



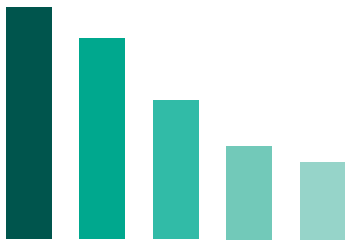
Kaspersky Hybrid Cloud Security

El enfoque empresarial actual en la transformación digital ha desencadenado una rápida adopción de la nube. Por un lado, estas iniciativas proporcionan muchas ventajas para las empresas, incluida una mayor eficiencia. Por otro lado, las infraestructuras se volvieron más complejas, lo que genera inquietudes significativas acerca de los riesgos de seguridad, la gobernanza, los recursos de persona, la optimización del rendimiento, las nuevas regulaciones y los gastos. Kaspersky Hybrid Cloud Security aborda todos estos desafíos.

Protección nativa de la nube y el mejor rendimiento para el entorno híbrido

Kaspersky Hybrid Cloud Security hace que la adopción de la nube, la transformación digital y los negocios en general sean más seguros y más eficientes. Este único producto asegura toda la infraestructura híbrida, lo que mitiga los riesgos, reduce el consumo de recursos de virtualización y es compatible con el cumplimiento normativo. Kaspersky Hybrid Cloud Security aumentó la visibilidad y simplificó la administración, además de ahorrarle a usted y a su equipo tiempo y recursos de presupuesto valiosos. La seguridad deja de ser algo de lo que preocuparse y tendrá más tiempo para enfocarse en otros aspectos de su recorrido de transformación digital.

Los desafíos de la nube



Seguridad	81%
Gestión del gasto en la nube	79 %
Gobernanza y cumplimiento	75 %
Gestión de nube múltiple	72 %
Migración a la nube	71 %

Según el informe Flexera State of the Cloud del 2021



La mejor protección en su clase, diseñada para abordar riesgos de seguridad de entornos híbridos

- Protección multicapa contra amenazas que combate de forma proactiva la gama más amplia de ciberataques, como el malware o el phishing, entre otros.
- Los algoritmos de aprendizaje automático impulsados por experiencia humana proporcionan los niveles más altos de detección con la cantidad mínima de falsos positivos.
- Los datos de inteligencia contra amenazas en tiempo real ayudan a defenderse de los exploits más recientes.



Un enfoque de nube nativa para el mejor rendimiento de seguridad de infraestructura híbrida

- El motor de ciberseguridad protege toda la infraestructura híbrida, sin importar la carga de trabajo: física, virtual o basada en nube privada, pública o híbrida.
- Un enfoque independiente de plataformas combinado con integraciones nativas permite que las nubes públicas cuenten con DevOps habilitados.
- Light Agent optimizado para cada SO reduce de forma eficaz el consumo de los recursos de virtualización de hasta el 30 % y así se liberan para utilizarlos en otras operaciones empresariales.



Administración conveniente y rentable para una transición hacia la nube más cómoda

- Un modelo de licencias flexible implica que solo debe elegir las capacidades que necesita, de modo que obtenga el mayor valor de su inversión en seguridad.
- Una consola en la nube unificada hace que la administración de seguridad de toda la infraestructura sea más simple, ya que ahorra en valiosos recursos de personal de TI.
- Tanto el inventario de infraestructura en la nube directo como el aprovisionamiento de seguridad automatizada sin importar la ubicación de los agentes contribuyen a la máxima visibilidad.



Seguridad lista para el cumplimiento de industrias con altos niveles de regulación

- Adaptativo y multifacético, este producto está diseñado para permitir y compatibilizar de forma continua el cumplimiento normativo completo, mediante tecnologías que van desde el fortalecimiento de sistemas y autodefensa de los agentes hasta asesorías de vulnerabilidad y administración de parches automatizada.
- La amplia gama de funciones proporciona adaptación al panorama de riesgos y cumplimiento, lo que mantiene la seguridad un paso adelante de las leyes actuales de forma continua.

