2020

Protección probada y orquestación sin límites para la nube híbrida

kaspersky

Obtenga más información en kaspersky.es
#truecybersecurity

Kaspersky Hybrid Cloud Security

La virtualización se ha convertido en un enfoque imprescindible para cualquier empresa que desea ser flexible y eficaz. La computación en nube es el siguiente paso. Ayuda a superar las limitaciones de la compatibilidad con infraestructuras complejas y ofrece un nivel de eficacia inalcanzable hasta ahora. Pero el viaje a la nube tiene peligros y complicaciones, tanto nuevos como heredados del mundo físico.

Kaspersky Hybrid Cloud Security ofrece seguridad unificada para cualquier fase o escenario de su migración a la nube. Adecuada tanto para la migración a la nube como para los escenarios de nube nativa, protege sus cargas de trabajo físicas y virtualizadas tanto si se ejecutan a nivel local, en un centro de datos o en una nube pública. Dado que sus aplicaciones se crearon con las características específicas de virtualización y funcionamiento del servidor en mente, ofrece una protección perfectamente equilibrada frente a las amenazas actuales y futuras más avanzadas, sin sacrificar el rendimiento del sistema.

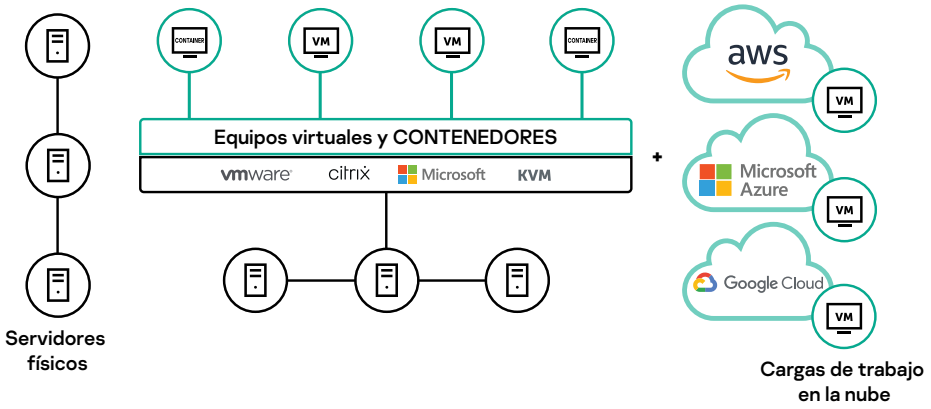
Principales desafíos de los usuarios de la nube:

- Un aumento de la complejidad de la infraestructura puede suponer un descenso de la transparencia
- Un enfoque a varios niveles, clave para una protección fiable, rara vez se encuentra en un único producto
- La pesada seguridad tradicional se alimenta de los preciados recursos de los sistemas
- Un enfoque compartimentado y los diferentes controles presentan desafíos administrativos y de seguridad
- El malware y el ransomware atacan terminales virtuales y físicos
- El incumplimiento de las medidas de ciberseguridad adecuadas para la protección de datos personales puede dar lugar a problemas legales.

¿Por qué Kaspersky Hybrid Cloud Security?

- Diseñada para cargas de trabajo físicas, virtuales y en la nube
- Seguridad a varios niveles integrada para todos los tipos de cargas de trabajo
- Seguridad coherente, automatizada y ágil para las nubes públicas AWS Azure y Google
- Conjunto completo de herramientas de seguridad que ayuda a cumplir los requisitos de responsabilidad compartida
- Organización fluida de la seguridad en toda la nube híbrida
- La protección más probada y más segura según numerosos premios y pruebas independientes[1]

Ventajas clave



Permite una migración a la nube segura, sin sacrificar los niveles de protección

- Las tecnologías patentadas y nuestro premiado motor de ciberseguridad protegen todas las cargas de trabajo: físicas, virtuales o basadas en la nube.
- Protección en tiempo real a varios niveles basada en el aprendizaje automático que protege los datos, procesos y aplicaciones frente a las amenazas emergentes.
- Un enfoque holístico para la seguridad de los datos ayuda a reducir los riesgos legales y de reputación relacionados con las normativas de protección de datos.

