2020

Protección comprobada y organización sin fronteras para su nube híbrida

kaspersky

Obtenga más información en kaspersky.com
#truecybersecurity

Kaspersky Hybrid Cloud Security

La virtualización se ha convertido en una estrategia fundamental para cualquier empresa que intente ser flexible y eficiente. La computación en la nube es el siguiente paso lógico. Su trabajo consiste en compensar las limitaciones que implica sustentar una infraestructura compleja y proporciona un nivel de eficiencia que antes era inalcanzable. Pero la migración a la nube tiene sus peligros y complicaciones, algunos de ellos son nuevos y otros se preservan desde el mundo físico.

Kaspersky Hybrid Cloud Security ofrece seguridad unificada para cualquier etapa o escenario de su migración a la nube. Es adecuado tanto para la migración a la nube como para los escenarios de nubes nativas, protege sus cargas de trabajo físicas y virtualizadas, ya sea que se ejecuten en un entorno local, en un centro de datos o en una nube pública. Debido a que sus aplicaciones se crearon con las características específicas de la virtualización y el funcionamiento de los servidores, proporciona una protección perfectamente equilibrada contra las amenazas más avanzadas tanto actuales como futuras, sin comprometer el rendimiento del sistema.

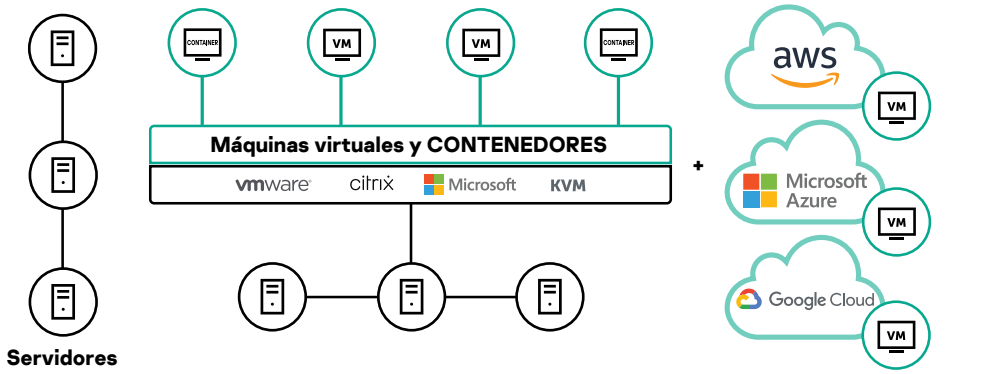
Principales desafíos para los usuarios de la nube:

- La creciente complejidad de la infraestructura puede ocasionar una reducción de la transparencia
- Un enfoque de varios niveles, es clave para una protección confiable, aunque esto rara vez se encuentra en un solo producto
- La seguridad tradicional que es verdaderamente importante consume valiosos recursos de los sistemas
- El enfoque de compartimentalización y los diversos controles traen consigo desafíos administrativos y de seguridad adicionales
- El malware y el ransomware atacan tanto los endpoints virtuales como los físicos
- No implementar las medidas de ciberseguridad adecuadas para la protección de los datos personales puede ocasionar problemas legales.

¿Por qué seleccionar Kaspersky Hybrid Cloud Security?

- Está diseñado para cargas de trabajo físicas, virtuales y de la nube
- Integra la seguridad en varios niveles para todo tipo de cargas de trabajo
- Proporciona una protección constante, automatizada y flexible para las nubes públicas de AWS, Azure y Google
- Ayuda a cumplir con la responsabilidad compartida mediante un conjunto completo de herramientas de seguridad
- Permite organizar la seguridad de manera eficiente en toda la nube híbrida
- Es la solución de seguridad con más experiencia y la que ofrece mayor protección, de acuerdo a numerosos reconocimientos y evaluaciones independientes[1]

Beneficios principales



Permite una migración segura hacia la nube, sin comprometer los niveles de protección

- Las tecnologías patentadas y nuestro reconocido motor de ciberseguridad protegen todas sus cargas de trabajo, ya sean físicas, virtualizadas o basadas en la nube.
- La protección en tiempo real de varios niveles, impulsada por el aprendizaje automático, protege sus datos, procesos y aplicaciones contra amenazas emergentes.
- Un enfoque holístico sobre la seguridad de los datos ayuda a reducir los riesgos legales y de reputación que están relacionados con las normas de protección de los datos.

