Windows			✓
- Agregación de sucesos			✓
Prevención de intrusiones	✓	✓	✓
Prevención de malware	✓	✓	✓
- Supervisión del comportamiento	✓	✓	✓
- Machine Learning			✓
Reputación de la web	✓	✓	✓
Inspección de registros	✓	✓	✓
Supervisión de la integridad	✓	✓	✓
Compatibilidad con contenedores de anclaje	✓	✓	✓
Windows Server 2016	✓		✓
Compatibilidad con Deep Security Manager SQL 2016			✓
Compatibilidad con PostgreSQL		✓ (inquilino único)	✓ (implementaciones multipropiedad y multi-AZ)
Instalación de drivers de red con impacto cero		✓	✓
Inicio de sesión único con SAML 2.0		✓	✓
Canal de noticias en el producto		✓	✓
Asignación de reglas TippingPoint y Deep Security (IPS)			✓

*Los lanzamientos de funciones recibirán respaldo a lo largo de su disponibilidad durante seis meses tras la próxima versión importante de Deep Security.

REQUISITOS DEL SISTEMA

Microsoft® Windows®

- Windows XP, Vista, 7, 8, 8.1, 10 (32 bits/64 bits)
- Windows Server 2003 (32 bits/64 bits)
- Windows Server 2008 (32 bits/64 bits), 2008 R2, 2012, 2012 R2, 2012 Server Core (64 bits), 2016 (64 bits), 2016 Server Core (64 bits)
- XP Embedded (32 bits/64 bits)[1]

Linux[2]

- Red Hat® Enterprise 5, 6, 7 (32 bits/64 bits)[3]
- SUSE® Enterprise 10, 11, 12 (32 bits/64 bits)[3]
- CentOS 5, 6, 7 (32 bits/64 bits)[5]
- Ubuntu 12, 14, 16 (64 bits, solo LTS)[4, 5]
- Oracle Linux 5, 6, 7 (32 bits/64 bits)[4, 5]
- CloudLinux 5, 6, 7 (32 bits/64 bits)[2, 4]
- Amazon Linux (32 bits/64 bits)[4, 5]
- Debian 6, 7 (64 bits)[2, 4]

Oracle Solaris™ [6, 7]

- SO: 10, 11 (SPARC de 64 bits), 10, 11 (x86 de 64 bits)[7, 8]
- Oracle Exadata Database Machine, Oracle Exalogic Elastic Cloud y SPARC SuperCluster a través de los sistemas operativos de Solaris compatibles

UNIX[6]

- AIX 5.3, 6.1, 7.1 en IBM Power Systems[7, 8]
- HP-UX 11i v3 (11.31)[7, 9]

VIRTUAL

- VMware® vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3
- Citrix®: XenServer[11]
- Microsoft®: HyperV[11]

[1] Debido a la posibilidad de personalización con Windows XP Embedded, solicitamos que los clientes comprueben el correcto funcionamiento de sus propios entornos para verificar que los servicios y puertos necesarios para ejecutar el agente de Deep Security se han habilitado.
[2] Consulte la documentación para ver los núcleos compatibles
[3] Soporte de la protección de SAP solo en Red Hat 6 (64 bits) y SUSE 11 (64 bits) de agente. Para que la función de la protección de SAP funcione correctamente, el módulo antimalware debe estar habilitado en el agente.
[4] Soporte antimalware solo para exploración bajo demanda
[5] Consulte las notas más recientes para ver las versiones compatibles
[6] Supervisión antimalware y de reputación de la web no disponible
[7] Compatible a través de agentes 9.0
[8] Antimalware no disponible
[9] Solo inspección de registros y supervisión de la integridad
[10] vCloud Networking and Security permite una supervisión antimalware y de la integridad sin agente
[11] Protección solo mediante agente de Deep Security

CON TECNOLOGÍA DE SEGURIDAD XGEN™

Deep Security forma parte de la solución Trend Micro Hybrid Cloud Security, con tecnología de XGen™.

Principales certificaciones y alianzas

- Partner tecnológico avanzado de Amazon
- Certificación Red Hat Ready
- Validación para Cisco UCS
- Common Criteria EAL 2+
- Validación para EMC VSPEX
- Partner empresarial de HP
- Programa de protección de aplicaciones de Microsoft
- Partner certificado de Microsoft
- Validación para NetApp FlexPod
- Partner de Oracle
- Pruebas de idoneidad según la norma PCI para HIPS (NSS Labs)
- Certificación SAP (NW-VSI 2.0 y HANA)
- Validación para VCE Vblock
- Virtualización por VMware

Securing Your Journey to the Cloud