▶ KASPERSKY SECURITY FOR STORAGE

Proteção de alto desempenho para armazenamentos EMC, NetApp e Hitachi

VISÃO GERAL

O malware letal pode espalhar-se por uma organização a uma velocidade aterradora, tirando partido da interoperabilidade das redes modernas. Num cenário de ameaças em constante crescimento, um único ficheiro infetado e inconscientemente armazenado pode expor todos os nós da rede a um risco imediato.

O Kaspersky Security for Storage oferece proteção robusta, de alto desempenho e escalável para dados empresariais valiosos e sensíveis mantidos em sistemas de armazenamento EMC Isilon™, Celerra e VNX™, NetApp, Hitachi e IBM.

- Proteção anti-malware em tempo real para EMC, NetApp, Hitachi e IBM
- Suporta os protocolos CAVA agent, RPC e ICAP
- Suporta tarefas dedicadas para verificações de áreas críticas do sistema
- Configuração flexível da verificação
- Escalável e com tolerância a falhas
- Utilização adaptável dos recursos do sistema
- Proteção de servidores de terminais
- Suporte para clusters de servidores
- Compatibilidade certificada com VMware
- Inclui otimização de verificação antivírus iSwift e iChecker
- Gestão Kaspersky Security Center
- Relatório do desempenho da aplicação
- Suporta a gestão de rede SNMP/MOM

DESTAQUES

PROTEÇÃO ANTI-MALWARE PODEROSA E EM TEMPO REAL

Proteção pró-ativa "sempre ligada" para soluções de armazenamento ligadas à rede (NAS). O poderoso motor anti-malware da Kaspersky verifica todos os ficheiros executados ou modificados relativamente a todas as formas de malware, incluindo vírus, worms e Trojans. A análise heurística avançada identifica até ameaças novas e desconhecidas.

DESEMPENHO OTIMIZADO

A verificação de alto desempenho, com tecnologia de verificação otimizada e definições de exceções flexíveis, oferece a máxima proteção, ao mesmo tempo que minimiza o impacto no desempenho do sistema.

FIÁVEL

A excecional tolerância a falhas é alcançada através de uma arquitetura simples, ao utilizar componentes unificados concebidos e construídos para trabalharem em conjunto sem falhas. O resultado é uma solução estável e resistente que, se forçada a encerrar, irá reiniciar-se automaticamente, para uma proteção fiável e contínua.

FÁCIL DE ADMINISTRAR

Os servidores são imediatamente instalados e protegidos remotamente, sem qualquer reinício, e são administrados em conjunto através de uma consola central simples e intuitiva – o Kaspersky Security Center – juntamente com as suas outras soluções de segurança Kaspersky.

FUNCIONALIDADES

SEGURANÇA PRÓ-ATIVA, SEMPRE LIGADA
O motor de verificação anti-malware líder da indústria da Kaspersky, criado pelos especialistas mundiais em informação de ameaças, proporciona proteção pró-ativa contra ameaças emergentes e potenciais ao utilizar tecnologias inteligentes para deteção melhorada.

ATUALIZAÇÕES AUTOMÁTICAS
As bases de dados de anti-malware são atualizadas automaticamente, sem qualquer interrupção da verificação, garantindo uma proteção contínua e minimizando a carga de trabalho do administrador.

PROCESSOS EXCLUÍDOS E ZONAS DE CONFIANÇA
O desempenho da verificação pode ser ajustado ao criar "zonas de confiança" que, juntamente com formatos de ficheiro definidos e processos como cópias de segurança de dados, podem ser excluídas da verificação.

VERIFICAÇÃO DE OBJETOS DE EXECUÇÃO AUTOMÁTICA
Para uma maior proteção dos servidores, as verificações de ficheiros de execução automática e sistemas operativos podem ser realizadas para evitar a execução de malware durante o arranque do sistema.

VERIFICAÇÃO FLEXÍVEL PARA UM DESEMPENHO OTIMIZADO
Reduz o tempo de verificação e configuração e promove o equilíbrio de cargas, ajudando a otimizar o desempenho do servidor. O administrador pode especificar e controlar a profundidade, abrangência e o momento da atividade de verificação, definindo que tipos de ficheiro e áreas têm de ser verificadas. A verificação a pedido pode ser agendada para períodos de baixa atividade do servidor.

PROTEGE SOLUÇÕES HSM E DAS
Suporta modos de verificação offline para uma proteção eficaz de sistemas Hierarchical Storage Management (HSM). A proteção de armazenamento de acesso direto (DAS) também ajuda a promover a utilização de soluções de armazenamento de baixo custo.

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

PROTEÇÃO DE SISTEMAS VIRTUAIS E SERVIDORES DE TERMINAIS
A segurança flexível inclui proteção para sistemas operativos virtuais (convidados) em ambientes virtuais Hyper-V e VMwares, bem como para infraestruturas de terminais Microsoft e Citrix.

ADMINISTRAÇÃO

INSTALAÇÃO E GESTÃO CENTRALIZADAS
A instalação, configuração e administração remotas, incluindo notificações, atualizações e relatórios flexíveis, são processadas através do intuitivo Kaspersky Security Center. A gestão de linha de comandos também está disponível, se preferível.

CONTROLO DOS PRIVILÉGIOS DO ADMINISTRADOR
Diferentes níveis de privilégios podem ser atribuídos a cada administrador de servidor, permitindo a conformidade com políticas de segurança de TI empresariais específicas.

CRIAÇÃO DE RELATÓRIOS FLEXÍVEL
Os relatórios podem ser entregues através de relatórios gráficos ou através da consulta dos registos de eventos do Microsoft Windows® ou do Kaspersky Security Center. Ferramentas de pesquisa e filtragem fornecem acesso rápido a dados em registos de grande volume.

REQUISITOS DO SISTEMA

HARDWARE:
- Sistemas compatíveis com x86 numa configuração de processador único ou de vários processadores
- Sistemas compatíveis com x86-64 em processador único ou vários processadores

ESPAÇO EM DISCO:
- Para a instalação de todos os componentes da aplicação: 70 MB
- Para a colocação de objetos em quarentena ou criação de cópias de segurança: 400 MB (recomendado)
- Para o armazenamento de registos: 1 GB (recomendado)
- Para o armazenamento de bases de dados: 2 GB (recomendado)

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

CONFIGURAÇÃO RECOMENDADA:
- Processador – 4 núcleos; velocidade de processamento de 2,4 GHz
- RAM: 2 GB
- 4 GB de espaço livre 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 Core mode)
- Microsoft Windows Server 2012/20012 R2 Essentials/ Standard/Foundation/Datacenter (incluindo Core mode)
- 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 2003 Server;
- Serviços de Terminal da Microsoft com base no Windows 2008 Server;
- Serviços de Terminal da Microsoft com base no 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 ARMAZENAMENTO:
Armazenamento de ficheiros EMC Celerra/VNX:
- EMC DART 6.0.36 ou superior;
- Celerra Antivirus Agent (CAVA) 4.5.2.3 ou superior.

Requisitos para o sistema de armazenamento EMC Isilon:
- EMC Isilon OneFS.

Requisitos para armazenamento em NetApp:
- Data ONTAP 7.x e Data ONTAP 8.x em regime de 7 modos;
- Data ONTAP 8.2.1 ou superior em regime de modo de cluster.

Requisitos para sistemas de armazenamento IBM:
- IBM System Storage N series.

vmware READY

Windows Server 2012 R2 Certified

KS-Storage/Version 2/January 2015/Global

KASPERSKY lab