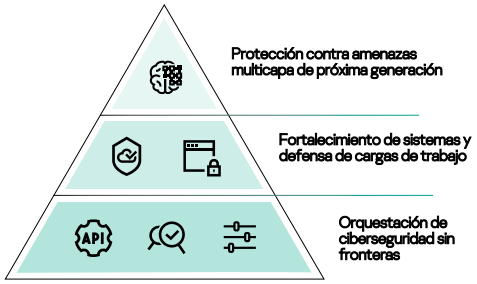
Garantiza que aproveche al máximo sus recursos e inversiones

- La protección ligera basada en agentes y sin agentes protege los activos virtualizados en redes normales y definidas por el software sin afectar su rendimiento.
- La integración con una protección nativa pública y administrada en la nube ayuda a proteger sus aplicaciones, sistemas operativos, flujos de datos y espacios de trabajo de los usuarios con el menor impacto en los recursos que es posible.
- La administración desde un solo punto de control de los recursos físicos y virtuales ahorra horas de trabajo durante el uso y el mantenimiento.

1. Las pruebas mencionadas cubren una amplia variedad de productos de Kaspersky, los cuales están basados en las mismas tecnologías de protección contra amenazas que se utilizan en Kaspersky Hybrid Cloud Security. Obtenga más información en kaspersky.com/top3.

Características

Características	Descripción
Varios niveles para la protección contra amenazas La protección contra malware de última generación de Kaspersky incorpora varios niveles de seguridad proactiva, los cuales son capaces de bloquear toda una amplia variedad de ciberataques que comprometan las cargas de trabajo más importantes de su empresa.	
Inteligencia contra amenazas global	Proporciona datos en tiempo real sobre el estado del panorama de amenazas, incluso cuando este cambia, lo que garantiza su protección en todo momento.
Aprendizaje automático	Las grandes bases de datos de la inteligencia contra amenazas globales se procesan mediante el poder combinado de los algoritmos de aprendizaje automático y la experiencia humana, para obtener altos niveles de detección con un mínimo de falsos positivos.
Protección contra amenazas web y en el correo electrónico	Permite que los equipos de escritorio virtuales y remotos funcionen de manera segura, ya que los protege de amenazas basadas en Internet y en el correo electrónico.
Inspección de registros	Escanea archivos de registro internos para llevar a cabo un proceso de limpieza óptimo.
Análisis del comportamiento	Supervisa las aplicaciones y los procesos, protegiéndolos contra amenazas avanzadas, incluidos malwares sin archivo o basados en scripts.
Motor de corrección	Revierte cualquier cambio malicioso que se haya realizado dentro de las cargas de trabajo en la nube, si es necesario.
Prevención de vulnerabilidades	Proporciona una protección eficaz contra los ataques dirigidos, mientras garantiza una compatibilidad perfecta con las aplicaciones que están protegidas, todo ello con un impacto mínimo en el rendimiento.
Funciones antiransomware	Protege las cargas de trabajo virtualizadas contra cualquier intento de retener los datos que son importantes para una empresa a cambio de un rescate, revierte los archivos afectados al estado que tenían antes del cifrado y bloquea el cifrado que se inició de forma remota.
Protección contra amenazas en la red	Detecta y previene intrusiones en la red de activos basados en la nube.
Protección para contenedores	Garantiza que las infecciones no se trasladen a su infraestructura de TI híbrida mediante los contenedores de Windows o Docker.
Fortalecimiento del sistema para aumentar la resiliencia	
Control de aplicaciones	Le permite bloquear todas las cargas de trabajo de la nube híbrida en el modo Denegación predeterminada para realizar un fortalecimiento óptimo del sistema, lo cual le permite limitar la variedad de aplicaciones que tenga en ejecución solo a las que sean legítimas y de confianza.
Control de dispositivos	Especifica cuáles son los dispositivos virtualizados que pueden acceder a las cargas de trabajo individuales en la nube.
Control web	Controla el uso de los recursos web que utilizan los equipos de escritorio virtuales y remotos para reducir los riesgos y aumentar la productividad.
Sistema de prevención contra intrusos basado en el host (HIPS)	Asigna categorías de confianza a las aplicaciones en ejecución, lo cual restringe su acceso a los recursos críticos y limita sus funciones.
Supervisión de la integridad de los archivos	Permite garantizar la integridad de los componentes críticos del sistema y de otros archivos importantes.
Administración de parches y evaluación de vulnerabilidades	Centraliza y automatiza las tareas de seguridad esenciales, así como la configuración y administración de los sistemas, por ejemplo, la evaluación de vulnerabilidades, la distribución de parches y actualizaciones, la administración de inventarios y la implementación de aplicaciones.
Visibilidad sin fronteras	
Administración unificada de la seguridad	Desde Kaspersky Security Center es mas sencillo administrar la seguridad desde un solo punto de control en toda la infraestructura, endpoints y servidores que se encuentran en la oficina, en su centro de datos y en la nube.
API en la nube	La integración perfecta con los entornos públicos de AWS y Azure permite el descubrimiento de infraestructuras, la implementación automatizada de agentes de seguridad y la administración basada en políticas, además de facilitar la creación de un registro y de proporcionar la seguridad.
Opciones de administración flexibles	Cuenta con funciones para múltiples usuarios, administración de cuentas basada en permisos y control de acceso basado en roles, lo cual brinda flexibilidad mientras se conservan todos los beneficios de que la organización esté unificada desde un solo servidor.
Integración SIEM	En infraestructuras con TI más consolidadas, la información sobre la seguridad y los sistemas de administración pueden utilizarse como una ventana unificada para los diferentes aspectos que implica la ciberseguridad de una empresa, con ayuda de toda la red híbrida de TI.



