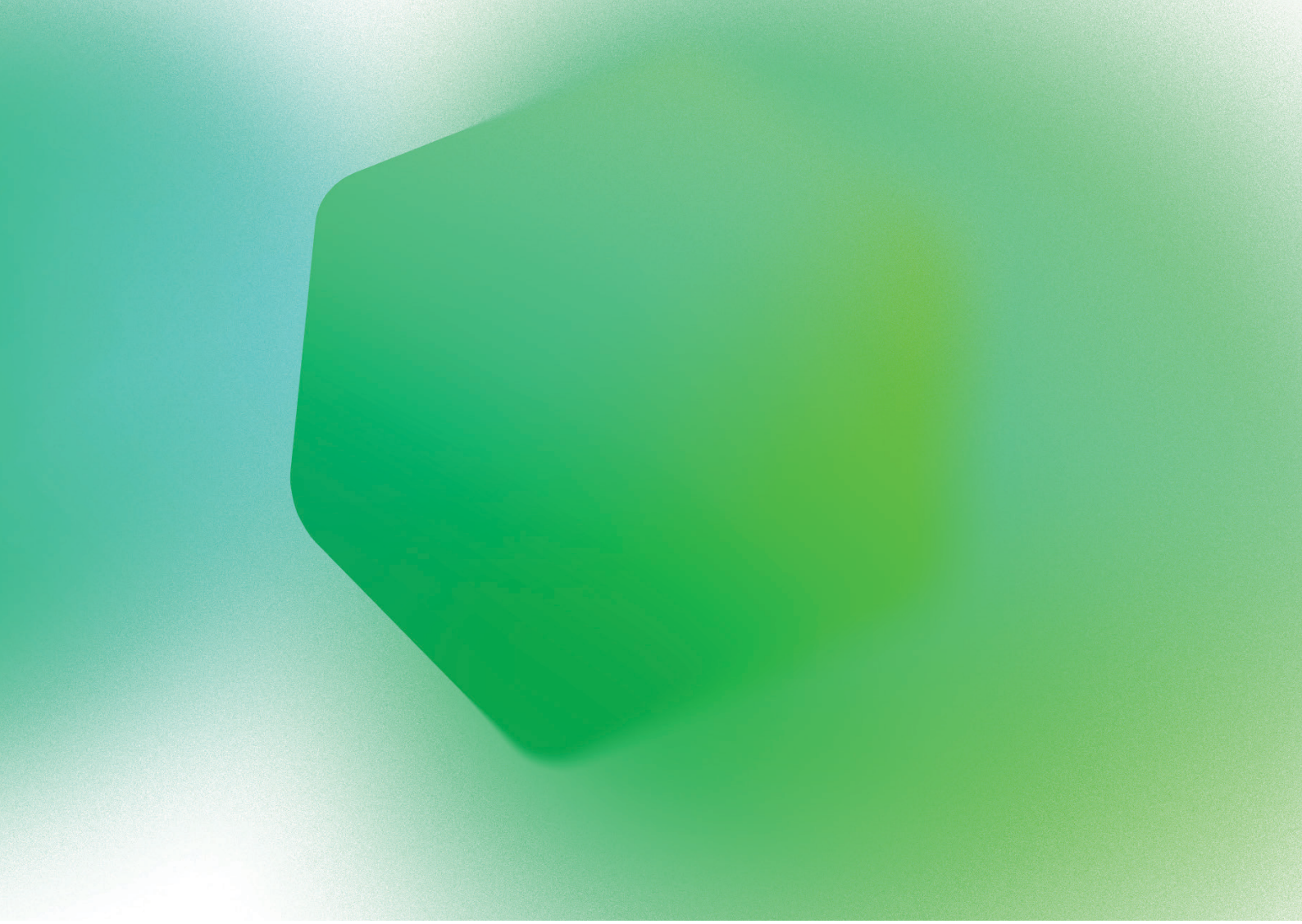


Toda la protección que necesita al pasarse a la nube

kaspersky

Obtenga más información en latam.kaspersky.com

La transformación digital está cambiando las características esenciales de la TI corporativa

Cuando las empresas van adoptando la transformación digital y van creando sus infraestructuras en la nube, deben enfrentarse a algunas luchas muy reales. ¿Podrá mantener el control de sus activos corporativos o se le arrebatará de las manos? ¿Cómo se cerrarán las brechas de integración y se eliminarán los límites para que pueda cosechar los beneficios del traslado? ¿Cómo puede minimizar el impacto en el rendimiento durante estos cambios y, al mismo tiempo, estar seguro de que está maximizando el retorno de su inversión sustancial?

