▶ KASPERSKY SECURITY FOR STORAGE

Proteção de alto desempenho para armazenamentos EMC, NetApp e Hitachi

VISÃO GERAL

Malware letais podem se disseminar para toda a organização em velocidade assustadora, aproveitando-se da interoperabilidade das redes modernas. No crescente cenário de ameaças, um único arquivo infectado inconscientemente colocado em armazenamento pode expor todos os nós da rede a risco imediato.

O Kaspersky Security for Storage proporciona proteção escalonável, robusta e de alto desempenho para dados corporativos sigilosos e valiosos armazenados em sistemas de armazenamento EMC Isilon™, Celerra e VNX™, NetApp, Hitachi e IBM.

- Proteção antimalware em tempo real para EMC, NetApp, Hitachi e IBM
- Dá suporte ao agente CAVA, RPC e protocolos ICAP
- Dá suporte a tarefas exclusivas de verificação de áreas críticas do sistema
- Configuração flexível da verificação
- Escalonável e tolerante a falhas
- Utilização adaptável dos recursos do sistema
- Proteção do servidor de terminal
- Suporte a clusters de servidores
- Compatibilidade certificada com o VMware
- Inclui otimização de verificações antivírus iSwift e iChecker
- Gerenciamento pelo Kaspersky Security Center
- Relatórios de desempenho de aplicativos
- Dá suporte ao gerenciamento de rede SNMP/MOM

DESTAQUES

AVANÇADA PROTEÇÃO ANTIMALWARE EM TEMPO REAL

Proteção proativa para soluções NAS (Network Attached Storage). O avançado mecanismo antimalware da Kaspersky verifica todos os arquivos executados ou modificados em relação a todas as formas de malware, incluindo vírus, worms e cavalos de Troia. A análise heurística avançada identifica ameaças novas e desconhecidas.

DESEMPENHO OTIMIZADO

A verificação de alto desempenho, com tecnologia de verificação otimizada e configurações de exclusão flexíveis, oferece máxima proteção e minimiza o impacto sobre o desempenho do sistema.

CONFIÁVEL

Uma tolerância a falhas excepcional é obtida através de uma arquitetura simples, utilizando componentes unificados criados e construídos para trabalharem em conjunto com perfeição. O resultado é uma solução estável e resistente que, quando desativada, será reiniciada automaticamente para uma proteção confiável e contínua.

FÁCIL ADMINISTRAÇÃO

Os servidores "prontos para usar" são instalados e protegidos remotamente, sem reinicializações, e administrados em conjunto através de um console central simples e intuitivo - o Kaspersky Security Center - junto com as outras soluções de segurança da Kaspersky.

RECURSOS

SEGURANÇA PROATIVA
O Kaspersky, líder do setor de mecanismos de verificação antimalware, desenvolvido por especialistas em inteligência de ameaças de todo o mundo, fornece proteção proativa contra ameaças emergentes e potenciais utilizando tecnologias inteligentes para uma detecção aprimorada.

ATUALIZAÇÕES AUTOMÁTICAS
Os bancos de dados antimalware são atualizados automaticamente, sem interromper a verificação, garantindo a proteção contínua e minimizando a carga de trabalho do administrador.

PROCESSOS DE EXCLUSÃO E ZONAS CONFIÁVEIS
O desempenho da verificação pode ser ajustado com o uso de "zonas confiáveis" que, juntamente com formatos de arquivo e processos, como backups de dados, podem ser excluídos da verificação.

VERIFICAÇÃO DE OBJETOS COM EXECUÇÃO AUTOMÁTICA
Para maior proteção do servidor, é possível realizar verificações do sistema operacional e dos arquivos com execução automática para evitar que malwares sejam inicializados durante a reinicialização do sistema.