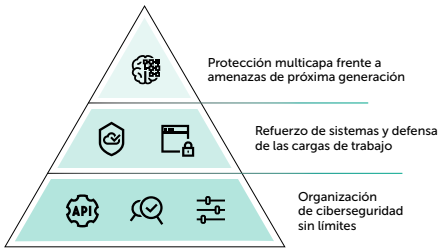
Garantiza que pueda aprovechar al máximo sus recursos e inversiones

- La protección sin agentes y basada en agentes ligeros mantiene la seguridad de los activos virtualizados en redes normales y definidas por software sin afectar al rendimiento.
- La integración con la seguridad en la nube nativa pública y gestionada ayuda a proteger las aplicaciones, los sistemas operativos, los flujos de datos y los espacios de trabajo de los usuarios con el menor número de recursos posible.
- La gestión desde un único punto de vista de los recursos físicos y virtuales ahorra horas de trabajo durante la adopción y el mantenimiento.

1 Las pruebas mencionadas cubren una amplia gama de productos de Kaspersky Lab basados en las mismas tecnologías de protección contra amenazas que utiliza Kaspersky Hybrid Cloud Security. Obtenga más información en kaspersky.com/top3

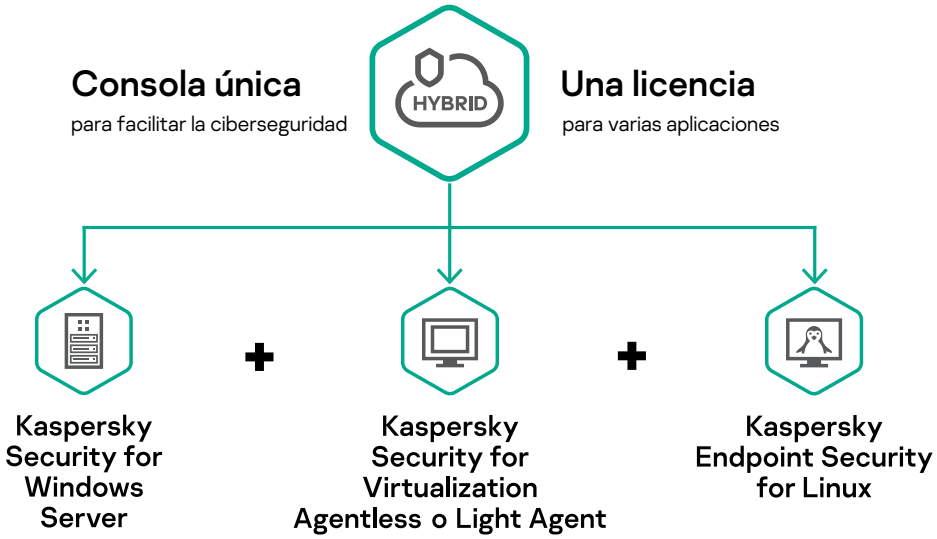
Características

Características	Descripción
Protección frente a amenazas a varios niveles La protección contra malware de próxima generación de Kaspersky Lab incorpora varios niveles de seguridad proactiva que pueden bloquear la gama más amplia de ciberataques que amenazan sus cargas de trabajo empresariales esenciales.	
Inteligencia global frente a amenazas	Proporciona datos en tiempo real sobre el estado del panorama de amenazas, incluso si cambia, para garantizar su protección en todo momento.
Aprendizaje automático	La información de inteligencia sobre amenazas global se procesa mediante algoritmos de aprendizaje automático y con supervisión humana, para ofrecer así unos altos niveles de detección probada, minimizando los falsos positivos.
Protección contra amenazas de correo electrónico y web	Permite el funcionamiento seguro de los equipos de escritorio virtuales y remotos, protegiéndolos frente a las amenazas del correo electrónico y basadas en la web.
Inspección de registros	Analiza los archivos de registro internos para una óptima higiene operativa.
Análisis del comportamiento	Supervisa las aplicaciones y los procesos, protegiendo así frente a amenazas avanzadas, incluido el malware basado en scripts o invisible.
Motor de corrección	Deshace cualquier cambio malicioso realizado dentro de las cargas de trabajo en la nube, si es necesario.
Prevención de exploits	Proporciona una protección eficaz contra el inicio de los ataques a la vez que garantiza una compatibilidad perfecta con aplicaciones protegidas, todo con un impacto mínimo en el rendimiento.
Protección antiransomware	Protege las cargas de trabajo virtualizadas contra cualquier intento de retener los datos empresariales esenciales a cambio de un rescate, la reversión de los archivos infectados a su estado previo al cifrado y el bloqueo del cifrado iniciado remotamente.
Protección contra amenazas de red	Detecta y previene las intrusiones basadas en la red en los activos basados en la nube.
Protección de contenedores	Asegura que las infecciones no se puedan transportar a su infraestructura híbrida de TI a través de contenedores comprometidos de Docker o Windows.
El refuerzo del sistema aumenta la resistencia	
Control de aplicaciones	Le permite bloquear todas sus cargas de trabajo en la nube híbrida en modo de denegación predeterminada para un refuerzo óptimo del sistema, lo que le permite limitar su gama de aplicaciones en ejecución solo a las de confianza y legítimas.
Control de dispositivos	Especifica qué dispositivos virtualizados pueden acceder a las cargas de trabajo en la nube individuales.
