SI NO ES KASPERSKY ENDPOINT SECURITY FOR BUSINESS, ES QUE NO ES UNA PLATAFORMA DE PROTECCIÓN DE ENDPOINTS

10 VENTAJAS

QUE SOLO PUEDE OFRECER UNA SOLUCIÓN DE SEGURIDAD BASADA EN UNA PLATAFORMA INTEGRADA

KASPERSKY lab

El Informe de Riesgos Global de Seguridad de IT de Kaspersky determinó que el 94 % de las empresas había experimentado algún tipo de incidente de seguridad externa en los últimos 12 meses[1].

Como el volumen y la complejidad de las amenazas aumenta de forma exponencial, las empresas de todos los tamaños están desarrollando soluciones para una mejor comprensión de los riesgos de seguridad de IT, en concreto sobre los ataques con un objetivo, y para una protección contra amenazas específicas, en lugar de adoptar un enfoque amplio y al azar de una noción generalizada de "malware".

Es una lástima que muchos proveedores de seguridad de IT continúen exactamente con este enfoque amplio y al azar, adquiriendo nuevas tecnologías y sumando bases de código dispares, a menudo incompatibles, creando complejidad y causando tantos problemas como los que resuelve.

[1] Informe de riesgos de seguridad de IT globales 2014.

Los días de seguridad de endpoint tradicional, con controles independientes antimalware, de cifrado, de dispositivo y de red, están llegando a su final. Las plataformas de protección de endpoints (EPP), que prometen tecnologías de seguridad perfectamente integradas, son la tendencia creciente en seguridad, prevención avanzada de amenazas y protección de datos de IT.

Pero hay un mundo de diferencias entre "integración" y una plataforma genuina. Y cuando se trata de integración, esta se presenta de manera más o menos completa. Para muchos proveedores, la "integración" se ha convertido en un sinónimo de "compatible".

Y para algunos proveedores, "compatible" significa sumar productos comprados a las aproximadamente 40 adquisiciones y tratar de que funcionen con su propia base de código, sin importarles sus clientes.

Hay muchos proveedores que prometen soluciones "integradas", pero investigue un poco más y verá que hay una diferencia importante entre "compatibilidad" y la verdadera sinergia que proviene del análisis del desarrollo y los planes detallados de productos. Algunos proveedores luchan por unificar sus adquisiciones empresariales, pero afirman que pueden ofrecer plataformas realmente integradas.

Comprar cualquier producto que pueda ser la siguiente gran novedad no puede ofrecer la misma integridad de visión, o protección.

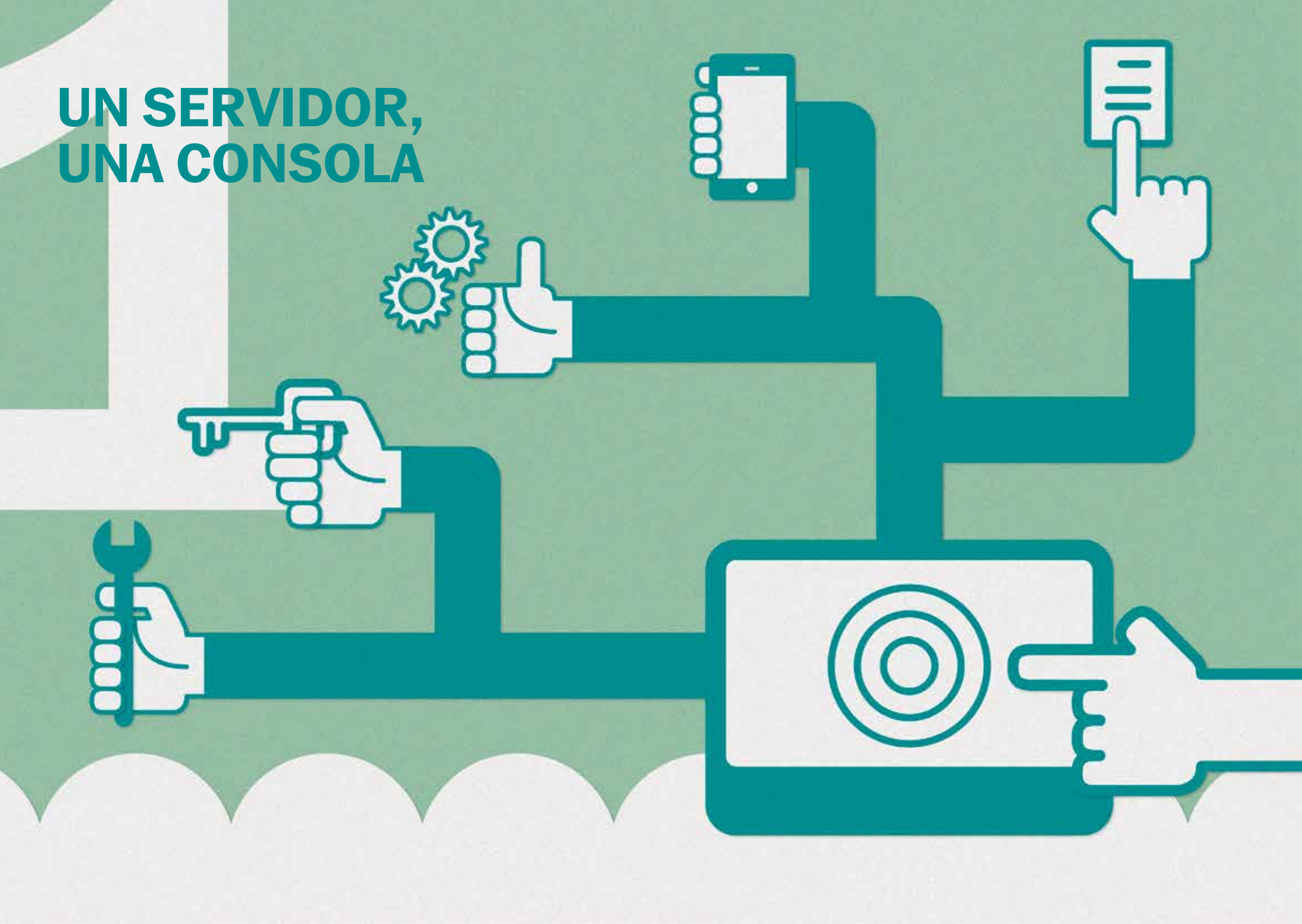
Hay algunas ventajas que solo puede ofrecer una plataforma integrada de forma genuina y en profundidad. Kaspersky Endpoint Security for Business se ha diseñado de forma única para ofrecer las siguientes ventajas a los administradores de IT:

1. Un servidor, una consola
2. Arquitectura de agente único*, instalación sencilla
3. La ventaja de una sola política
4. El efecto sinérgico: mayor que la suma de sus partes
5. Gestión unificada de derechos de administración: mayor capacidad de auditoría y control a través de una consola

6. Estructura, apariencia y comportamiento unificados: generación de informes más rápida y fácil
7. Una vista más clara y profunda de los datos: generación de informes y paneles de control integrados
8. Gestión y control unificados de las licencias: fomento de la eficacia y toma del control
9. Una base de código única, desarrollada internamente, que fomenta una integración más profunda
10. Modelo integrado de adquisición: todas las funciones que necesita, en una sola compra

* Arquitectura de agente único por plataforma (Windows, Linux, Mac).

UN SERVIDOR, UNA CONSOLA



1 UN SERVIDOR, UNA CONSOLA

La solución de Kaspersky Lab es la única que ofrece un servidor de gestión y una consola de administración estrechamente integrados que cubren cada aspecto de la seguridad de endpoints, desde el antimalware a la protección de datos, la gestión de dispositivos móviles y la gestión de sistemas: Kaspersky Security Center.

Las políticas y la generación de informes de seguridad se gestionan a través de una sola consola, integrada con recursos externos como directorios LDAP y Microsoft Exchange. Las bases de datos de inventario de hardware y software, así como las vulnerabilidades/actualizaciones de software, también se incluyen, lo que fomenta el aumento de las posibilidades de integración y sinergia, ya que los mismos datos se pueden utilizar en varias funciones. No es necesario seguir realizando la sincronización con varios servidores o conjuntos de datos. Todo se instala una vez, en el mismo servidor, y se gestiona a través de la misma consola.

Estas profundas capacidades de integración y sinergia ofrecen una ventaja que nos distingue de soluciones de la competencia, muchas de las cuales se componen de tecnologías adquiridas con varias bases de datos independientes, que sencillamente no pueden ofrecer la misma profundidad de integración que la plataforma de Kaspersky.

Las ventajas:

- **Implementación rápida y fácil:** un proceso de servidor de gestión, instalación de consola y configuración ofrece una funcionalidad totalmente integrada, lista para ser usada.

- **Un solo hardware de servidor de gestión:** sin complicaciones por los requisitos de diferentes componentes de hardware, sistemas o componentes adicionales para cada servidor de administración y consola. Kaspersky requiere solo UN servidor para la mayoría de implementaciones.

- **Un solo software de servidor de gestión:** infraestructura fácil de gestionar para pequeñas empresas, aunque con capacidad de ampliación para implementaciones de mayor tamaño.
  - — Algunos productos requieren la instalación de paquetes adicionales después de la implantación inicial para ofrecer una funcionalidad similar a la de Kaspersky Lab.
  - — Para mayor comodidad, la plataforma de Kaspersky incluye aplicaciones adicionales (por ejemplo, las necesarias en un entorno de Microsoft) como parte del proceso de instalación y autoinstalación, lo que permite ahorrar tiempo y problemas. Simplemente funciona.

ARQUITECTURA DE AGENTE ÚNICO*, INSTALACIÓN SENCILLA

* Arquitectura de agente único por plataforma (Windows, Linux, Mac).

2 ARQUITECTURA DE AGENTE ÚNICO*, INSTALACIÓN SENCILLA

La solución de Kaspersky es la única que ofrece un agente para endpoints que aprovecha una profunda integración de código para garantizar fácilmente una compatibilidad y una sinergia completas en todas las configuraciones de hardware y software.

Las genuinas plataformas de protección de endpoints disponen de una arquitectura optimizada, lo que reduce la complejidad y hace que la integración sea más profunda gracias al uso de un mínimo de agentes independientes para ejecutar las tareas. Las funciones relacionadas, como el análisis de vulnerabilidades, la actualización de aplicaciones y la aplicación de parches, junto con módulos de protección como el antimalware y el cifrado, tienen una arquitectura de agente único, lo que optimiza el rendimiento y reduce el impacto en la gestión.

