



Kaspersky® Security for Windows Servers

Seguridad resiliente para servidores Windows

Las máquinas basadas en Windows Server pueden alojar una gran variedad de tareas, incluidas muchas que pueden ser fundamentales para su organización. Por lo tanto, es importante que no haya ningún incidente de seguridad o problema de rendimiento que interrumpa el funcionamiento continuo de los servidores. La protección debe darse como una solución que repercuta muy poco en el uso de los recursos y en la estabilidad de los sistemas y que garantice, a la vez, la seguridad de los diversos escenarios de negocio que los servidores pueden estar apoyando.

Kaspersky Security for Windows Servers proporciona una seguridad de última generación resiliente para servidores en todas las funciones que desempeñen. Para conseguir la rentabilidad máxima, se puede activar la funcionalidad adecuada mediante diferentes licencias según el tipo de tarea que se aborde.

Información destacada

- **Perfecto para escenarios primordiales**
Altamente adaptable a diferentes roles de servidor, incluidos escenarios fundamentales, gracias a una amplia gama de componentes de protección, junto con unos menores requisitos de mantenimiento (tales como la necesidad de reiniciar).
- **Adecuado para sistemas antiguos**
Bajo impacto en el rendimiento para entornos antiguos con recursos de hardware limitados. Es compatible con Windows Server 2003 (que ya no soporta Microsoft).
- **Solución certificada**
Se ha certificado la compatibilidad de la aplicación con las plataformas de virtualización y los sistemas operativos.

VENTAJAS

Protección más premiada, más reconocida y más apreciada

Kaspersky Security for Windows Servers se basa en tecnologías que reconocen de forma constante los analistas, posiciones de podio en las pruebas independientes y la satisfacción de nuestros clientes. Una confirmación independiente de que nos puede confiar sus servidores fundamentales.

Versatilidad excepcional

Kaspersky Security for Windows Servers es adecuado para una amplia gama de actividades de servidor y tipos de uso, incluida la protección de los servidores de archivos, el almacenamiento de redes y otros elementos clave de la infraestructura corporativa para asegurar su funcionamiento sin problemas y seguro.

Adaptado a la nube y preparado para la nube

Kaspersky Security for Windows Servers está diseñado para proteger tanto a los servidores físicos como a los servidores virtualizados, permitiendo ejecutar cargas de trabajo de servidor de forma segura en su infraestructura de nube híbrida; on premise, en el centro de datos o en las nubes públicas.

Gestión centralizada: ahorro de tiempo y dinero

Kaspersky Security Center ofrece una consola unificada para administrar la seguridad. Si su objetivo fundamental es la facilidad de uso o el control más detallado sobre todos los aspectos de su infraestructura desde una vista de panel único, puede ajustar los detalles específicos de su seguridad corporativa a la configuración y requisitos de sus sistemas y reducir los costes operativos.

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:

- Windows Server 2003/2003 R2 SP2
- Windows Server 2008/2008 R2 SP1 o posterior (incluido el modo Core)
- Windows Server 2012/2012 R2 (incluido el modo Core)
- Windows Server 2016 (incluido el modo Core)
- Small Business Server 2008/2011
- Windows MultiPoint Server 2011
- Windows Hyper-V Server 2008 R2 SP1 o posterior/2012/2012 R2/2016
- Windows Storage Server 2012/ 2012 R2/2016

Kaspersky Security for Windows Server se puede instalar en los siguientes servidores de terminal

- Microsoft Remote Desktop Services basados en Windows 2008/2008 R2/2012/2012 R2/2016 Server
- Citrix XenApp 6.0, 6.5, 7.0, 7.5, 7.6, 7.15
- Citrix XenDesktop 7.0, 7.1, 7.5, 7.6, 7.15

Kaspersky Security 10.1 for Windows Servers puede utilizarse para proteger los siguientes dispositivos de almacenamiento conectados a la red:

NetApp® con uno de los siguientes sistemas operativos:

- Data ONTAP® 7.x y Data ONTAP 8.x en modo de 7 modos
- Data ONTAP 8.2.1 o posterior en modo de clúster

Dell EMC Celerra/VNX con el siguiente software:

- EMC DART 6.0.36 o superior
- Celerra Anti-Virus Agent (CAVA) 4.5.2.3 o superior
- Dell EMC Isilon con OneFS 7.0 o posterior

Hitachi NAS en una de las siguientes plataformas:

- HNAS 4100
- HNAS 4080
- HNAS 4060
- HNAS 4040
- HNAS 3090
- HNAS 3080

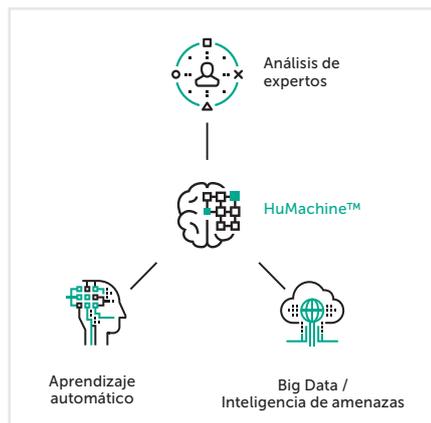
IBM serie NAS IBM System Storage serie N

Serie de sistemas NAS de Oracle serie Oracle ZFS Storage Appliance

Dell NAS en la plataforma Dell Compellent FS8600

Requisitos mínimos de hardware:

- Procesador: 1,4 GHz de un solo núcleo
- RAM: 1 GB
- Subsistema de disco duro: 4 GB



Características de la herramienta

Protección de última generación contra malware y mucho más. Kaspersky Security for Windows Servers se basa en nuestra exclusiva plataforma de protección a varios niveles, con el respaldo del aprendizaje automático y la experiencia humana, permitiendo la detección de todas las formas de ataque de malware, incluidas las amenazas avanzadas, sofisticadas y emergentes. Kaspersky Security Network (KSN) ofrece una respuesta rápida a las nuevas amenazas y mejora el rendimiento en materia de protección y reduce el riesgo de falsos positivos a casi cero.

Protección del almacenamiento y carpetas compartidas contra malware cifrado. Un único componente anticryptor bloquea el cifrado de archivos en los recursos compartidos originado por un proceso malicioso que se ejecuta en una máquina diferente de la red. Esta funcionalidad se aplica tanto a sistemas de almacenamiento de Windows y como de NetApp

NOVEDAD: Prevención de exploits. La potente tecnología de prevención de exploits supervisa los procesos protegidos para evitar que los exploits ataquen las vulnerabilidades a las que no se han aplicado parches e incluso de día cero en aplicaciones y componentes del sistema.

NOVEDAD: Refuerzo de la seguridad de los sistemas. La adopción de un escenario de denegación predeterminada, mediante el control de inicio de las aplicaciones, optimiza la resiliencia de su sistema para las fugas de datos. Al prohibir la ejecución de cualquier aplicación que no sean determinados programas, servicios y componentes del sistema de confianza, puede bloquear automáticamente la mayoría de las formas de malware completamente. Implementado junto con el control de dispositivos de Kaspersky, su ejecución en modo de denegación predeterminada también evita el almacenamiento no solicitado, lo que reduce considerablemente su superficie de ataque y aumenta la seguridad del servidor.

NOVEDAD: Integridad de los sistemas. Garantizar que los componentes y procesos (así como aplicaciones) críticos del sistema permanecen intactos es esencial tanto para el buen funcionamiento de los servidores como para la seguridad de los datos confidenciales con los que están trabajando. Componentes de Kaspersky Security for Windows Server, como la supervisión de la integridad de archivos y la inspección de registros no solo identifican cambios no deseados en sus sistemas, también pueden detectar diferentes indicadores de una brecha de seguridad, en cumplimiento con las regulaciones, incluidas PCI/DSS.

NOVEDAD: Seguridad del tráfico. Kaspersky Security for Windows Server ahora filtra el tráfico para detectar el malware, verifica los enlaces web y proporciona control de recursos web, basándose en categorías de Kaspersky, para cualquier sistema externo que admita el protocolo ICAP, incluidos servidores proxy y dispositivos de almacenamiento.

Protección para servidores de terminal. Se puede proteger una amplia gama de entornos de acceso remoto, incluidos Microsoft Remote Desktop Services y Citrix XenApp/Xen Desktop.

NOVEDAD: Gestión del firewall de Windows. Los firewalls del servidor de Windows pueden configurarse directamente desde Kaspersky Security Center, lo que permite una gestión de firewalls local a través de una única consola unificada.

NOVEDAD: Integración con SIEM. Kaspersky Security for Windows Server se integra con los principales sistemas de SIEM, convierte los eventos en registros de aplicación en formatos admitidos por el servidor syslog, para que se puedan reconocer e importar en el SIEM. La aplicación admite la conversión tanto en formatos JSON como en datos estructurados.

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
- Kaspersky Hybrid Cloud Security

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

www.kaspersky.es

© 2018 Kaspersky Lab Iberia, España. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.