La transformación digital adopta muchas formas. Crear nuevas funciones de TI desde cero en la nube. Migrar servidores o aplicaciones existentes. Facilitar la retirada del hardware antiguo al pasarse a la nube. Permitir la escalada automática del servicio, permitir el cambio rápido de los estilos de trabajo, y así sucesivamente.

El traslado a la nube: más relevante que nunca en este momento

La realidad es que solo hemos comenzado a ver la punta del iceberg de lo que puede significar la adopción de la nube para todos nosotros.

Durante la pandemia del coronavirus desencadenada en 2020 y el resultante cambio masivo al trabajo remoto, los proveedores de la nube pública han sido capaces de satisfacer la demanda sin esfuerzo aparente, acelerando los nodos a una velocidad vertiginosa. Trabajar desde casa también ha demostrado (como si no lo supiéramos ya) cuánto dependen todos los aspectos de la vida corporativa del acceso y las comunicaciones online ininterrumpidos, y la facilidad (o no) con la que podemos gestionar nuestras infraestructuras sin acceso físico a la capa de hardware. Las empresas que ya habían llevado a cabo la adopción de la nube han visto realmente los beneficios de este traslado durante esta última crisis, y los proveedores de la nube fueron aclamados como "héroes anónimos".[1]

Otra tecnología que ha experimentado un gran aumento de uso instantáneo durante la pandemia es la infraestructura de escritorio virtual (VDI, del inglés "Virtual Desktop Infrastructures"). Muchas empresas se han dado cuenta de que son incapaces de proporcionar por sí mismas los portátiles y ordenadores necesarios a fin de ofrecer a todos los empleados el equipo necesario para trabajar de forma remota, y han tenido que solicitar a sus empleados que trabajen desde sus propios dispositivos. Aquellos que se han adaptado y han implementado la tecnología VDI han podido operar de manera segura y controlada, a la vez que han permitido que sus empleados trabajen desde una amplia variedad de dispositivos. La tecnología VDI también ofrece una gran variedad de opciones de copia de seguridad en caso de que un dispositivo deje de funcionar: el trabajo se puede reanudar casi instantáneamente desde cualquier otro dispositivo disponible.

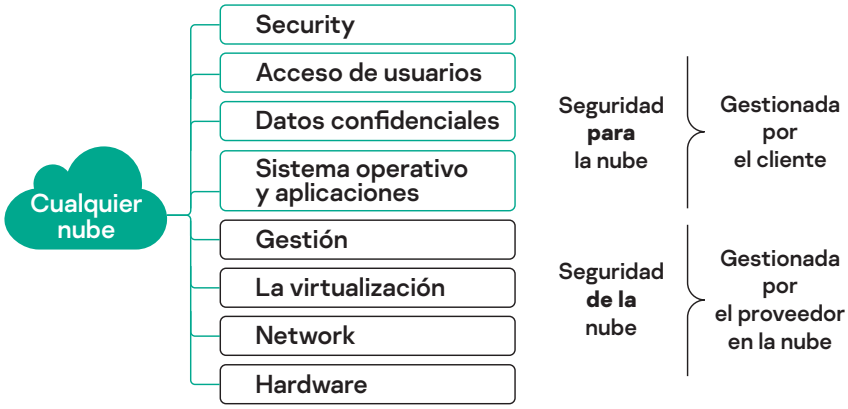
Debido a que el trabajo basado en la nube ha demostrado proporcionar beneficios claros en términos de continuidad y resiliencia del negocio durante los momentos más difíciles, es casi inevitable que la gran mayoría de las empresas pasen a la nube en algún momento futuro. Y el proceso de evolución con la nube y hacia ella probablemente dará lugar a una etapa intermedia en la que trabajaremos con una compleja infraestructura híbrida heterogénea que abarca plataformas físicas, virtuales y en la nube, las cuales se deben gestionar, ajustar y respaldar, todo al mismo tiempo.

Su infraestructura de repente no está en su red

Hubo un momento en el que, como nuestros propios creadores y propietarios de redes, podíamos ejecutar una herramienta de detección que creara un inventario de nuestras estaciones de trabajo, servidores, servicios y aplicaciones. Y esto era relativamente fácil de hacer, porque teníamos control sobre nuestra propia red. Podíamos rastrear un cable. Podíamos profundizar en la configuración del hipervisor para averiguar el alcance de nuestra red definida por software.

