▶ KASPERSKY SECURITY FOR COLLABORATION

Proteção e controlo de dados para plataformas de colaboração, incluindo farms de SharePoint.

A plataforma que utiliza para partilhar ficheiros e informações também constitui o sistema de trânsito ideal e rápido para malware perigoso e outras ameaças de TI.
Para garantir a segurança e um bom ambiente de trabalho partilhado, a Kaspersky Lab desenvolveu uma solução que combina facilidade de gestão com proteção premium em tempo real contra ataques de malware e fugas de dados confidenciais.

- Motor anti-malware premiado
- Pesquisa e proteção de dados confidenciais
- Controlo de acesso a dados
- Proteção em tempo real baseada na nuvem – Kaspersky Security Network
- Filtragem de conteúdo e ficheiros
- Proteção anti-phishing
- Cópia de segurança e armazenamento
- Gestão centralizada e flexível
- Consola de administrador intuitiva

DESTAQUES

SEGURANÇA COMPLETA PARA A SUA PLATAFORMA SHAREPOINT.

Se utiliza o Microsoft SharePoint Server sabe que, como todo o conteúdo é armazenado numa base de dados SQL, as soluções tradicionais para terminais não são adequadas para este caso. O Kaspersky Security for Collaboration aplica uma proteção anti-malware avançada e premiada em toda a farm do SharePoint e todos os respetivos utilizadores. Através do Kaspersky Security Network apoiado pela nuvem é fornecida uma proteção potente contra ameaças conhecidas, desconhecidas e avançadas, enquanto a tecnologia anti-phishing protege contra ameaças baseadas na Web a dados colaborativos.

PREVENÇÃO CONTRA FUGA DE DADOS CONFIDENCIAIS.

Para controlar e proteger a circulação de dados confidenciais, esses dados devem primeiro ser identificados. Utilizando categorias de dados e dicionários pré-instalados ou personalizados, o Kaspersky Security for Collaboration verifica todos os documentos colocados nos servidores SharePoint, procurando informações confidenciais, palavra a palavra e frase a frase. Os dados pessoais e de cartões de pagamento obtêm proteção e controlo específicos, ao passo que as pesquisas baseadas em estrutura detetam documentos confidenciais, como bases de dados de clientes.

APLICAÇÃO DE POLÍTICAS DE COMUNICAÇÃO.

Funcionalidades de filtragem de conteúdos e ficheiros ajudam a implementar as suas políticas e padrões de comunicação, identificando e bloqueando conteúdo inadequado, ao mesmo tempo que evitam o armazenamento desnecessário de ficheiros e formatos de ficheiro inapropriados.

FÁCIL DE GERIR.

A segurança de toda a farm de servidores pode ser administrada centralmente a partir de um único painel de controlo intuitivo. A administração é rápida e simples, sem que seja necessária formação especial.

PROTEÇÃO ANTIVÍRUS

- **Análise no acesso** – os ficheiros são analisados em tempo real, durante o carregamento ou a transferência.
- **Análise em segundo plano** – os ficheiros armazenados no servidor são verificados regularmente utilizando as assinaturas de malware mais recentes.
- **Integração com o Kaspersky Security Network** – fornece proteção assistida pela nuvem em tempo real, mesmo contra ameaças de dia zero.

SUPORTE DAS POLÍTICAS DE COMUNICAÇÃO DA SUA ORGANIZAÇÃO

- **Filtragem de ficheiros** – ajuda a aplicar as políticas de armazenamento de documentos e a reduzir a necessidade de dispositivos de armazenamento. Ao analisar formatos dos ficheiros reais, independentemente do nome da extensão, a aplicação garante que os utilizadores não podem utilizar um tipo de ficheiro banido em violação da política de segurança.
- **Proteção para wikis/blogues** – protege todos os repositórios SharePoint, incluindo wikis e blogues.
- **Filtragem de conteúdo** – impede o armazenamento de ficheiros que incluam conteúdos inadequados, seja qual for o tipo de ficheiro. O conteúdo de cada ficheiro é analisado com base em palavras-chave. Os clientes também podem criar os seus próprios dicionários personalizados para filtragem de conteúdos.

PREVENÇÃO CONTRA FUGAS DE DADOS CONFIDENCIAIS

- **Verificação de informações confidenciais em documentos** – o Kaspersky Security for Collaboration verifica todos os documentos transferidos em servidores SharePoint quanto a informações confidenciais.

  A solução integra módulos que identificam tipos de dados específicos, confirmando que cumprem as normas legais relevantes – por exemplo, dados pessoais (conforme definido pelas conformidades regulamentares, como a HIPAA ou a Diretiva da UE 95/46/CE) ou os dados da norma PCI DSS (Norma de Segurança dos Dados para a Indústria dos Cartões de Pagamento).

  Os dados são analisados em relação a dicionários temáticos atualizados regularmente que abrangem categorias como "Finanças", "Documentos administrativos" e "Linguagem humilhante e abusiva" e dicionários personalizados.
- **Pesquisa de dados estruturados** – caso sejam detetadas informações apresentadas em estruturas específicas numa mensagem, estas serão tratadas como potencialmente confidenciais, o que permite garantir o controlo sobre dados confidenciais, como bases de dados de clientes que se encontrem em matrizes complexas.

GESTÃO FLEXÍVEL

- **Facilidade de gestão** – é possível gerir centralmente uma farm de servidores completa a partir de uma única consola. Uma interface intuitiva e que inclui todos os cenários administrativos cuja utilização é mais comum.
- **Painel de controlo único** – um painel de controlo com um esquema simples oferece acesso em tempo real ao estado atual do produto, versão da base de dados e estado da licença de todos os servidores protegidos.
- **Criação de cópias de segurança de ficheiros modificados** – em caso de incidente, os ficheiros originais podem ser restaurados, se necessário, podendo também utilizar-se informações de cópias de segurança detalhadas sobre ficheiros modificados para apoiar as investigações.
- **Integração com o Active Directory®** – permite a autenticação de utilizadores do Active Directory.

REQUISITOS DO SISTEMA

Servidores SharePoint

- Microsoft SharePoint 2010;
- Microsoft SharePoint 2013.

Sistema operativo (para instalar a solução)

Para o SharePoint Server 2010:

- Windows Server 2008 x64/ 2008 R2 / 2012 R2.

Para o SharePoint Server 2013:

- Windows Server 2008 R2 x64 SP1 / 2012 x64 / 2012 R2.

A lista completa de requisitos do sistema encontra-se disponível em kaspersky.pt

Como adquirir

O Kaspersky Security for Collaboration pode ser adquirido como parte do Kaspersky Total Security for Business ou como uma solução independente

Nota! Ao adquirir este produto, a opção para evitar fugas de informação confidencial é vendida separadamente.

Kaspersky Security for Collaboration/Versão 0.3/Jan 2015/Global

KASPERSKY lab