▶ KASPERSKY SECURITY FOR STORAGE

Protección de alto rendimiento para los sistemas de almacenamiento EMC, NetApp e Hitachi

INTRODUCCIÓN

El malware letal puede propagarse por la empresa a una velocidad terrorífica, ya que se aprovecha de la interoperabilidad de las redes modernas. En un panorama donde cada vez hay más amenazas, el hecho de guardar un solo archivo infectado sin saberlo puede suponer un riesgo inmediato para todos los nodos de la red.

Kaspersky Security for Storage proporciona una protección sólida, de alto rendimiento y escalable para los valiosos datos corporativos confidenciales que se ubican en sistemas de almacenamiento como EMC Isilon™, Celerra/VNX™, NetApp, Hitachi e IBM.

- Protección antimalware en tiempo real para EMC, NetApp, Hitachi e IBM
- Compatible con los protocolos de agente CAVA, RPC e ICAP
- Compatible con tareas exclusivas para el análisis de áreas críticas del sistema
- Configuración de análisis flexible
- Escalable y a prueba de fallos
- Uso adaptable de los recursos del sistema
- Protección para servidores de terminal
- Compatibilidad con clústeres de servidor
- Certificación de compatibilidad con VMware
- Optimización de análisis antivirus iSwift e iChecker
- Gestión con Kaspersky Security Center
- Informes de rendimiento de aplicaciones
- Compatible con la gestión de red SNMP/MOM

INFORMACIÓN DESTACADA

POTENTE PROTECCIÓN ANTIMALWARE EN TIEMPO REAL

Protección proactiva e ininterrumpida para soluciones de almacenamiento conectado a la red (NAS). El potente motor antimalware de Kaspersky analiza todos los archivos utilizados o modificados en busca de todo tipo de malware como virus, gusanos y troyanos. El análisis heurístico avanzado identifica tanto amenazas nuevas como desconocidas.

RENDIMIENTO OPTIMIZADO

El análisis de alto rendimiento, con tecnología de análisis optimizada y configuración flexible de excepciones, ofrece la máxima protección a la vez que minimiza el impacto en el rendimiento del sistema.

FIABILIDAD

Gracias a una sencilla arquitectura con componentes unificados, diseñados y creados para trabajar en perfecta sintonía, se logra una tolerancia ante los errores excepcional. El resultado es una solución estable y resistente que, en caso de que se produzca un cierre forzoso, se reinicia automáticamente para proporcionar una protección continua y fiable.

FACILIDAD DE ADMINISTRACIÓN

Los servidores están instalados de forma remota y cuentan con protección inmediata que no necesita ningún reinicio. Además, se administran a través de una sencilla e intuitiva consola central, Kaspersky Security Center, junto con otras soluciones de seguridad de Kaspersky.

FUNCIONES

SEGURIDAD PROACTIVA E ININTERRUMPIDA
El motor de análisis antimalware de Kaspersky líder en el sector y diseñado por expertos mundiales en inteligencia frente amenazas, ofrece una protección proactiva contra amenazas emergentes y potenciales mediante el uso de tecnologías inteligentes que mejoran el proceso de detección.

ACTUALIZACIONES AUTOMÁTICAS
Las bases de datos antimalware se actualizan automáticamente sin interrumpir el análisis, lo que garantiza una protección continua y una reducción de la carga de trabajo del administrador.

PROCESOS EXCLUIDOS Y ZONAS DE CONFIANZA
El rendimiento de los análisis puede afinarse mediante la creación de "zonas de confianza" que, junto con formatos de archivo definidos y procesos como la copia de seguridad de los datos, pueden excluirse del análisis.

ANÁLISIS DE ARCHIVOS DE EJECUCIÓN AUTOMÁTICA
Para proporcionar una mayor protección al servidor, pueden realizarse análisis de sistemas operativos y de archivos de ejecución automática con el fin de evitar que el malware se ejecute durante el inicio del sistema.

ANÁLISIS FLEXIBLE PARA OPTIMIZAR EL RENDIMIENTO
Reduce el tiempo del análisis y de configuración y equilibra la carga del sistema, de forma que se optimiza el rendimiento del servidor. El administrador puede especificar y controlar la profundidad, amplitud y duración del análisis definiendo qué tipos de archivos y qué áreas deben incluirse en el mismo. También pueden programarse análisis a petición en periodos de baja actividad del servidor.