En el mundo de la Infraestructura como Servicio (IaaS, del inglés "Infrastructure as a Service"), ya no disponemos de ese lujo, y esto es algo bueno. Podemos relajarnos, la capa de hardware ya no es nuestra responsabilidad. Ahora depende del proveedor de IaaS.

Responsabilidad compartida en materia de seguridad



1 https://www.crn.com/news/cloud/in-coronavirus-crisis-public-cloud-is-an-unsung-hero-

Ahora que ya no tenemos esa responsabilidad, el control y, por desgracia, la visibilidad también han desaparecido. La antigua manera de hacer las cosas todavía es posible: puede unir varias partes de las infraestructuras y tratar sus activos de TI en la nube de la misma manera que trata sus cargas de trabajo virtualizadas. Pero lo más importante es que, con más frecuencia de lo deseado, en realidad no le interesa trabajar de esta forma, porque cada vez que elige la manera antigua en lugar de la nueva, también está rechazando los beneficios del nuevo enfoque.

Nuevas herramientas para nuevas realidades

Y he aquí un dilema. Las herramientas antiguas no funcionan bien con infraestructuras híbridas. Además, las herramientas nuevas se centran en los aspectos de migración, y con demasiada frecuencia abordan la seguridad de la carga de trabajo como un problema posterior a la migración. La única opción que tenemos a nuestra disposición la mayoría de nosotros es el uso de diferentes herramientas de seguridad para las diferentes partes de la infraestructura. El resultado es la expansión de dominios de responsabilidad, brechas de visibilidad, fallos de control y, finalmente, esas brechas de seguridad que los cibercriminales tanto aman.

Para impulsar la evolución digital, las herramientas que utiliza necesitan cambiar y adaptarse a las nuevas realidades, así como funcionar de manera útil en numerosas plataformas independientemente de donde se encuentren estas, ya sea en las instalaciones, físicas o virtualizadas, o "en la nube", un término al que nos hemos acostumbrado, pero que para la mayoría de las personas aún significa "en el ordenador de otra persona".

Visibilidad coherente de todas las cargas de trabajo

En Kaspersky pensamos en las brechas de seguridad casi tanto como en las amenazas que las utilizan. No hay duda de que la incapacidad para controlar, aplicar políticas y garantizar la uniformidad de la configuración en toda su infraestructura es un peligro mayor que una vulnerabilidad en su sistema operativo o aplicación de la línea de negocios. El proveedor de software o el proveedor de seguridad pueden corregir las vulnerabilidades en el software. Pero ¿quién va a detectar una diferencia en la configuración de varias consolas de gestión de la seguridad que ha creado un punto de entrada cómodo para un atacante interesado?

Creemos que una consola de gestión de "panel único" se ocupa de este problema de mejor manera. Cuando puede controlar a la perfección la seguridad de todos los elementos físicos, virtualizados, móviles y en la nube de su entorno, las posibilidades de que se produzcan errores humanos que creen una brecha de seguridad son mucho menores.

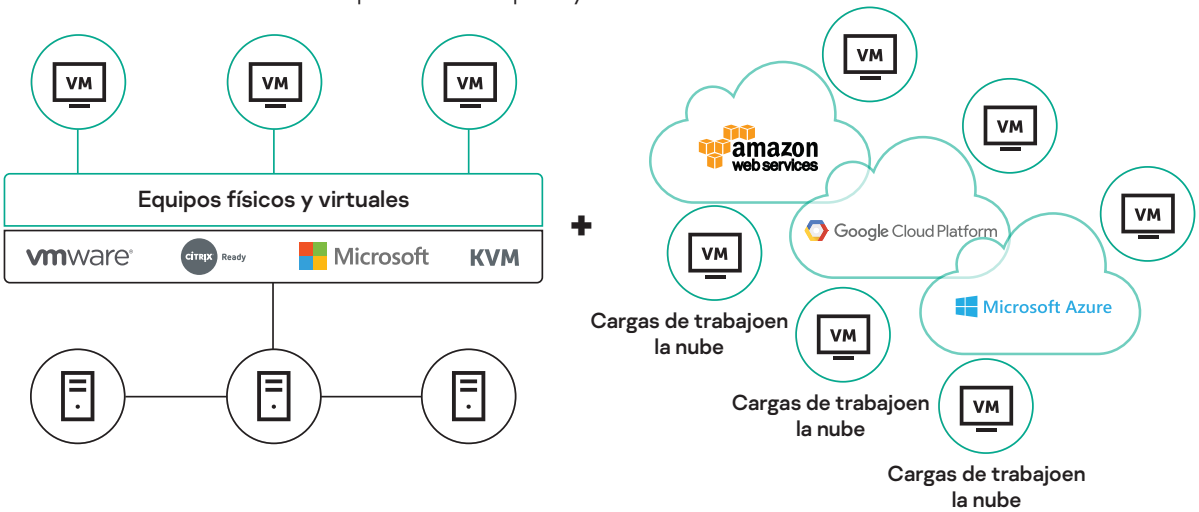
Seguridad generalizada para empresas híbridas complejas