Muchas ofertas de la competencia requieren agentes en el mismo equipo para funciones y características como los parches, el control de la aplicación o el cifrado. Esto genera posibles problemas con la compatibilidad de los agentes y requiere la realización de pruebas adicionales.

* Arquitectura de agente único por plataforma (Windows, Linux, Mac).

Las ventajas:

- **Ahorro de tiempo en la implementación inicial y las actualizaciones:** una simple tarea de instalación para el control, sin dependencias ni necesidad de numerosos reinicios.

- **Sin complicaciones con los diferentes requisitos del sistema:** no es un secreto que el crecimiento mediante adquisición genera desafíos de compatibilidad de software. La funcionalidad adquirida puede generar nuevos requisitos de asistencia independientes, además del software en el que se incluye. Es una pena que descubra esto cuando ya ha iniciado una implementación… Solo un enfoque orgánico e integrado de la implementación puede garantizar una compatibilidad perfecta para los diferentes componentes de software de plataformas/dispositivos de endpoints gestionados. Esto también supone la reducción del número de pruebas de compatibilidad por parte del cliente.

- **Menor impacto:** impacto en el rendimiento y la gestión del sistema.

- **Base para el desarrollo de escenarios de sinergia:** la profunda integración permite disfrutar de flexibilidad y una mayor funcionalidad. Esto supone una ampliación de las capacidades sin aumentar el impacto en los recursos.

LA VENTAJA DE UNA SOLA POLÍTICA

3 LA VENTAJA DE UNA SOLA POLÍTICA

La complejidad es enemiga de la seguridad, aunque la gestión de todos los aspectos de la seguridad de la información en toda una organización a menudo conlleva el uso de varias soluciones muy diferentes. Cuanto más pueda simplificar los procesos de gestión, más aumentará la claridad y reducirá los riesgos.

Una verdadera plataforma de protección de endpoints controla la detección, la implementación, la configuración de las políticas y la actualización de los endpoints en toda la infraestructura de la empresa. Un agente único por plataforma de Kaspersky Endpoint Security significa que los administradores pueden establecer una política activa para un grupo gestionado que abarque todos los componentes necesarios sin necesidad de varias revisiones de políticas o correlación.

El "agente de red" conecta el endpoint con el servidor de administración, realizando las tareas de gestión de sistemas (como el inventario de software y hardware, el análisis de vulnerabilidades y la gestión de parches), lo que permite disfrutar de verdadera flexibilidad y sinergia entre las funciones.

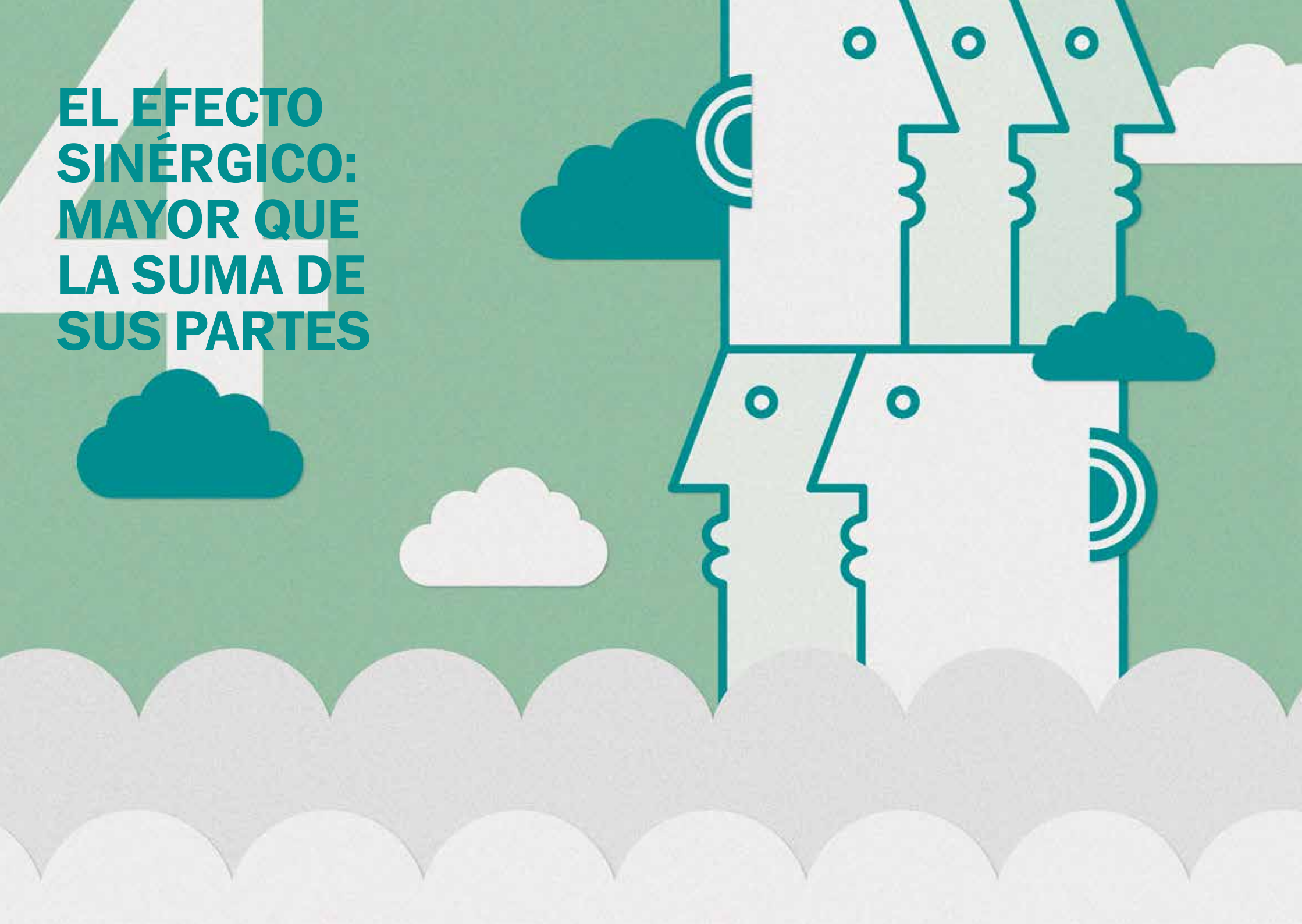
Las ventajas:

- **Gestión de políticas y tareas simplificada:** gracias a un solo conjunto de parámetros y requisitos previos compartidos (grupos gestionados, ajustes de entrega y notificaciones), la implementación de las políticas se optimiza, eliminando los procesos y las tareas redundantes para el administrador de IT.

- **Control más fácil de la implementación de políticas y tareas:** el panel único y la generación de informes de implementación y ejecución proporcionan una vista completa e inmediata del estado y el cumplimiento de las políticas en toda la red.

- **Cambios optimizados en las políticas y tareas:** las modificaciones se realizan en un solo paso. La asignación de políticas automática puede cubrir varios parámetros de seguridad de una vez, desde varios ajustes de protección a controles de aplicaciones, dispositivos y web, además de políticas de cifrado.

EL EFECTO SINÉRGICO: MAYOR QUE LA SUMA DE SUS PARTES



4 EL EFECTO SINÉRGICO: MAYOR QUE LA SUMA DE SUS PARTES

Las funciones integradas de protección de endpoints forman el núcleo de la plataforma de seguridad de Kaspersky, lo que hace que incluso los escenarios de seguridad avanzados y complejos sean fáciles de implementar. La integración verdadera brinda una seguridad superior a cada uno de los componentes por separado, por ejemplo:

Para implementar una protección completa frente a las amenazas en Internet, junto con el análisis del tráfico web y los archivos descargados basado en políticas, una empresa puede utilizar la función de control de aplicaciones de Kaspersky para aplicar el uso de un solo navegador aprobado por IT.
Este navegador, a su vez, se puede proteger más aún mediante la aplicación de parches de vulnerabilidad automáticos de alta prioridad, así como hacer frente a ataques de día cero mediante la prevención automática contra exploits. De esta forma, las funciones integradas de Kaspersky proporcionan un manto de seguridad frente a un gran vector de ataque. A eso nos referimos con el efecto sinérgico.

Las ventajas:

- **Uso compartido cruzado de las prácticas de gestión de seguridad y la información recopilada de diferentes funciones, por ejemplo:**
  - — La información recopilada de dispositivos extraíbles se emplea para el cifrado y control de dispositivos.
  - — La información sobre las aplicaciones se introduce en el control de aplicaciones y las políticas de cifrado.
  - — La gestión de dispositivos móviles (MDM) se integra en la seguridad de los datos de los dispositivos.
  - — Las decisiones de gestión de parches se pueden basar en la valoración de vulnerabilidades.

El efecto sinérgico no se limita a los escenarios descritos anteriormente: la profunda integración de código de Kaspersky garantiza una compatibilidad y una sinergia completas en todas las configuraciones de hardware y software. Con la plataforma de Kaspersky, la seguridad se extiende más allá de cada componente de la función.

GESTIÓN UNIFICADA DE DERECHOS DE ADMINISTRACIÓN: MAYOR CAPACIDAD DE AUDITORÍA Y CONTROL A TRAVÉS DE UNA CONSOLA

5 GESTIÓN UNIFICADA DE DERECHOS DE ADMINISTRACIÓN: MAYOR CAPACIDAD DE AUDITORÍA Y CONTROL A TRAVÉS DE UNA CONSOLA

Los departamentos de IT faltos de personal son un problema habitual para muchas pymes y grandes empresas. Los recortes económicos y la mayor complejidad de IT suponen que los administradores de IT tienen que realizar más tareas y tienen menos tiempo para hacerlo.

La plataforma de protección de endpoints de Kaspersky afronta este desafío, ya que proporciona herramientas de gestión unificadas para las tareas de seguridad de día a día. La profunda integración permite controlar los privilegios y gestionar los registros desde una sola consola. Un registro para todas las acciones: al contrario que los productos de la competencia, que a menudo tienen que recuperar los datos en consolas y servidores independientes.