Características



Protección frente a amenazas a varios niveles

Inteligencia global frente a amenazas	Recopila datos en tiempo real sobre el estado del panorama de amenazas, incluso cuando este cambia.
Aprendizaje automático	Potencia los macrodatos de inteligencia contra amenazas global con algoritmos de aprendizaje automático y experiencia humana.
Protección contra amenazas de correo electrónico y web	Asegura los escritorios virtuales y remotos, ya que los protege de amenazas basadas en el correo electrónico y la web.
Inspección de registros	Analiza los archivos de registro para una higiene operativa óptima.
Análisis del comportamiento	Protege contra amenazas avanzadas, incluidos los malware sin cuerpo y basados en scripts, mediante el monitoreo de procesos y aplicaciones.
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 las amenazas de penetración en total compatibilidad con las aplicaciones protegidas, lo que resulta en un impacto mínimo al rendimiento.
Funcionalidad antiransomware	Protege los datos empresariales críticos de cualquier intento de retención, incluido bloquear de forma remota el encriptado iniciado y volver a un estado previo a la encriptación los archivos afectados.
Protección contra amenazas de red	Detecta y previene las intrusiones basadas en la red en los activos basados en la nube.
Protección de contenedores	Previene infecciones provenientes del transporte a la infraestructura híbrida de TI debido a contenedores infectados.



El refuerzo del sistema aumenta la resistencia

Control de aplicaciones	Permite bloquear todas las cargas de trabajo de la nube híbrida en el modo de denegación predeterminada para un fortalecimiento óptimo del sistema, lo que permite limitar la gama de aplicaciones en ejecución solo a las legítimas y de confianza.
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 unificada de la seguridad	La protección de servidor y de endpoint para toda la infraestructura se puede administrar a través de una consola, en la oficina, en el centro de datos y en la nube.
API de la nube	la integración perfecta con los entornos públicos 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	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	Permite integrar el producto en el sistema de información y administración de seguridad, lo que reúne en un solo lugar distintos aspectos de la ciberseguridad corporativa, en toda la red de TI híbrida.

¿Por qué Kaspersky Hybrid Cloud Security?

30 %

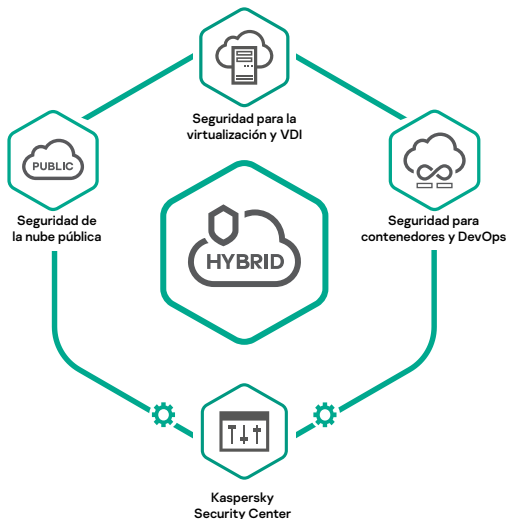
ahorros potenciales en recursos de hardware de virtualización comparados con el uso de soluciones de seguridad de endpoints tradicionales.

TRES PRIMEROS PUESTOS

rendimiento excelente sostenido. El año pasado, los productos Kaspersky nuevamente alcanzaron estándares de rendimiento excelentes en varias pruebas independientes, consiguieron 57 premios de primer lugar y 63 resultados en los mejores tres (obtenga más información en kaspersky.com/top3).



Un producto para todas sus necesidades de seguridad de la nube



Opiniones de los clientes

"Esta solución ayuda a proteger los entornos virtuales y de nube sin afectar el rendimiento del sistema ni interrumpir la experiencia del usuario".

"Es una excelente manera de combinar todas las soluciones de seguridad en una sola licencia".

"No hay necesidad de instalar software antivirus y otros agentes adicionales".

"Solución de nube centralizada para la protección de datos. En un solo lugar".

"La protección se aplica al instante en todas las MV, ya que no se necesita descargar nuevas actualizaciones en absoluto".

"La solución óptima que no requiere largas capacitaciones de administración".

Ejemplos de reseñas de Amazon y Gartner

Solicitar una demostración