Kaspersky Hybrid Cloud Security protege las infraestructuras de TI híbridas, ya que ofrece una visibilidad coherente a través de "un panel único" y centraliza el control en las cargas de trabajo basadas en la nube, en la infraestructura virtualizada y en los equipos físicos, además de en cada etapa de su proceso de transición, entre muchos otros elementos. Seguirá manteniendo el cumplimiento absoluto en todo momento, y el rendimiento de los sistemas no se verá afectado. Una única consola de gestión con políticas unificadas reduce el tiempo de gestión y la complejidad, y ayuda a cerrar todas esas brechas de seguridad importantes.

Nubes públicas: visibilidad y comodidad

Kaspersky Hybrid Cloud Security simplifica la organización de las implementaciones de nube pública a través de aspectos como los siguientes:

- Una consola de gestión de panel único que se puede implementar en cualquier número de subinfraestructuras y organizar en una jerarquía de servidores de gestión para abarcar incluso las implementaciones más complejas, sin brechas.
- Integración de API nativa con las plataformas AWS, Microsoft Azure y Google Cloud.
- Protección para cargas de trabajo en Windows y Linux.
- Un inventario de infraestructura de nube muy sencillo y aprovisionamiento automatizado de la seguridad de agentes de seguridad, independientemente de su ubicación.
- Un modelo de consumo flexible:
  - Pago por uso (PPU, del inglés "Pay-Per-Use"), que permite la adquisición y facturación de los servicios de seguridad directamente a través del mercado del proveedor de nube.
  - Contratos anuales con cumplimiento de SaaS disponibles en plataformas seleccionadas.
  - Modelo BYOL ("Bring Your Own License", uso de su propia licencia): la solución puede activarse con una licencia obtenida de un partner de Kaspersky.



Detección e implantación automáticas

La integración con las API de la nube proporciona automatización y flexibilidad administrativa. La consola de gestión debe ser capaz de ver todas las instancias que se ejecutan en las cuentas especificadas, y utilizar esa información para implementar agentes de seguridad y aplicar políticas de seguridad a las mismas. Cuando se crea una nueva instancia, se puede utilizar una función de gestión de identidad y acceso (IAM, del inglés "Identity and Access Management") o un mecanismo de implementación de script para garantizar que la instancia esté completamente protegida en el momento en que se crea.

Compatibilidad con grupos de escalada automática

La capacidad de configuración flexible de Kaspersky Hybrid Cloud Security se traduce en que la solución puede responder automáticamente a la carga en aumento a medida que la nube crea y ejecuta nuevas instancias. Las políticas de API y de escalada automática garantizan que cada nueva instancia en cada grupo de escalada automática tenga implementada la seguridad y cumpla con la política establecida por la organización.

Seguridad de los contenedores

Uno de los casos de uso importantes para la nube pública es la habilitación de DevOps. Sin embargo, la adopción y el amplio uso (a menudo controlado vagamente) de tecnologías de contenedores, como Docker, crean un desafío persistente para los responsables de la seguridad. Kaspersky Hybrid Cloud Security protege los contenedores de Docker and Windows para evitar que un atacante utilice un componente de contenedor malicioso como trampolín al interior de la organización. La protección de la memoria del host de creación de contenedores, las tareas para el análisis de contenedores e imágenes, y las interfaces que permiten ejecutar scripts, permiten aplicar el enfoque de "seguridad como código", con la capacidad de integrar tareas de seguridad en los flujos de procesos de CI/CD.