La gestión unificada de derechos e inicio de sesión mejora el control y la supervisión de las acciones del personal, lo que redunda en una gestión más eficaz de los permisos. El resultado: un mayor control de la seguridad y las auditorías en las operaciones y la gestión de IT. Desde una consola.

Las ventajas:

- **Permisos fáciles de definir y controlar:** en una pyme típica, en la que el "chico de IT" se encarga de todo, debería resultar fácil realizar todas las tareas relacionadas con la seguridad, incluida la configuración de permisos de lectura/modificación, acceso, etc.

- **Respuesta a incidencias rápida y registro de eventos unificado:** los administradores de IT son solo humanos; se cometen errores y, en caso de una incidencia de seguridad, una respuesta rápida es esencial. Es vital disponer de una funcionalidad que permita los cambios y bloqueos rápidos en la admisión, junto con la capacidad de realizar un seguimiento de dichos cambios. Con las soluciones independientes, las incidencias complejas pueden requerir la creación de varios procesos de análisis. Kaspersky elimina la complejidad y cubre todos los cambios en la seguridad de endpoints, las políticas y las actividades de gestión en un solo archivo de registro, proporcionado por una sola interfaz de consola de gestión.

ESTRUCTURA, APARIENCIA Y COMPORTAMIENTO UNIFICADOS: GENERACIÓN DE INFORMES MÁS RÁPIDA Y FÁCIL

6 ESTRUCTURA, APARIENCIA Y COMPORTAMIENTO UNIFICADOS: GENERACIÓN DE INFORMES MÁS RÁPIDA Y FÁCIL

Los administradores bajo presión aprovecharán cualquier oportunidad para ahorrar tiempo o hacer que una tarea sea más fácil de realizar. Las plataformas de protección de endpoints con funciones unificadas e integradas y una interfaz común permiten gestionar con mayor facilidad la generación de informes, el análisis y las incidencias: Kaspersky Security Center genera una estructura de informes similar con una apariencia y un comportamiento comunes.

Un día de trabajo de un administrador de IT implica normalmente multitud de tareas tan vitales como rutinarias, que hay que supervisar y de las que hay que generar informes. En un entorno de soluciones mixto, esto conlleva varios paneles de control, todos los cuales generan informes en diferentes formatos, desde PDF a HTML o correo electrónico directo. ¿Quién tiene tiempo de mirarlo todo y asegurarse de que funciona como debería?

En este entorno, incluso la mejora más pequeña en la facilidad de uso o la eficacia puede ahorrar mucho tiempo y reducir la carga de trabajo (por no mencionar el estrés) de los ya saturados administradores de seguridad de IT. La generación de informes habitual, con una apariencia y un comportamiento comunes, puede facilitar el análisis y la valoración, mejorando la gestión de incidencias y respaldando un enfoque proactivo de la seguridad de IT.

Las ventajas:

- **Análisis de informes más rápido y fácil:** la misma terminología y estructura se utilizan en todas las plantillas de informes. "Ordenador, PC, nodo, equipo": todos son sinónimos del mismo endpoint gestionado. Todos se utilizan indistintamente en la documentación de los productos y los proveedores. Si añadimos suficientes productos a la mezcla, las cosas se pueden poner un poco confusas. ¿Y si todos los componentes de seguridad de su entorno de soluciones mixto tuvieran un problema de lenguaje similar? ¿Y si cada parámetro de cada uno de estos componentes tuviera "los mismos" nombres, "pero diferentes"? En un entorno tan complicado, la realización de investigaciones sobre amenazas y otras incidencias se hace mucho más complicada de lo necesario, incluso para administradores familiarizados con la configuración. Los administradores deben aceptar la complejidad, pero ¿que ocurre en una situación en la que participan investigadores externos, como auditores o reguladores…? Si les ofrece una descripción general confusa de su infraestructura, es probable que dé la impresión equivocada.

- **Gestión de incidencias simplificada:** reconozca fácilmente incidencias similares en los diferentes nodos de la infraestructura de IT, como malware y filtraciones en las políticas.

UNA VISTA MÁS CLARA Y PROFUNDA DE LOS DATOS: GENERACIÓN DE INFORMES Y PANELES DE CONTROL INTEGRADOS

7 UNA VISTA MÁS CLARA Y PROFUNDA DE LOS DATOS: GENERACIÓN DE INFORMES Y PANELES DE CONTROL INTEGRADOS

Las plataformas de protección de endpoints deben proporcionar un enfoque más amplio de los paneles de control y la generación de informes. La integración verdadera va más allá de la apariencia y el comportamiento de la interfaz: por ejemplo, hacer clic en una sola pestaña de "propiedades de endpoints" en una consola de administración debe ofrecer información sobre todos los aspectos de la seguridad del cliente gestionado, como las políticas aplicadas, las actualizaciones de estado y las incidencias.

Los paneles de control y los informes también deben facilitar el proceso de investigación y generar una mayor flexibilidad del endpoint: la integración permite que la información se recopile de varios componentes, lo que facilita bastante las cosas.

Las ventajas:

- **Único panel de control para todos los componentes de seguridad de endpoints:** un panel facilísimo que no es necesario estar investigando toda la mañana e incluye la información más importante sobre el estado de los endpoints gestionados, la implementación de la ejecución de las tareas y el control de las licencias, además de los principales eventos de seguridad e incidencias.