VERIFICAÇÃO FLEXÍVEL PARA UM DESEMPENHO OTIMIZADO
Reduz o tempo de verificação e configuração e promove o balanceamento de carga, ajudando a otimizar o desempenho do servidor. O administrador pode especificar e controlar a profundidade, amplitude e duração da atividade de verificação, definindo quais são os tipos de arquivos e as áreas que devem ser verificados. A verificação por demanda pode ser programada para períodos de baixa atividade do servidor.

PROTEGE SOLUÇÕES HSM E DAS
Dá suporte aos modos de verificação off-line para proteção eficiente dos sistemas de Gerenciamento de Armazenamento Hierárquico (HSM). A proteção DAS (Direct Attached Storage) também ajuda a promover a utilização de soluções de armazenamento de baixo custo.

SUPORTE PARA TODOS OS PRINCIPAIS PROTOCOLOS
O Kaspersky Security for Storage suporta os principais protocolos usados por diferentes sistemas de armazenamento: agente CAVA RPC e ICAP.

PROTEÇÃO DE SISTEMAS VIRTUAIS E SERVIDORES DE TERMINAL
A segurança flexível inclui proteção para sistemas operacionais virtuais (convidados) em ambientes virtuais Hyper-V e VMware e para infraestruturas de terminais Microsoft e Citrix.

SIMPLIFICADA

INSTALAÇÃO E GERENCIAMENTO CENTRALIZADOS
A instalação, a configuração e o gerenciamento remotos, incluindo notificações, atualizações e relatórios flexíveis, são administrados através do intuitivo Kaspersky Security Center. O gerenciamento por linha de comando também está disponível, se preferido.

CONTROLE SOBRE PRIVILÉGIOS DE ADMINISTRADOR
Níveis de privilégios diferentes podem ser atribuídos a cada administrador do servidor, ajudando a manter a conformidade com as políticas corporativas específicas da segurança de TI.

RELATÓRIOS FLEXÍVEIS
São fornecidos por meio de relatórios gráficos ou revisões dos logs de eventos do Microsoft Windows® ou do Kaspersky Security Center. Ferramentas de pesquisa e de filtragem proporcionam acesso rápido a dados em logs de grande volume.

REQUISITOS DO SISTEMA

HARDWARE:
- Sistemas compatíveis com x86 com um ou vários processadores
- Sistemas compatíveis com x86-64 com um ou vários processadores

ESPAÇO EM DISCO:
- Para a instalação de todos os componentes do aplicativo: 70 MB
- Para o armazenamento de objetos em quarentena ou backup: 400 MB (recomendado)
- Para o armazenamento de logs: 1 GB (recomendado)
- Para o armazenamento de bancos de dados: 2 GB (recomendado)

CONFIGURAÇÃO MÍNIMA:
- Processador - 1 núcleo; velocidade de processamento 1,4 GHz
- RAM: 1 GB
- 4 GB de espaço disponível no disco rígido

CONFIGURAÇÃO RECOMENDADA:
- Processador - 4 núcleos; velocidade de processamento 2,4 GHz
- RAM: 2 GB
- 4 GB de espaço disponível no disco rígido

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

SERVIDORES:
- Serviços de Terminal da Microsoft com base no Windows Server 2003;
- Serviços de Terminal da Microsoft com base no Windows Server 2008;
- Serviços de Terminal da Microsoft com base no Windows Server 2012/ 2012 R2;
- 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 ARMAZENAMENTO:
Armazenamento de arquivos EMC Celerra/VNX:
- EMC DART 6.0.36 ou superior;
- Celerra Antivirus Agent (CAVA) 4.5.2.3 ou superior.

Requisitos para armazenamento EMC Isilon:
- EMC Isilon OneFS.

Requisitos de armazenamento do NetApp:
- Data ONTAP 7.x и Data ONTAP 8.x em 7-mode;
- Data ONTAP 8.2.1 ou superior em cluster-mode.

Requisitos para armazenamentos IBM:
- Armazenamento do sistema IBM série N.

vmware READY

Windows Server 2012 R2 Certified

KS-Storage/Version 2/January 2015/Global

KASPERSKY lab