Virtualización: equilibrio entre seguridad y eficacia en el centro de datos

Aunque las nubes públicas pueden estar cambiando las características esenciales de la TI, la virtualización en las instalaciones y las nubes privadas han llegado para quedarse. La gestión del riesgo corporativo implica proteger cada máquina virtual (VM, del inglés "Virtual Machine") y almacenamiento de virtualización, pero, aunque los objetivos de seguridad para las nubes públicas y privadas son los mismos (reducir y gestionar el ciberriesgo), los desafíos a los que se enfrentan son diferentes.

En el caso de la virtualización, todo gira en torno a sacar el máximo partido de sus recursos de hardware en las instalaciones, con los que se puede lograr mucho más que con las máquinas físicas. Por lo tanto, los beneficios del rendimiento de la inversión en virtualización deben asegurarse mediante la aplicación de la seguridad adecuada diseñada específicamente para proteger los entornos virtuales. La seguridad eficaz de la virtualización debe encontrar maneras de centralizar las tareas de seguridad, reutilizar la información disponible y eliminar la redundancia, equilibrar la carga entre las máquinas virtuales y utilizar las posibilidades que proporcionan las plataformas de virtualización para maximizar la protección con el menor impacto posible en el rendimiento.

Protección para servidores virtualizados y la VDI

Diseñado y creado específicamente para usarse en entornos virtualizados y eliminar todas las operaciones y datos superfluos, Kaspersky Hybrid Security permite ahorrar hasta un 30 % de recursos de hardware de virtualización en comparación con el uso de una solución de seguridad de endpoints tradicional. Después de conocer el entorno, a menudo la solución es capaz de producir instantáneamente un veredicto, sin desperdiciar ni un solo ciclo adicional. La funcionalidad de consolidación de los sistemas, rica y flexible, reduce drásticamente la superficie de ataque, evita la ejecución de código arbitrario en servidores y bloquea exploits, todo ello sin un aumento notable del consumo de recursos.

En el caso de los escritorios virtuales, el tiempo de inicio de sesión se reduce drásticamente en comparación con las soluciones de seguridad de endpoints tradicionales al tiempo que elimina los cortes y los puntos de estrangulamiento al escalar y superar los límites del host de virtualización. Con el mismo conjunto de funciones de seguridad amplias que nuestras soluciones para endpoints físicos, Kaspersky Hybrid Cloud Security crea un entorno de usuario seguro y con capacidad de respuesta, lo que permite a los usuarios centrarse en su trabajo sin riesgo de convertirse en víctima de malware sin archivos, ransomware, exploits y similares. Kaspersky Hybrid Cloud Security dispone de varias opciones de implementación para satisfacer mejor las necesidades de los clientes en términos de complejidad de la implementación, integración y compatibilidad de las plataformas, optimización del uso de los recursos, conjuntos de funciones y, en última instancia, el nivel de seguridad.

Seguridad sin agentes

VMware cuenta con una API que permite una seguridad "sin agentes" en el nivel de archivos para su plataforma de virtualización vSphere, y permite que Kaspersky Hybrid Cloud Security se integre de manera nativa con el ecosistema VMware, además de vShield Endpoint y NSX Guest Introspection, a la vez que protege de forma perfecta y al instante todos los activos virtualizados. Para eliminar la gestión de las máquinas virtuales individuales y reducir en gran medida el consumo de recursos, lo único que se necesita por host es una máquina virtual de seguridad (SVM), es decir, una máquina virtual especializada que incorpora un motor de análisis antimalware y bases de datos de firmas.

Seguridad con agente ligero

Otro enfoque, adoptado por la aplicación de "agente ligero" también disponible en Kaspersky Hybrid Cloud Security, es el uso de una solución independiente de la plataforma que utilice un agente ligero optimizado para funcionar en el sistema operativo de cada máquina virtual protegida. La tecnología de agente ligero tiene un impacto mucho menor en los recursos que una solución de agente completo tradicional gracias a la gestión centralizada del motor de análisis de archivos y las bases de datos en la SVM. La solución se sitúa entre los sistemas tradicionales de agente completo y "sin agentes" en términos de consumo de recursos, pero no está ligada o limitada por tecnologías de VMware; además, se puede usar en plataformas populares como Microsoft Hyper-V, Citrix Hypervisor y KVM para proporcionar un nivel bastante más alto de seguridad.