Control web	Regula el uso de los recursos web por parte de los equipos de escritorio virtuales y remotos para reducir los riesgos y aumentar la productividad.
Sistema de prevención de intrusiones basado en host (HIPS)	Asigna categorías de confianza a las aplicaciones iniciadas para restringir su acceso a los recursos esenciales y limitar sus funciones.
Supervisión de la integridad de archivos	Ayuda a garantizar la integridad de los componentes esenciales del sistema y otros archivos importantes.
Evaluación de las vulnerabilidades y gestión de parches	Centraliza y automatiza la seguridad esencial, la configuración del sistema y las tareas de gestión, como la evaluación de vulnerabilidades, la distribución de parches y actualizaciones, la gestión del inventario y las implementaciones de aplicaciones.
Visibilidad sin límites	
Gestión centralizada de la seguridad	La gestión centralizada de la seguridad de Kaspersky Security Center facilita la administración de seguridad de un solo punto de vista en todos los terminales, infraestructuras y servidores: en la oficina, en su centro de datos y en la nube.
API de la nube	La integración perfecta con los entornos públicos de AWS y Azure permite el descubrimiento de la infraestructura, la implementación del agente de seguridad automatizada y la gestión basada en políticas, además de facilitar la realización del inventario y el aprovisionamiento de seguridad.
Opciones de gestión flexibles	Incluyen funciones multiusuario, gestión de cuentas basada en permisos y control de acceso basado en funciones, lo que proporciona flexibilidad, a la vez que se mantienen los beneficios de una organización unificada desde un solo servidor.
Integración con SIEM	En infraestructuras con una TI más madura, los sistemas de información y gestión de la seguridad pueden utilizarse como una ventana unificada para diferentes aspectos de la ciberseguridad de una empresa en toda la red híbrida de TI.



Ofrece visibilidad y control transparentes, independientemente de la configuración de su infraestructura híbrida

- Facilita el aprovisionamiento de los servicios de seguridad y las operaciones basadas en políticas, que se habilitan en la nube híbrida.
- La capacidad de gestión y la organización de la seguridad funcionan perfectamente en varias nubes.
- Visibilidad completa, control y protección holística frente a las amenazas más avanzadas para cada trabajo y en cada ubicación.



Kaspersky Hybrid Cloud Security ofrece varias tecnologías de seguridad premiadas y reconocidas en el sector para respaldar y simplificar la transformación de su entorno de TI. Protege su migración del entorno físico al virtual y a la nube, mientras que la visibilidad y transparencia garantizan una organización perfecta de la seguridad.

Seguridad centralizada para cualquier nube:

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

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

Entornos de VDI
- Vmware Horizon
- Citrix Virtual Apps and Desktops

Servidores físicos
- Windows
- Linux

Escritorios físicos:
- Windows
- Linux

Noticias sobre ciberamenazas: www.securelist.es
Noticias de seguridad de ITI: business.kaspersky.es
Ciberseguridad para pymes: kaspersky.es/business
Ciberseguridad para empresas: kaspersky.es/enterprise

www.kaspersky.es

Seguridad probada. Somos una empresa independiente. Somos transparentes. Nos comprometemos a construir un mundo más seguro en el que la tecnología mejore nuestras vidas. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que ofrece la tecnología. Proteja su futuro gracias a la ciberseguridad.

Obtenga más información en kaspersky.es/transparency

Proven. Transparent. Independent.