KASPERSKY SECURITY FOR COLLABORATION

Protección de datos y control para plataformas de colaboración, incluidos los grupos de servidores de SharePoint.

La plataforma que se utiliza para compartir archivos e información también proporciona un sistema de tránsito rápido ideal para malware peligroso y otras amenazas de IT.
Para proporcionar un entorno de trabajo de uso compartido fluido y seguro, Kaspersky Lab ha desarrollado una solución que combina la facilidad de gestión con una protección excelente en tiempo real contra ataques de malware y fugas de datos confidenciales.

- Motor antimalware galardonado
- "Búsqueda y protección" de datos confidenciales
- Controles de acceso a datos
- Protección en tiempo real basada en la nube: Kaspersky Security Network
- Filtrado de contenidos y archivos
- Protección antiphishing
- Copia de seguridad y almacenamiento
- Gestión centralizada flexible
- Consola de administración intuitiva

INFORMACIÓN DESTACADA

PROTECCIÓN COMPLETA PARA SU PLATAFORMA SHAREPOINT

Si está ejecutando Microsoft SharePoint Server, sabrá que, dado que todo el contenido se almacena en una base de datos SQL, las soluciones tradicionales de endpoint no pueden realizar el trabajo. Kaspersky Security for Collaboration aplica una protección antimalware avanzada galardonada a todo el grupo de servidores de SharePoint y a todos sus usuarios. Kaspersky Security Network con asistencia en la nube proporciona una potente protección contra amenazas conocidas, desconocidas y sofisticadas, mientras que la tecnología antiphishing protege los datos de colaboración frente a amenazas basadas en la web.

PREVENCIÓN DE LA FILTRACIÓN DE DATOS CONFIDENCIALES

Para controlar y proteger la circulación de datos confidenciales, en primer lugar es necesario identificar los datos. Mediante las categorías de datos y los diccionarios preinstalados o personalizados, Kaspersky Security for Collaboration busca información confidencial en cada documento depositado en los servidores SharePoint, palabra por palabra y frase por frase. Los datos personales y de tarjetas de pago son el objetivo principal de la protección y el control, si bien las búsquedas basadas en estructuras detectan documentos confidenciales, como bases de datos de clientes.

IMPLEMENTACIÓN DE POLÍTICAS DE COMUNICACIÓN

Las funciones de contenido y filtrado contribuyen a la aplicación de las políticas y normas relativas a las comunicaciones, ya que identifican y bloquean el contenido inadecuado a la vez que evitan que se desaproveche el espacio de almacenamiento con archivos y formatos que no son apropiados.

ADMINISTRACIÓN SENCILLA

La seguridad destinada al grupo completo de servidores puede administrarse de forma centralizada gracias a la presencia de un único panel intuitivo. La administración es rápida y sencilla y no necesita recibir formación específica.

PROTECCIÓN ANTIVIRUS

- **Análisis por acceso**: los archivos se analizan en tiempo real, al cargarse o descargarse.
- **Análisis en segundo plano**: los archivos almacenados en el servidor se comprueban de forma periódica mediante las últimas firmas de malware.
- **Integración con Kaspersky Security Network**: protección con asistencia en la nube en tiempo real incluso contra amenazas de día cero.

COMPATIBILIDAD CON LAS POLÍTICAS DE COMUNICACIÓN DE SU ORGANIZACIÓN

- **Filtrado de archivos**: ayuda a aplicar políticas de almacenamiento de documentos y reducir las solicitudes de los dispositivos de almacenamiento. Mediante el análisis de los formatos de archivos reales, independientemente del nombre de extensión, la aplicación garantiza que los usuarios no pueden utilizar un tipo de archivo prohibido para que no infrinjan la política de seguridad.
- **Protección de wikis y blogs**: protege todos los repositorios de SharePoint, incluidos wikis y blogs.
- **Filtrado de contenidos**: evita el almacenamiento de archivos que incluyen contenido inapropiado, independientemente del tipo de archivo. El contenido de cada archivo se analiza en función de palabras clave. Los clientes también pueden crear sus propios diccionarios personalizados para filtrar contenido.

PREVENCIÓN DE FUGA DE DATOS CONFIDENCIALES

- **Análisis de documentos en busca de información confidencial**: Kaspersky Security for Collaboration analiza todos los documentos descargados en servidores de SharePoint en busca de información confidencial.

  La solución integra módulos que identifican tipos específicos de datos para confirmar que cumplen los estándares legales correspondientes; por ejemplo, los datos personales (definidos por el cumplimiento de las normativas, como la ley HIPAA o la Directiva de la Unión Europea 95/46/EC) o los datos estándar PCI DSS (norma relativa a la seguridad de los datos del sector de las tarjetas de pago).

  Los datos se analizan y se contrastan con los diccionarios temáticos integrados actualizados que abarcan categorías como: "Finanzas", "Documentos administrativos" y "Lenguaje humillante y abusivo" y con los diccionarios personalizados.
- **Búsqueda estructurada de datos**: si se encuentra en un mensaje información presentada en estructuras específicas, se tratará como potencialmente confidencial, garantizando el control de los datos confidenciales (tales como bases de datos de clientes, que pueden presentarse de formas más complejas).

GESTIÓN FLEXIBLE

- **Facilidad de gestión**: se puede gestionar un grupo completo de servidores de forma centralizada desde una única consola. Una interfaz intuitiva incluye todas las situaciones administrativas más habituales.
- **Un único panel**: un panel de visualización claro proporciona acceso en tiempo real al estado actual del producto, a la versión de la base de datos y el estado de la licencia de todos los servidores protegidos.
- **Copia de seguridad de archivos modificados**: en caso de cualquier incidente, los archivos originales se pueden restaurar si es necesario y la información detallada de las copias de seguridad sobre archivos modificados se puede utilizar para ayudar en 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 comprarlo

Kaspersky Security for Collaboration puede adquirirse como parte integrante de Kaspersky Total Security for Business o como solución adaptada independiente.

Nota: Al comprar este producto, la opción para evitar la filtración de datos confidenciales se vende por separado.

Kaspersky Security for Collaboration/Versión 0.3/Enero de 2015/Global

KASPERSKY lab