

KASPERSKY SECURITY FOR WINDOWS SERVER™

Solución desarrollada específicamente para servidores corporativos de alto rendimiento

El aumento en la complejidad de las redes corporativas de IT conlleva niveles de protección de los servidores cada vez más elevados. La presencia de un único archivo infectado en el sistema puede propagar el virus a todos los ordenadores de la red y provocar daños incalculables. Una solución de seguridad para los servidores específica y adecuada no solo garantiza la protección de los datos importantes contra las últimas amenazas de malware, sino que, además, elimina el riesgo de que este software penetre en las copias de seguridad de los archivos y provoque brotes repetidos.

Kaspersky Security for Windows Server brinda seguridad rentable, fiable y escalable para el almacenamiento de archivos compartidos con un impacto mínimo en los recursos.

Aspectos destacados de la aplicación

PROTECCIÓN CONTRA MALWARE CONOCIDO, DESCONOCIDO Y SOFISTICADO

Nuestro motor antimalware líder del sector garantiza análisis más rápidos y un menor impacto en los recursos del sistema, lo que proporciona el índice de detección más elevado a través de seguridad y asistencia en la nube (Kaspersky Security Network).

SEGURIDAD AVANZADA PARA SERVIDORES FUNDAMENTALES

El potente control de inicio de las aplicaciones en combinación con inteligencia de seguridad global y funciones anticifrado añade más niveles de protección avanzada para los sistemas de almacenamiento y servidores corporativos.

SOLUCIÓN CERTIFICADA

Se ha certificado la compatibilidad de la aplicación con las plataformas de virtualización y los sistemas operativos.

Características de la aplicación

PROTECCIÓN EFICAZ FRENTE A PROGRAMAS MALICIOSOS

Protección antimalware siempre activa y análisis programados. La aplicación analiza todos los archivos iniciados o modificados; además, trata, elimina o pone en cuarentena los objetos sospechosos. Si se instala un nuevo software o se sospecha de la infección de un archivo, el administrador también puede iniciar un análisis antimalware en las zonas sospechosas.

Protección con asistencia en la nube. Kaspersky Security Network (KSN) ofrece una respuesta más rápida que nunca ante las amenazas, lo que mejora el rendimiento de los componentes de protección y minimiza el riesgo de falsos positivos.

Potente control de inicio de las aplicaciones en servidores. Proporciona una seguridad sin precedentes mediante el uso de reglas configuradas para permitir o bloquear el inicio de archivos ejecutables, scripts y paquetes MSI, o la carga de módulos DLL a los servidores.

Protección de carpetas compartidas frente a malware de cifrado (anticifrado). Al eliminar una actividad de cifrado, la aplicación bloquea el acceso a cualquier recurso de archivos de la red por parte de la máquina de origen.

Bloqueo del acceso a los hosts con actividades sospechosas. Funcionalidad que bloquea el acceso del equipo a carpetas de redes compartidas de un servidor protegido si dicho equipo muestra actividad maliciosa al ejecutar tareas de protección en tiempo real o anticifrado.

Protección proactiva frente a malware. Las tecnologías de protección antimalware avanzadas incluyen un analizador heurístico y pueden identificar programas maliciosos con un alto nivel de precisión, incluso si su firma no se ha añadido todavía a las bases de datos antimalware.

Análisis de las áreas fundamentales del sistema operativo. Se puede ejecutar una tarea exclusiva para analizar las áreas del sistema operativo más expuestas a las infecciones. Por ejemplo, si se analizan archivos de ejecución automática, se puede evitar que el malware se inicie al arrancar el sistema, así como detectar procesos ocultos.

Ajustes de análisis flexibles. La configuración de análisis de archivos permite al administrador:

- Excluir determinados procesos del análisis
- Configurar el nivel de protección
- Especificar los tipos de archivo que siempre deben analizarse y los que deben omitirse
- Predefinir las respuestas ante objetos infectados o sospechosos en función del tipo de amenaza

Este enfoque permite optimizar la carga del servidor y garantiza una gestión flexible de la seguridad de la red empresarial.

Protección de servidores virtuales y de terminales. La aplicación ofrece protección para Microsoft Terminal Services y los servidores Citrix XenApp, y garantiza que los usuarios finales que trabajan en los modos de edición de aplicaciones o escritorio estén constantemente protegidos y reciban notificaciones de los eventos. También son compatibles los entornos Hyper-V, XenDesktop y VMware™.