- **Profundización y análisis optimizados:** profundice en los informes independientes para analizar y recopilar los datos desde distintos ángulos, incluidos la gestión de endpoints, la valoración de vulnerabilidades y aplicación de parches, el inventario de hardware y aplicaciones, y las cuentas de usuario creadas. Visibilidad fácil del estado de la protección y las incidencias, incluidos la detección de malware y el estado del cifrado de los datos. Esto hace que el análisis y la investigación de seguridad sean un proceso fácil y optimizado.

- **Generación de informes ejecutivos lista para usar:** la generación de informes ejecutivos es un componente fundamental de las responsabilidades de un administrador de seguridad de IT. La creación de informes completos en varias consolas y conjuntos de datos es lenta y supone un quebradero de cabeza. Por eso la plataforma de seguridad de endpoints de Kaspersky proporciona una función de generación de informes ejecutivos lista para usar. No es necesario personalizar los informes utilizando herramientas de terceros, por lo que aumenta el tiempo para centrarse en otros proyectos.

GESTIÓN Y CONTROL UNIFICADOS DE LAS LICENCIAS: FOMENTO DE LA EFICACIA Y TOMA DEL CONTROL

8 GESTIÓN Y CONTROL UNIFICADOS DE LAS LICENCIAS: FOMENTO DE LA EFICACIA Y TOMA DEL CONTROL

La gestión de las licencias de todas las soluciones de seguridad en toda la red de la empresa nunca ha resultado más fácil. Con Kaspersky Labs, todas (y queremos decir TODAS) las funciones se activan utilizando una sola licencia: seguridad de endpoints, protección de datos, gestión de dispositivos móviles y gestión de sistemas.

Una licencia única es fácil de distribuir por toda la infraestructura de endpoints, independientemente de su estado o ubicación, de su condición de tipo de máquina física o virtual, o de si la red es fija o móvil. La función de gestión de licencias integrada de Kaspersky le permite usar de forma más eficaz lo que está pagando, a la vez que mantiene un control más estricto de la validez de las licencias.

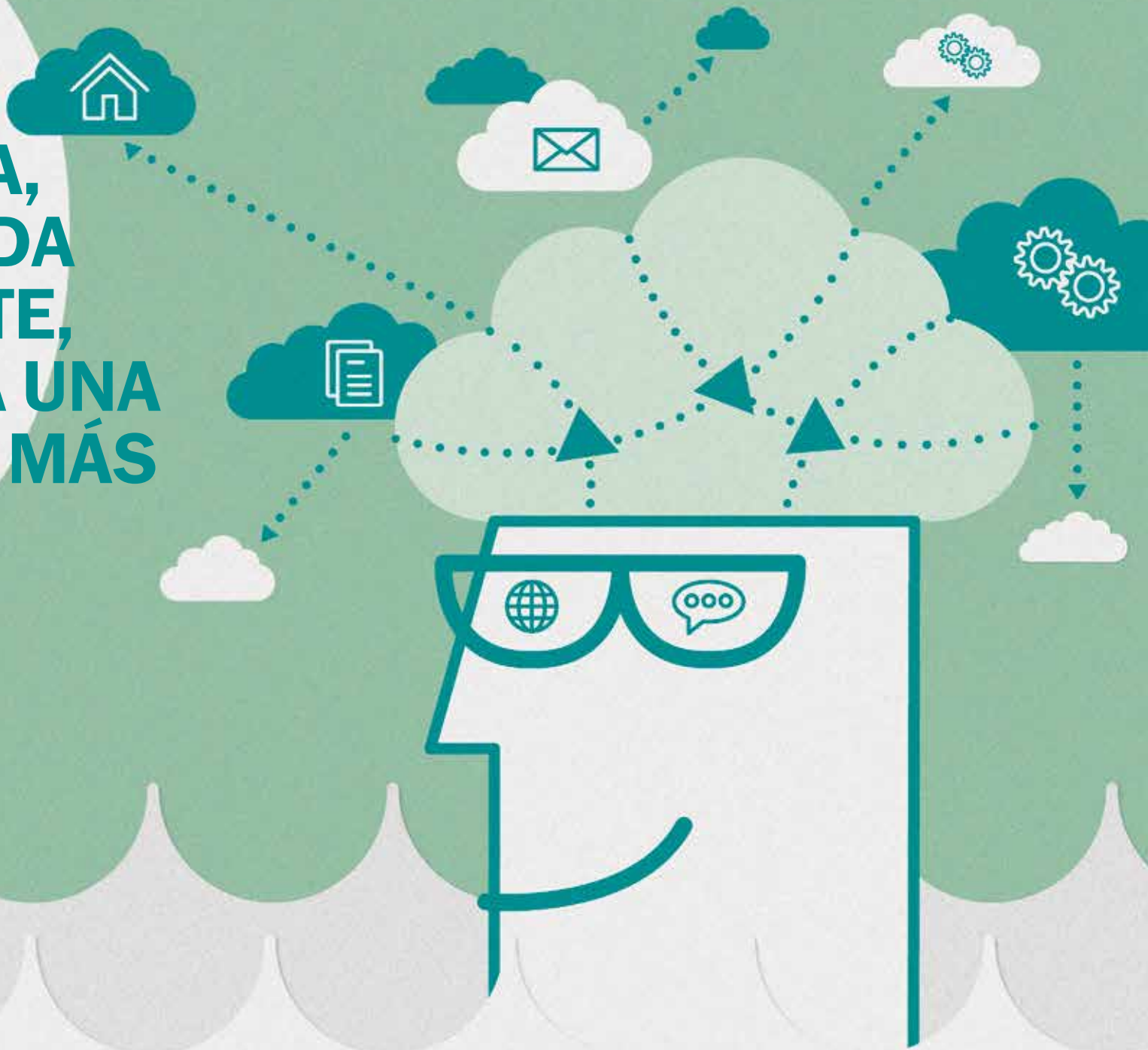
Las ventajas:

- **Único panel de control para auditoría de licencias:** sin necesidad de recurrir a diferentes herramientas de control de licencias para supervisar y comprobar el estado.

- **Uso eficiente de las licencias:** reduzca los costes mediante una distribución flexible en un entorno de IT cambiante. Por ejemplo, migración desde PC y portátiles tradicionales a dispositivos móviles con funcionalidad simultánea.

- **Actualización sencilla de la solución de seguridad:** con la plataforma de protección de endpoints de Kaspersky, puede aumentar la funcionalidad de la seguridad según sus necesidades. Empiece con la seguridad para endpoints y simplemente active funciones como el cifrado o la gestión de sistemas añadiendo una nueva licencia.

UNA BASE DE CÓDIGO ÚNICA, DESARROLLADA INTERNAMENTE, QUE FOMENTA UNA INTEGRACIÓN MÁS PROFUNDA



9 UNA BASE DE CÓDIGO ÚNICA, DESARROLLADA INTERNAMENTE, QUE FOMENTA UNA INTEGRACIÓN MÁS PROFUNDA

La base de código único de Kaspersky, diseñada y mantenida internamente, es el corazón de nuestra plataforma de seguridad de endpoints integrada.

Mientras otros proveedores han seguido estrategias de adquisición para aumentar su oferta de productos en un panorama que cambia rápidamente, Kaspersky es la única empresa que está desarrollando y manteniendo todo internamente. Al contrario que ocurre con otros proveedores, esto respalda una profunda integración de la base de código, lo que nos permite ofrecer las muchas ventajas descritas anteriormente en este documento.

Las ventajas:

- Un solo servidor de gestión y consola de administración
- Arquitectura de cliente de endpoints única
- Políticas únicas y tareas unificadas
- Efecto sinérgico de la funcionalidad integrada
- Notificación y paneles de control integrados

La misma base de código y el mismo proceso de desarrollo facilitan la aplicación más rápida de actualizaciones y parches: los usuarios de Kaspersky pueden actualizar una sola aplicación en lugar de dos o más (y los componentes que incluyen), como requieren muchos productos de la competencia.

MODELO INTEGRADO DE ADQUISICIÓN: TODAS LAS FUNCIONES QUE NECESITA, EN UNA SOLA COMPRA

10 MODELO INTEGRADO DE ADQUISICIÓN: TODAS LAS FUNCIONES QUE NECESITA, EN UNA SOLA COMPRA

Un solo pedido cubre todas las necesidades y funciones de seguridad, y basta con una sola licencia para activar todos los componentes.

Las ventajas:

- **Atención de distintas necesidades en un solo paquete:** los usuarios de Kaspersky puede adquirir distintos niveles y versiones de funcionalidad integrada que atienden diferentes necesidades de los clientes, todos los cuales utilizan un solo paquete de licencia. Esto es algo exclusivo.

POR ÚLTIMO...

Con Kaspersky Lab, los usuarios obtienen una plataforma de protección de endpoints genuina, desarrollada de principio a fin con la misma base de código y organización de I+D. Nuestras tecnologías de vulnerabilidad de antimalware y software integradas han sido desarrolladas por nuestro grupo de investigación interno especializado, que estudia constantemente cómo las amenazas modernas penetran en los sistemas para desarrollar una protección más eficaz.

El grupo de investigación de marcado en lista blanca y vulnerabilidades de aplicaciones propias de Kaspersky Lab gestiona nuestro ecosistema de socios y proveedores, y ofrece una base de datos de software legítimo que se actualiza constantemente, a la vez que proporciona la información más actualizada sobre disponibilidad de parches.

La convergencia de la tecnología de seguridad de endpoints y gestión de clientes/sistemas es una tendencia creciente. Kaspersky Lab, con su base de código y su proceso de desarrollo totalmente internos, se encuentra en una posición privilegiada para explotar las evidentes sinergias entre las funciones de seguridad y los tradicionalmente percibidos como componentes de la gestión de sistemas.