Seguridad unificada para cualquier nube:

Nubes públicas
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Centros de datos privados
- Vmware NSX
- Microsoft Hyper-V
- Citrix Hypervisor
- KVM
- Proxmox

Entornos VDI
- Vmware Horizon
- Citrix Virtual Apps and Desktops

Servidores físicos
- Windows
- Linux

Equipos de escritorio físicos:
- Windows
- Linux

aws

Microsoft Azure

vmware

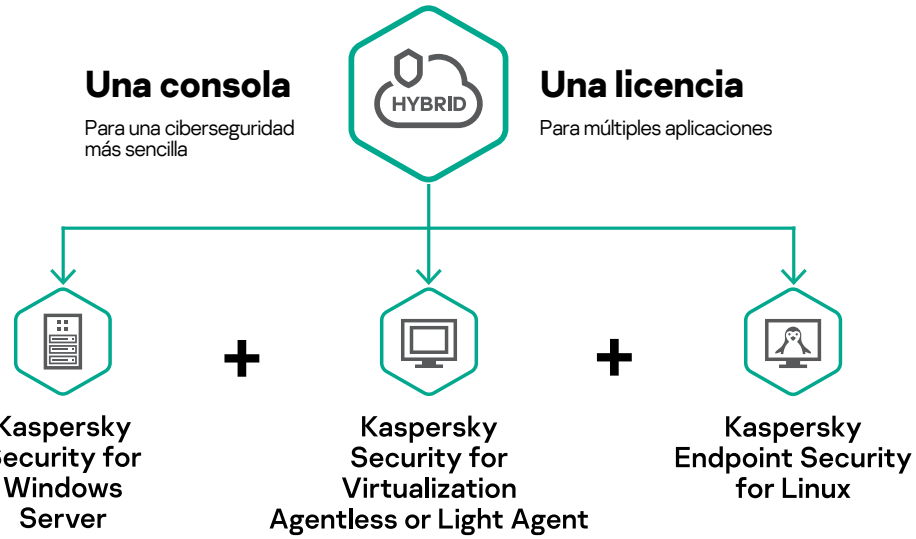
citrix

Google Cloud

KVM

Proporciona visibilidad y control constantes independientemente de la configuración que tenga en su infraestructura híbrida

- Facilita el suministro de servicios de seguridad y las operaciones basadas en políticas que estén habilitadas correctamente en toda la nube híbrida.
- Permite que tanto la administración como la organización de la seguridad funcionen sin problemas en varias nubes.
- Proporciona visibilidad completa, control y protección integral contra las amenazas más avanzadas para cada carga de trabajo, en cada ubicación.



Kaspersky Hybrid Cloud Security ofrece varias tecnologías de seguridad confiables y con amplio reconocimiento en la industria, las cuales le permitirán respaldar y simplificar la transformación en su entorno de TI. Esto protege su migración desde sistemas físicos a virtuales y a la nube, mientras que la visibilidad y la transparencia garantizan que pueda organizar su seguridad de una manera impecable.

Noticias sobre las amenazas cibernéticas: www.securelist.com
Noticias sobre la seguridad de TI: business.kaspersky.com
Ciberseguridad para PYMES: kaspersky.com/business
Ciberseguridad para empresas: kaspersky.com/enterprise

www.kaspersky.com

Tenemos experiencia. Somos independientes. Somos transparentes. Estamos comprometidos en desarrollar un mundo más seguro, donde la tecnología mejore nuestras vidas. Por eso lo protegemos, para que todos en cualquier parte disfruten las innumerables oportunidades que ofrece. Acceda a la ciberseguridad para vivir un mañana más seguro.

Obtenga más información en kaspersky.com/transparency

Proven. Transparent. Independent.