KASPERSKY SECURITY FOR COLLABORATION

Protección de datos y control para plataformas de colaboración, incluidas las granjas de SharePoint.

La plataforma que utiliza para compartir archivos e información también proporciona un sistema de tránsito rápido, el que es ideal para malware peligroso y otras amenazas de TI.
Para proporcionar un entorno de trabajo compartido que sea seguro y no tenga incidentes, Kaspersky Lab ha desarrollado una solución que combina la facilidad de administración con la protección en tiempo real de primer nivel contra ataques de malware y fugas de datos confidenciales.

- Motor anti-malware premiado
- "Búsqueda y protección" de datos confidenciales
- Controles de acceso a los datos
- Protección en tiempo real basada en la nube – Kaspersky Security Network
- Filtrado de archivos y contenido
- Protección Anti-phishing
- Copias de seguridad y almacenamiento
- Administración centralizada y flexible
- Consola de administración intuitiva

ASPECTOS DESTACADOS

PROTECCIÓN COMPLETA PARA SU PLATAFORMA SHAREPOINT.

Si está ejecutando Microsoft SharePoint Server, sabrá que, debido a que todo el contenido se almacena en una base de datos SQL, las soluciones de endpoint tradicionales no pueden realizar el trabajo. Kaspersky Security for Collaboration aplica la protección antimalware avanzada y galardonada en toda la granja de SharePoint y a todos sus usuarios. Se entrega una poderosa protección contra amenazas conocidas, desconocidas y avanzadas a través de Kaspersky Security Network compatible con la nube, a la vez que la tecnología antiphishing protege contra amenazas en la web a los datos de colaboración.

PREVENCIÓN DE FUGA DE DATOS CONFIDENCIALES.

Para controlar y proteger la circulación de datos confidenciales, primero hay que identificar dichos datos. Mediante el uso de diccionarios preinstalados o personalizados y de categorías de datos, Kaspersky Security for Collaboration comprueba cada documento que se coloque en los servidores SharePoint para detectar información sensible, palabra por palabra y frase por frase. La protección y el control se dirigen específicamente a datos de tarjetas de pago y personales, a la vez que las búsquedas estructuradas cazan documentos sensibles, como bases de datos de clientes.

CUMPLIMIENTO DE LAS POLÍTICAS DE COMUNICACIÓN.

Las funciones de contenido y filtrado ayudan a hacer cumplir sus políticas y normas de comunicación, dado que identifican y bloquean el contenido inapropiado, mientras al mismo tiempo evitan el almacenamiento ineficaz de archivos y de formatos de archivos inadecuados.

FACILIDAD DE ADMINISTRACIÓN.

Se puede administrar la seguridad de toda la granja de servidores desde un panel único e intuitivo. La administración es rápida y expedita, sin necesidad de capacitaciones especiales.

PROTECCIÓN ANTIVIRUS

- **Escaneo en el momento de acceso** - escaneo de los archivos en tiempo real, durante la carga o descarga.
- **Escaneo en segundo plano** - comprobación periódica de los archivos almacenados en el servidor a través de las firmas de malware más recientes.
- **Integración con Kaspersky Security Network** - entrega de protección en tiempo real asistida por la nube incluso contra las amenazas de día cero.

ADMITE LAS POLÍTICAS DE COMUNICACIÓN DE SU ORGANIZACIÓN

- **Filtrado de archivos** - permite implementar las políticas de almacenamiento de documentos y reducir las exigencias sobre los dispositivos de almacenamiento. Mediante el análisis de formatos de archivos reales, independientemente del nombre de la extensión, la aplicación garantiza que los usuarios no puedan utilizar un tipo de archivo prohibido que viole la política de seguridad.
- **Protección para wikis/blogs** - protege todos los repositorios de SharePoint, incluidos wikis y blogs.
- **Filtrado de contenido** - evita el almacenamiento de archivos que incluyen contenidos inapropiados, independientemente del tipo de archivo. Se utilizan palabras clave para analizar el contenido de cada archivo. Además, los clientes pueden crear sus propios diccionarios personalizados para el filtrado de contenido.

PREVENCIÓN DE FUGA DE DATOS CONFIDENCIALES

- **Escaneo de documentos para detectar información confidencial** - Kaspersky Security for Collaboration escanea todos los documentos descargados en servidores SharePoint para detectar información confidencial.

  La solución integra módulos que identifican tipos específicos de datos y comprueban que cumplen con las normas jurídicas correspondientes, por ejemplo, de datos personales (definidas por el cumplimiento de normativas, como por ejemplo, HIPAA (Ley de Transferibilidad y Responsabilidad de Seguros Médicos) o la Normativa de la UE 95/46/CE) o datos de los estándares PCI DSS (Estándares de Seguridad de Datos de la Industria de las Tarjetas de Pago).

  Los datos se escanean y se comparan con diccionarios temáticos incorporados que se actualizan regularmente y que abarcan categorías como "Finanzas", "Documentos administrativos" y "Lenguaje humillante y abusivo", y se comparan con diccionarios personalizados.
- **Búsqueda estructurada de datos** - si en un mensaje se encuentra información presentada en estructuras específicas, se considerará como potencialmente confidencial, lo que garantiza el control de datos sensibles, como las bases de datos de los clientes, que se mantienen en conjuntos complejos.

ADMINISTRACIÓN FLEXIBLE

- **Facilidad de administración** - la totalidad de la granja de servidores se puede administrar de forma centralizada desde una consola única. Una interfaz intuitiva incluye todos los escenarios administrativos utilizados de forma más común.
- **Panel único** - el panel de diseño claro proporciona acceso en tiempo real al estado actual del producto, la versión de la base de datos y el estado de la licencia de todos los servidores protegidos.
- **Copia de respaldo de archivos modificados** - en caso de algún incidente, y de ser necesario, es posible restaurar los archivos originales y se puede utilizar la información de la copia de respaldo detallada acerca de los archivos modificados para brindar apoyo a las investigaciones.
- **Integración con Active Directory®** - permite la autenticación de los usuarios de Active Directory.

REQUISITOS DEL SISTEMA

Servidores de SharePoint:

- Microsoft SharePoint 2010;
- Microsoft SharePoint 2013.

Sistema operativo (para instalar la solución)

Para SharePoint Server 2010:

- Windows Server 2008 x64/2008 R2/2012 R2.

Para SharePoint Server 2013:

- Windows Server 2008 R2 x64 SP1/2012 x64/2012 R2

La lista completa de requisitos del sistema está disponible en kaspersky.com

Cómo comprar

Kaspersky Security for Collaboration se puede adquirir como parte de Kaspersky Total Security for Business o como una solución focalizada independiente.

Nota: Cuando compra este producto, la opción para evitar fugas de información confidencial se vende por separado.

Kaspersky Security for Collaboration/Versión 0.3/15 Ene/Global

KASPERSKY lab