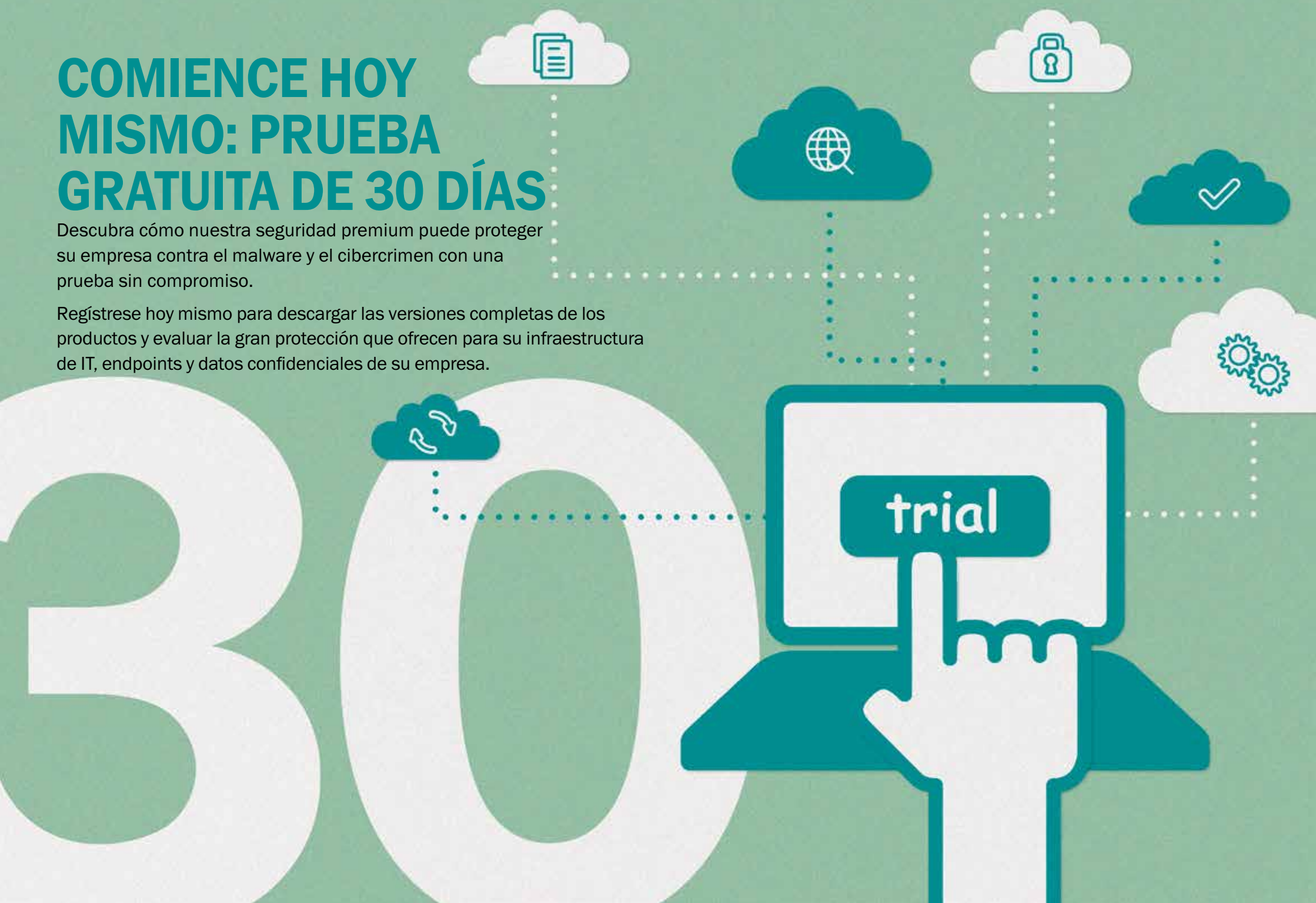
La integración de Kaspersky Lab ofrece una verdadera plataforma de protección de endpoints. La protección es óptima, no opcional.

Más información en **www.kaspersky.com/sp/business**.

COMIENCE HOY MISMO: PRUEBA GRATUITA DE 30 DÍAS

Descubra cómo nuestra seguridad premium puede proteger su empresa contra el malware y el cibercrimen con una prueba sin compromiso.

Regístrese hoy mismo para descargar las versiones completas de los productos y evaluar la gran protección que ofrecen para su infraestructura de IT, endpoints y datos confidenciales de su empresa.



ACERCA DE KASPERSKY LAB

Kaspersky Lab es el mayor proveedor privado de soluciones de protección de endpoints del mundo. La empresa figura entre los cuatro proveedores principales de soluciones de seguridad para usuarios de endpoints.* A lo largo de sus más de 17 años de historia, Kaspersky Lab se ha mantenido como una empresa innovadora en seguridad de IT y suministra eficaces soluciones de seguridad digitales para grandes empresas, pymes y particulares. Kaspersky Lab, cuya sociedad de cartera está registrada en el Reino Unido, opera actualmente en casi 200 países y territorios del globo, y brinda protección a más de 300 usuarios en todo el mundo.
Más información en **www.kaspersky.es**.

* La empresa logró el cuarto puesto en el índice de IDC de ingresos de seguridad para endpoints en todo el mundo por proveedor de 2012. Este índice se publicó en el informe de IDC "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC núm. 242618, agosto de 2013). En el informe se clasifican los proveedores de software según los ingresos de ventas de soluciones de seguridad para endpoints en 2012.

ÚNASE A LA CONVERSACIÓN

#securebiz

Véanos en YouTube


Véanos en Slideshare


Síganos en Facebook


Consulte nuestro blog


Síganos en Twitter

Únase a nosotros en LinkedIn

KASPERSKY lab