PROTECCIÓN DE SOLUCIONES HSM Y DAS
Al ser compatible con los modos de análisis sin conexión, ofrece una protección efectiva de los sistemas de gestión de almacenamiento jerárquico (HSM). La protección del almacenamiento de conexión directa (DAS) también ayuda a promover el uso de soluciones de almacenamiento de bajo coste.

COMPATIBILIDAD CON TODOS LOS PRINCIPALES PROTOCOLOS
Kaspersky Security for Storage es compatible con los principales protocolos utilizados por diferentes sistemas de almacenamiento: agente CAVA, RPC e ICAP.

PROTECCIÓN DE SISTEMAS VIRTUALES Y SERVIDORES DE TERMINAL
La seguridad flexible incluye protección para sistemas operativos virtuales (invitados) en entornos virtuales de Hyper-V y VMware, así como infraestructuras de terminales de Microsoft y Citrix.

ADMINISTRACIÓN

INSTALACIÓN Y GESTIÓN CENTRALIZADAS
La instalación, configuración y administración remotas, incluidas las notificaciones, actualizaciones y generación de informes flexible, se gestionan a través de la intuitiva herramienta Kaspersky Security Center. Si lo prefiere, también tiene a su disposición la gestión mediante línea de comandos.

CONTROL SOBRE LOS PRIVILEGIOS DE ADMINISTRADOR
El hecho de que cada administrador del servidor pueda tener asignados diferentes niveles de privilegios posibilita el cumplimiento de determinadas políticas de seguridad de IT corporativas.

INFORMES FLEXIBLES
Los informes pueden generarse en formato gráfico o mediante la consulta de los registros de eventos de Microsoft Windows® o de Kaspersky Security Center. Las herramientas de búsqueda y filtrado proporcionan un acceso rápido a los datos de registros de gran volumen.

REQUISITOS DEL SISTEMA

HARDWARE:
- Sistemas compatibles con x86 en una configuración con uno o varios procesadores
- Sistemas compatibles con x86/x64 con uno o varios procesadores

ESPACIO EN DISCO:
- Para la instalación de todos los componentes de la aplicación: 70 MB
- Para el almacenamiento de objetos en cuarentena o con copia de seguridad: 400 MB (recomendado)
- Para el almacenamiento de registros: 1 GB (recomendado)
- Para el almacenamiento de bases de datos: 2 GB (recomendado)

CONFIGURACIÓN MÍNIMA:
- Procesador: 1 núcleo con una velocidad de procesamiento de 1,4 GHz
- RAM: 1 GB
- 4 GB de espacio libre en el disco duro

CONFIGURACIÓN RECOMENDADA:
- Procesador: 4 núcleos con una velocidad de procesamiento de 2,4 GHz
- RAM: 2 GB
- 4 GB de espacio libre en el disco duro

SOFTWARE:
- Microsoft Windows Server 2003/2003 R2 x86/x64 Standard/ Enterprise Edition
- Microsoft Windows Server 2008/2008 R2 x86/x64 Standard/ Enterprise/Datacenter Edition (incluido el modo Core)
- Microsoft Windows Server 2012/20012 R2 Essentials/ Standard/Foundation/Datacenter (incluido el modo Core)
- Microsoft Windows Hyper-V Server 2008 R2
- Microsoft Windows Hyper-V Server 2012/2012 R2

SERVIDORES:
- Microsoft Terminal Services basados en Windows 2003 Server
- Microsoft Terminal Services basados en Windows 2008 Server
- Microsoft Terminal Services basados en Windows 2012/2012 R2 Server
- Citrix Presentation Server 4.0, 4.5
- Citrix XenApp 4.5, 5.0, 6.0, 6.5
- Citrix XenDesktop 7.0, 7.1, 7.5

PLATAFORMAS DE ALMACENAMIENTO:
Almacenamiento de archivos EMC Celerra/VNX:
- EMC DART 6.0.36 o posterior
- Celerra Antivirus Agent (CAVA) 4.5.2.3 o posterior

Requisitos de almacenamiento de EMC Isilon:
- EMC Isilon OneFS

Requisitos de almacenamiento de NetApp:
- Data ONTAP 7.x и Data ONTAP 8.x en régimen de 7 modos
- Data ONTAP 8.2.1 o posterior en régimen de modo de clúster

Requisitos de almacenamiento de IBM:
- IBM System Storage serie N

vmware READY

Windows Server 2012 R2 Certified

KS-Storage/Versión 2/Enero de 2015/Global

KASPERSKY lab