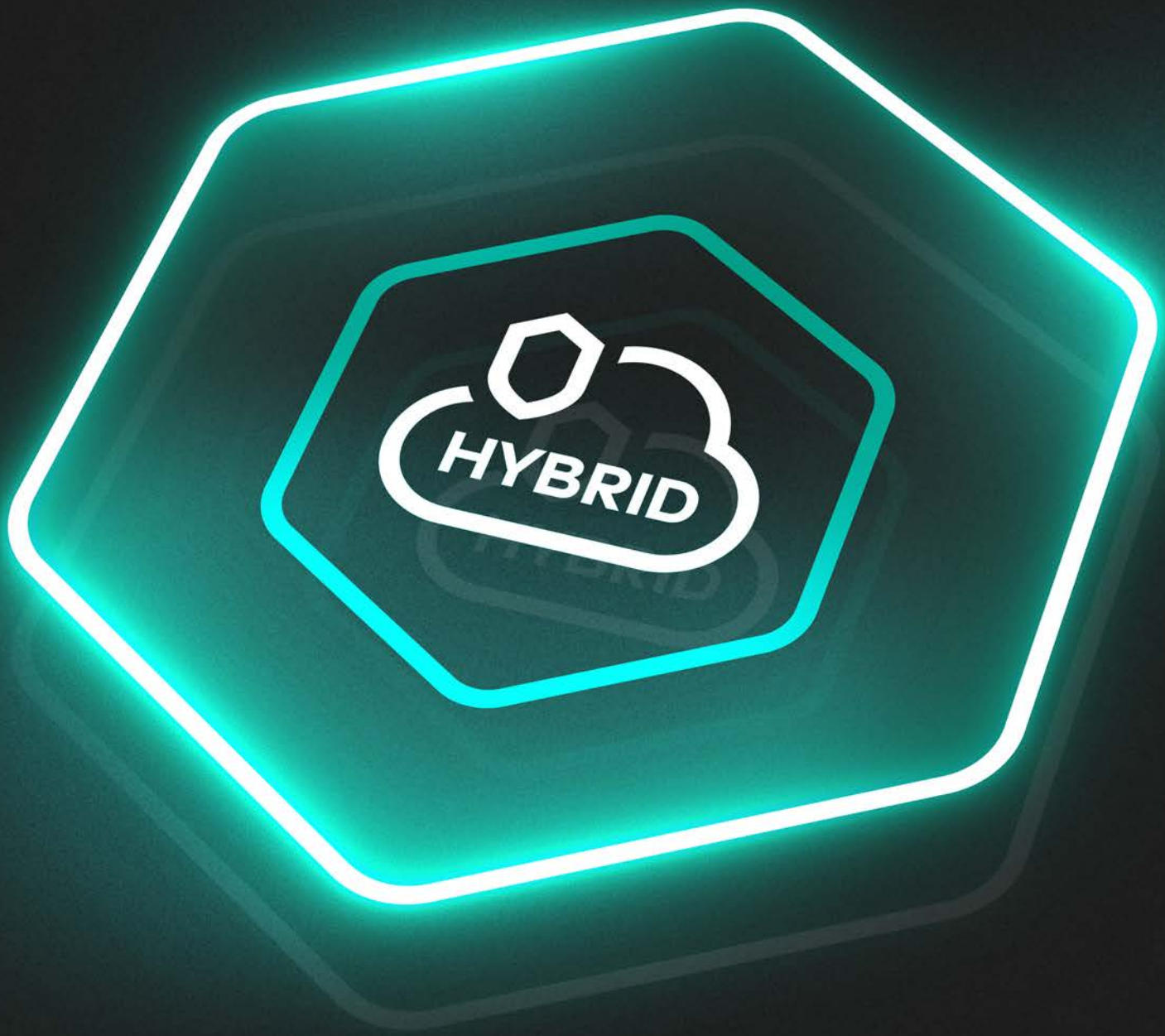


Kaspersky Hybrid Cloud Security

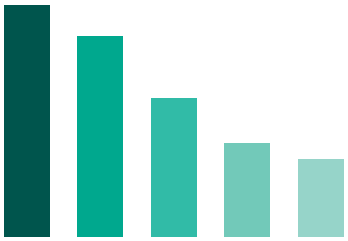
kaspersky PREPARADOS PARA EL FUTURO

El enfoque actual en la transformación digital de las empresas activó 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 en términos de riesgo de la seguridad, control, recursos de personal, optimización del rendimiento, nuevas regulaciones y gastos. Kaspersky Hybrid Cloud Security aborda todos estos desafíos.

Protección nativa de nube comprobada y el mejor rendimiento para los entornos híbridos

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 solo producto asegura toda la infraestructura híbrida, lo que mitiga los riesgos, reduce el consumo de recursos de virtualización y cumple con la normativa. 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 una preocupación y usted tendrá más tiempo para enfocarse en otros aspectos de su recorrido de transformación digital.

Principales desafíos en la nube



- Seguridad **81 %**
- Gasto de administración de la nube **79 %**
- Control y cumplimiento **75 %**
- Administración de varias nubes **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, incluidos el malware, el phishing y mucho más.
- Los algoritmos de aprendizaje automático optimizados con conocimiento humano proporcionan los niveles más altos de detección con la cantidad mínima de falsos positivos.
- Los datos de inteligencia contra amenazas en tiempo real permiten defenderse de los exploits más recientes.