Compatibilidad con clústeres. La aplicación es idónea para una compleja arquitectura de clústeres de servidor, ya que protege tanto los discos locales como los discos compartidos del clúster, de los que se encarga actualmente el nodo protegido.

Alto rendimiento

Escalabilidad. Para los servidores con varios procesadores, el administrador puede especificar el número de subprocesos de antimalware para garantizar un procesamiento rápido de las solicitudes de servidor.

Equilibrio de carga. Los recursos pueden asignarse entre Kaspersky Security for Windows Server y otras aplicaciones en función de prioridades previamente establecidas; el análisis antimalware también puede ejecutarse en un segundo plano.

Selección de procesos fiables. El administrador puede excluir del análisis aquellos procesos que sean seguros, como la realización de copias de seguridad de datos o la desfragmentación de la unidad de disco duro, con el objetivo de optimizar el rendimiento.

Funcionamiento continuo del servidor. Kaspersky Security for Windows Server no requiere un servidor para reiniciarse cuando la protección antimalware se instale o se actualice.

Administración flexible

Selección de herramientas de gestión. La aplicación puede gestionarse directamente, o bien de forma remota a través de Microsoft Management Console, Kaspersky Security Center o la línea de comandos. La última versión del producto proporciona una intuitiva interfaz gráfica para Microsoft Management Console.

Herramientas de instalación y gestión fáciles de utilizar. Kaspersky Security Center es una consola de administración que admite la instalación y configuración remotas de la aplicación de manera simultánea en varios servidores y que, además, ayuda a gestionar su funcionamiento y recibe actualizaciones y notificaciones.

Control sobre los privilegios de administrador. La aplicación permite la asignación de varios niveles de privilegios a cada administrador del servidor, lo que facilita el cumplimiento de cualquier requisito de cumplimiento de IT específico de un departamento o de seguridad interna.

Configuración flexible de los tiempos de análisis. Configure fácilmente los periodos de inicio y finalización de los análisis para reducir al mínimo las interrupciones y aumentar la disponibilidad de los recursos del servidor.

Sistema de notificaciones. La aplicación admite las notificaciones de una amplia lista de eventos al administrador a través del servicio de mensajería o del correo electrónico. La aplicación tiene integrado Simple Network Management Protocol (SNMP) y puede funcionar con Microsoft Operations Manager (MOM); además, el administrador puede supervisar el funcionamiento de la aplicación a través de los registros de eventos de Microsoft Windows o Kaspersky Security Center.

Cómo comprarlo

Kaspersky Security for Windows Server puede adquirirse como parte integrante de:

- Kaspersky Endpoint Security for Business – Select (control de inicio de las aplicaciones excluido)
- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

También se puede adquirir como parte integrante de una solución adaptada: Kaspersky Security for File Server y Kaspersky Security for Storage.

La lista completa de partners de Kaspersky Lab está disponible en: www.kaspersky.com/buyoffline.

Para obtener más información, visite: www.kaspersky.es

REQUISITOS DEL SISTEMA

- Kaspersky Security for Windows Server se ha diseñado para servidores con las versiones de 32 bits o 64 bits de Microsoft Windows:
 - Microsoft Windows Server 2008/2008 R2 x86/x64 Standard/Enterprise/Datacenter SP1 o posterior (incluido el modo Core)
 - Microsoft Windows Hyper-V Server 2008 R2 SP1 o posterior
 - Microsoft Windows Server 2012/2012 R2 Essentials/Standard/Foundation/Datacenter (incluido el modo Core)
 - Microsoft Windows Hyper-V® Server 2012/2012 R2
- Kaspersky Security for Windows Server se puede instalar en los siguientes servidores de terminal
 - Microsoft Remote Desktop Services basados en Windows 2008 Server
 - Microsoft Remote Desktop Services basados en Windows 2008/2012/2012 R2 Server
 - Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6
 - Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6.

Consola de gestión:

- Microsoft Windows XP SP2/Vista®/7/8/10 Enterprise/Professional x86/x64
- Microsoft Windows Server 2008/2008 R2 Standard/Enterprise/Datacenter SP1 o posterior x64
- Microsoft Windows Server 2012/2012 R2 Essentials/Standard/Foundation/Datacenter x64
- Microsoft Windows Hyper-V Server 2008 R2 SP1/2012/2012 R2 o posterior x64

Requisitos mínimos de hardware:

- Procesador – Intel® Pentium® IV
- Velocidad de procesamiento de 2,4 GHz
- RAM: 512 MB
- Subsistema de disco duro: – 1 disco IDE