Estos enfoques permiten la implementación eficaz de la virtualización segura y resuelven los problemas siguientes:

- Consumo de recursos excesivo. Mediante la centralización de la mayoría de las tareas de seguridad, el uso de una sola instancia de una base de datos y el almacenamiento en caché de los veredictos, podemos evitar replicar las bases de datos de firmas y los motores antimalware activos en cada máquina virtual protegida.
- "Tormentas". Con las colas inteligentes, el equilibrio de la carga y el almacenamiento en caché de los veredictos en la máquina virtual de seguridad, podemos eliminar las tormentas ocasionadas por las actualizaciones simultáneas de la base de datos o los procesos de análisis antimalware en cada máquina virtual, así como ver y evitar el riesgo de las "ventanas de vulnerabilidades" causadas por los retrasos en el análisis.
- "Brechas de seguridad instantáneas". Las bases de datos y los módulos no se pueden actualizar en las máquinas virtuales inactivas. De este modo, desde el momento del arranque de la máquina virtual hasta que finaliza el proceso de actualización, la máquina virtual es vulnerable a los ataques. Esto se resuelve con el uso de una máquina virtual de seguridad que siempre está encendida y siempre está actualizada.

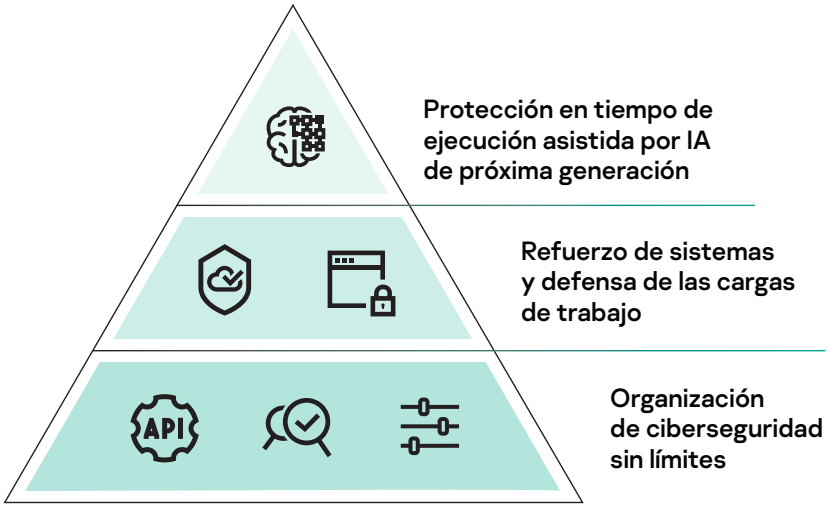
Máquinas físicas y dispositivos móviles

Los servidores físicos y, más importantes aún, las estaciones de trabajo físicas y los dispositivos móviles, también necesitan seguridad; esta es la función de otra solución de Kaspersky: Kaspersky Endpoint Security for Business. La combinación de varias capas de protección y control con las herramientas de automatización de procesos de seguridad se traduce en que el estado de seguridad de cada estación de trabajo, portátil, tablet o teléfono móvil es totalmente visible y está bajo su control absoluto como parte de su infraestructura híbrida más amplia, y todo está arropado por la protección de Kaspersky, galardonada y la mejor de su categoría.

La mejor protección de su categoría

La misma regla se aplica si su seguridad se ejecuta en un teléfono móvil, un servidor físico, una máquina virtual o en la nube: debe estar a la altura del trabajo que debe desempeñar.

Esta protección, la mejor de su categoría, es el núcleo de todos los productos y servicios de Kaspersky. Nuestras tecnologías se basan en recursos inigualables de inteligencia frente a amenazas y aprendizaje automático en tiempo real. Además, están en constante evolución para proteger sus endpoints de las vulnerabilidades más recientes, lo que le permite mantener sus datos y carpetas compartidas seguros frente a las amenazas y el ransomware más avanzados.



Hybrid Cloud Security se basa en el mismo conjunto de funciones inigualables, ya sea para proteger endpoints, cargas de trabajo o servidores tanto físicos como virtuales en las nubes públicas. Entre ellas:

- **Nuestro galardonado motor antimalware** proporciona protección automática y en tiempo real en el nivel de archivos a cualquier ordenador, máquina virtual y carga de trabajo, por acceso y a petición.
- **La inteligencia con asistencia en la nube** identifica rápidamente nuevas amenazas y proporciona actualizaciones automáticas.
- **La detección de comportamiento** supervisa aplicaciones y procesos, protege frente a las amenazas avanzadas e incluso el malware invisible, y revierte cualquier cambio malicioso si es necesario.
- **La prevención de exploits** controla los procesos operativos de los sistemas y el comportamiento de las aplicaciones, lo que ayuda a bloquear las amenazas avanzadas y el ransomware.
- **La protección antiransomware** protege las cargas de trabajo en la nube, los endpoints virtuales y físicos, y las redes compartidas contra ataques, y revierte los archivos afectados a su estado cifrado previo.
- **HIPS/HIDS** detecta y previene las intrusiones basadas en la red en los activos físicos y basados en la nube.
- **Los controles de aplicaciones** le permiten bloquear todas sus cargas de trabajo en la nube híbrida en el modo de denegación predeterminada para un refuerzo óptimo de los sistemas, además de establecer qué aplicaciones se pueden ejecutar en qué lugar y a qué pueden acceder.
- **El control web** ofrece protección contra las ciberamenazas basadas en Internet y aquellas que se aprovechan de la ignorancia o los errores de los empleados, además de impulsar la productividad mediante la reducción del tiempo que se pierde en las comunicaciones a través de las redes sociales y la navegación irrelevante.
- **La segmentación de la red** proporciona visibilidad y protección automatizada de las redes de infraestructura de nube híbrida.
- **La seguridad del correo electrónico** y el antispam protegen el tráfico de correo electrónico en las cargas de trabajo en la nube.
- **La seguridad web** y el antiphishing protegen contra amenazas de sitios web y scripts potencialmente peligrosos.

Problemas de

El cumplimiento es un requisito importante para cualquier organización. Los productos de Kaspersky permiten garantizar el cumplimiento a través de varios controles y funciones, como por ejemplo:

- **Jerarquía de servidores de gestión**, que proporciona la flexibilidad necesaria para respaldar la complejidad de la infraestructura.
- **Diferentes opciones de implementación**: en las instalaciones o en la nube.
- Informes e inspección de registros **integrales y altamente configurables** para simplificar las auditorías.
- **Control de acceso basado en roles (RBAC, del inglés "Role-Based Access Control")** para garantizar la segregación de los derechos de control entre diferentes grupos de administradores de acuerdo con la estructura empresarial y las políticas de TI.
- **Protección y autodefensa de la contraseña de los agentes** para evitar la manipulación de los sistemas de seguridad.
- **Comunicaciones seguras** entre todos los componentes de la solución.
- **Evaluación de vulnerabilidades y la gestión automatizada de parches**, que evita que el malware avanzado y las amenazas de día cero aprovechen las vulnerabilidades sin parches.
- **Cifrado con certificación FIPS 140-2 transparente para el usuario**, que protege completamente los datos confidenciales tanto in situ como en los dispositivos portátiles. La tecnología integrada implica que el cifrado se puede reforzar de forma centralizada.
- **Refuerzo de sistemas**: bloqueo ejecutable con el modo de denegación predeterminada y la prevención de los ataques de sustitución mediante la supervisión de la integridad de los archivos (FIM, del inglés "File Integrity Monitoring").
- **Control de dispositivos** para el control detallado del almacenamiento conectado, la cámara, el micrófono y cualquier otro hardware en uso.
- **Protección antimalware configurable y firewalls personales** para mejorar la seguridad de los servidores y las estaciones de trabajo.

También están disponibles funciones y mecanismos para garantizar una visibilidad completa, suficiente nivel de detalle y altos niveles de control, además de mejoras y adaptación continuas al panorama de riesgos.

Convertimos en realidad el sueño de la transformación digital segura

La transformación digital produce una gama completa de nuevas oportunidades, tanto para usted como para los cibercriminales que le acechan. Aproveche al máximo sus propias oportunidades de negocio a la vez que elimina con firmeza todas las oportunidades de ocasionar daños de sus atacantes con las mejores soluciones de seguridad de su categoría integradas de Kaspersky para entornos híbridos.

Kaspersky Hybrid Cloud Security: https://**latam**.kaspersky.**com**/enterprise-security/azure-hybrid-cloud-security
Seguridad para AWS: https://**latam**.kaspersky.**com**/enterprise-security/aws-hybrid-cloud-security
Seguridad para Microsoft Azure: https://**latam**.kaspersky.**com**/enterprise-security/azure-hybrid-cloud-security
Seguridad para Google Cloud: www.kaspersky.com/gcp

latam.kaspersky.com

kaspersky **PREPARADOS PARA EL FUTURO**