Kaspersky® Hybrid Cloud Security

Protección probada y organización sin límites para su infraestructura híbrida

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 endpoints virtuales y físicos
- El incumplimiento de las medidas de ciberseguridad adecuadas para la protección de datos personales puede dar lugar a problemas legales

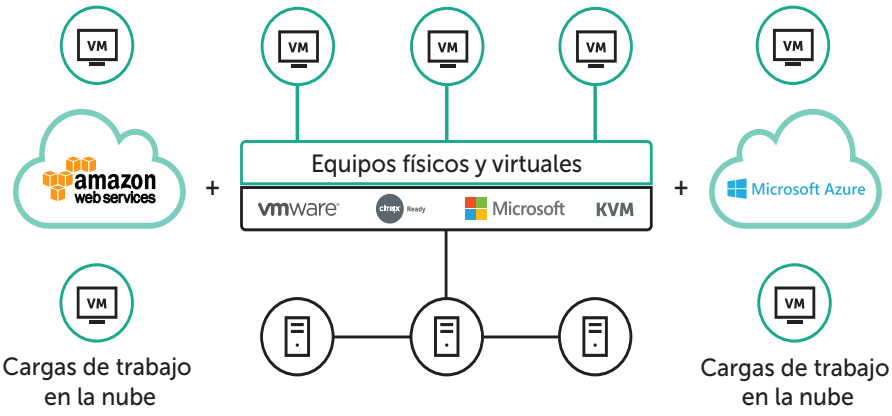
¿Por qué Kaspersky Hybrid Cloud Security?

- 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 y Azure
- 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]
- Basada en tecnologías que se han ganado la confianza y el reconocimiento de los clientes, incluido el premio Platinum Customer Award de Gartner Peer Insights

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.

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 "on-premise", 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 contra las amenazas actuales y futuras más avanzadas, sin sacrificar el rendimiento del sistema.



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.

Enfoque Kaspersky Humachine™

Sobre la base de la perfecta fusión de la inteligencia sobre amenazas del Big Data, las funciones de aprendizaje automático y la experiencia de expertos humanos, Kaspersky HuMachine™ proporciona varios beneficios y ofrece una protección eficaz. La combinación de cada elemento permite mejorar los componentes individuales en un conjunto aún más eficiente y eficaz.

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.

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

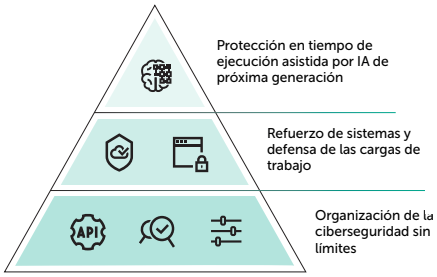
- La capacidad de gestión y la organización de la seguridad funcionan perfectamente en varias nubes.
- Visibilidad completa, control y protección holística contra las amenazas más avanzadas para cada trabajo y en cada ubicación.
- Facilita el aprovisionamiento de los servicios de seguridad y las operaciones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

Funcionalidades

Protección contra amenazas basada en HuMachine y 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.

- **La inteligencia sobre amenazas global** 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.
- **La protección contra amenazas web y de correo** permite el funcionamiento seguro de los equipos de escritorio virtuales y remotos, protegiéndolos de las amenazas del correo electrónico y basadas en la web.
- **La supervisión de la integridad de los archivos** ayuda a garantizar la integridad de los componentes esenciales del sistema y otros archivos importantes.
- **La inspección de registros** analiza los archivos de registro internos para una óptima higiene operativa.
- **El análisis del comportamiento** supervisa las aplicaciones y los procesos, protegiendo así contra amenazas avanzadas, incluido el malware basado en scripts o invisible.
- **El motor de corrección** deshace cualquier cambio malicioso realizado dentro de las cargas de trabajo en la nube, si es necesario.
- **La 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.
- **La funcionalidad 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.
- **La protección contra amenazas de red** detecta y previene las intrusiones basadas en la red en los activos basados en la nube.



Seguridad unificada para cualquier nube

Nubes públicas
- Amazon Web Services (AWS)
- Microsoft Azure

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

Entornos de VDI
- Vmware Horizon
- Citrix XenDesktop

Servidores físicos
- Windows
- Linux

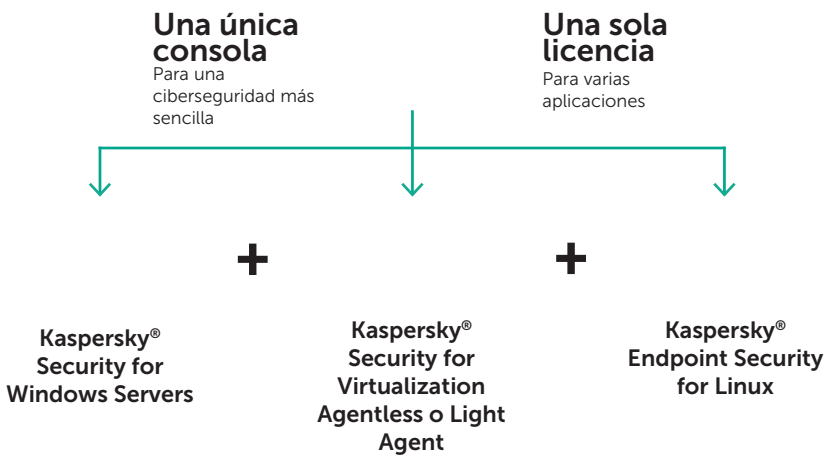
El refuerzo del sistema aumenta la resistencia

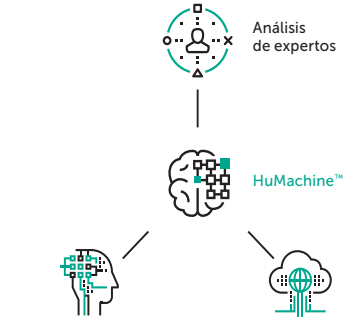
- **El control de aplicaciones** le permite bloquear todas sus cargas de trabajo en la nube híbrida en modo de denegación predeterminada para un refuerzo óptimo del sistema, lo que le permite limitar su gama de aplicaciones en ejecución solo a las de confianza y legítimas.
- **El control de dispositivos** especifica qué dispositivos virtualizados pueden acceder a las cargas de trabajo en la nube individuales.
- **El 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.
- **El 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.

Visibilidad sin límites

- **La gestión de la seguridad unificada** de Kaspersky Security Center facilita la administración de seguridad de un solo punto de vista en todos los endpoints, 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.
- **Las 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 IT 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 IT.

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 IT. 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.





Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Noticias de ciberamenazas: **https://securelist.es**
Noticias de seguridad de IT: **business.kaspersky.com/**
Nuestro enfoque exclusivo: **https://www.kaspersky.es/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.es