Un enfoque nativo de nube para lograr el mejor rendimiento de seguridad de infraestructuras híbridas

- 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 multiplataforma combinado con integración nativa habilita completamente las nubes públicas para DevOps.
- Los agentes ligeros, optimizados para cada SO, reducen de forma eficaz el consumo de los recursos de virtualización en hasta un 30 %, lo que permite utilizarlos en otras operaciones empresariales.

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

- Un modelo de licencias flexible le permite elegir solo las capacidades que necesita, de modo que obtenga el mayor valor de su inversión en seguridad.
- Una consola de nube unificada logra que la administración de seguridad de toda la infraestructura sea más simple, ya que ahorra 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 que cumple con la normativa para industrias con altos niveles de regulación

- Este producto, adaptativo y multifacético, está diseñado para permitir y cumplir de forma continua con toda la normativa mediante tecnologías que van desde el fortalecimiento del sistema y la autodefensa de los agentes hasta la evaluación de vulnerabilidades y la administración automatizada de parches.
- La amplia gama de funciones proporciona el cumplimiento normativo y la adaptación al panorama de riesgos, lo que mantiene la seguridad continuamente actualizada conforme a la legislación vigente.

Características

Protección de varias capas contra amenazas

Global Threat Intelligence	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 globales con algoritmos de aprendizaje automático y conocimiento humano.
Protección contra las amenazas de Internet y de correos electrónicos	Asegura los escritorios virtuales y remotos, ya que los protege de amenazas en correos electrónicos y en Internet.
Inspección de registros	Analiza los archivos de registro para contar con una depuración operativa óptima.
Análisis de comportamiento	Protege contra amenazas avanzadas, incluidos los malware sin cuerpo y basados en scripts, mediante el monitoreo de procesos y aplicaciones.
Motor de corrección	Revierte cualquier cambio malicioso hecho dentro de las cargas de trabajo de la nube, si es necesario.
Prevención de exploits	Proporciona una protección eficaz contra la penetración de amenazas en total compatibilidad con las aplicaciones protegidas, lo que genera un impacto mínimo en el rendimiento.
Funcionalidad antiransomware	Protege los datos empresariales esenciales de cualquier intento de retención, incluido bloquear el cifrado iniciado de forma remota y volver a un estado previo al cifrado de 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 mediante contenedores infectados.

Fortalecimiento del sistema que aumenta la resistencia

Control de aplicaciones	Permite bloquear todas las cargas de trabajo de la nube híbrida en el modo de denegación predeterminada para lograr 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 escritorios virtuales y remotos, lo que reduce los riesgos y aumenta la productividad.
Sistema de prevención de intrusiones basada en host (HIPS)	Asigna categorías de confianza a las aplicaciones iniciadas, lo que restringe su acceso a recursos esenciales y limita sus capacidades.
Monitoreo de integridad de los archivos	Ayuda a asegurar la integridad de los componentes críticos del sistema y otros archivos importantes.
Evaluación de las vulnerabilidades y administración de parches	Centraliza y automatiza las tareas esenciales en materia de seguridad, configuración del sistema y administración, como la evaluación de vulnerabilidades, la distribución de parches y actualizaciones, la administración del inventario y la implementación de las aplicaciones.

Visibilidad sin restricciones

Administración de seguridad unificada	La protección de servidores y endpoints 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 perfecta integración en entornos públicos permite el descubrimiento de infraestructuras, la implementación automatizada de agentes de seguridad y la administración basada en directivas, así como un inventario y aprovisionamiento de seguridad más fáciles.
Opciones de administración flexibles	Las capacidades multiempresa, la administración de cuentas basada en permisos y el control de acceso basado en roles proporcionan flexibilidad y conservan los beneficios de la organización unificada desde un solo servidor.
Integración en 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 elegir Kaspersky Hybrid Cloud Security?

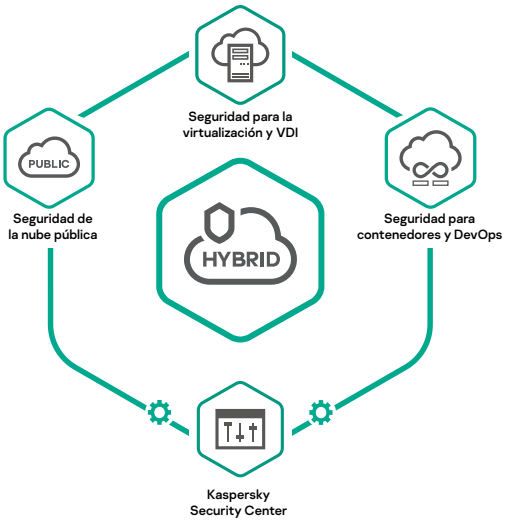
El 30 %

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

TOP 3

en rendimiento excelente sostenido. El año pasado, los productos Kaspersky nuevamente alcanzaron estándares de rendimiento excelentes en varias pruebas independientes y consiguieron 57 primeros lugares 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



Contenedores

Nubes públicas

Equipos físicos y virtuales

Un producto | Una consola | Una licencia

Opiniones de clientes

"Esta solución permite proteger los entornos virtuales y en la 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 adicionales ni otros agentes".

"Solución de nube centralizada para la protección de datos. Todo en un lugar".

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

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

Proveniente de reseñas de Amazon y Gartner

Solicite una demostración

latam.kaspersky.com