KASPERSKY SECURITY FOR COLLABORATION

Protection et contrôle des données pour les plates-formes collaboratives, y compris les fermes SharePoint.

La plate-forme que vous utilisez pour partager des fichiers et des informations est également le système de transit rapide et idéal pour les programmes malveillants et autres menaces informatiques.

Pour un environnement de travail partagé sécurisé et ininterrompu, Kaspersky Lab a développé une solution qui combine facilité de gestion et haute protection en temps réel contre les attaques de programmes malveillants et contre les fuites de données confidentielles.

- Moteur de protection contre les programmes malveillants primé
- « Recherche et protection » des données confidentielles
- Contrôles de l'accès aux données
- Protection en temps réel et basée dans le Cloud : Kaspersky Security Network
- Filtre des contenus et des fichiers
- Protection contre le phishing
- Sauvegarde et stockage
- Gestion centralisée et flexible
- Console d'administration intuitive

Bénéfices

PROTECTION COMPLÈTE DE LA PLATE-FORME SHAREPOINT
Si vous utilisez Microsoft SharePoint Server, tous les contenus sont stockés dans une base de données SQL. Les solutions de protection traditionnelles ne sont donc pas adaptées. Kaspersky Security for Collaboration applique une protection avancée primée contre les programmes malveillants dans toute la ferme SharePoint et pour tous les utilisateurs de celle-ci. Kaspersky Security Network offre une protection efficace dans le Cloud contre les menaces connues, inconnues et avancées, tandis que la technologie de lutte contre le phishing protège les données collaboratives des cybermenaces.

LUTTE CONTRE LES FUITES DE DONNÉES CONFIDENTIELLES
Les données confidentielles en circulation qui doivent être protégées et contrôlées doivent d'abord être identifiées. Grâce à l'utilisation de dictionnaires et catégories de données préinstallés ou personnalisés, Kaspersky Security for Collaboration vérifie mot par mot, phrase par phrase les données sensibles de chaque document placé sur les serveurs SharePoint. Les données personnelles et les données concernant les cartes de paiement sont en particulier protégées et contrôlées. Les recherches de données structurées se concentrent, quant à elles, sur les documents sensibles comme les bases de données des clients.

APPLICATION DES POLITIQUES DE COMMUNICATION INTERNES
Les fonctions de filtrage du contenu vous aident à appliquer vos politiques et normes en matière de communication. Pour ce faire, elles identifient et bloquent les contenus inappropriés et empêchent le stockage inutile de fichiers et de formats de fichiers non autorisés.

SIMPLICITÉ DE GESTION
Vous pouvez administrer de façon centralisée la sécurité de votre ferme de serveurs depuis un seul tableau de bord intuitif. L'administration se fait donc de manière simple et rapide, sans nécessiter de formation particulière.

PROTECTION ANTIVIRUS
- **Analyse en temps réel** : les fichiers sont analysés en temps réel, lors de leur téléchargement.
- **Analyse en arrière-plan** : les fichiers stockés sur le serveur sont régulièrement vérifiés à l'aide des dernières signatures de programmes malveillants.
- **Intégration à Kaspersky Security Network** : fournit une protection dans le Cloud et en temps réel contre les menaces zero-day.

PRISE EN CHARGE DES POLITIQUES DE COMMUNICATION DE L'ENTREPRISE

- **Filtrage des fichiers** : permet d'appliquer des stratégies d'enregistrement des documents et de limiter la sollicitation des périphériques de stockage. L'application analyse les formats de fichiers réels, quel que soit le nom de l'extension. Les utilisateurs ne peuvent donc pas utiliser des types de fichiers interdits par la politique de sécurité.
- **Protection contre les wikis / blogs** : protège tous les types de référentiels SharePoint, y compris les wikis et les blogs.
- **Filtrage des contenus** : empêche le stockage de fichiers dont les contenus sont inappropriés, tout type de fichier confondu. Le contenu de chaque fichier est analysé selon des mots clés. Les clients peuvent également créer leurs propres dictionnaires personnalisés afin de filtrer le contenu.

LUTTE CONTRE LES FUITES DE DONNÉES CONFIDENTIELLES

- **Analyse des documents à la recherche d'informations confidentielles** : Kaspersky Security for Collaboration analyse tous les documents téléchargés sur les serveurs SharePoint pour savoir s'ils contiennent des informations confidentielles.

  La solution intègre des modules qui identifient des types de données spécifiques, ce qui confirme qu'elle respecte les normes juridiques en vigueur, par exemple, les données personnelles (définies par la règlementation en vigueur, comme la loi HIPAA ou la Directive européenne 95/46/EC), ou les données PCI DSS (Payment Card Industry Data Security Standard) en vigueur.

  Les données sont analysées et comparées à des dictionnaires thématiques intégrés et régulièrement mis à jour, qui couvrent des catégories comme : la « Finance », les « Documents administratifs » et le « Vocabulaire offensant et obscène ». Ces données sont également comparées à des dictionnaires personnalisés.
- **Recherche de données structurées** : si des informations présentées dans des structures spécifiques figurent dans un message, elles seront traitées comme potentiellement confidentielles, ce qui garantit un contrôle sur les données sensibles se trouvant dans des séries complexes, comme les bases de données clients.

GESTION FLEXIBLE

- **Gestion simple** : la totalité d'une ferme de serveurs peut être gérée de manière centralisée depuis une même console. Une interface intuitive inclut tous les scénarios administratifs les plus couramment utilisés.
- **Tableau de bord unique** : un tableau de bord parfaitement clair permet un accès en temps réel au statut actuel du produit, à la version de la base de données et au statut des licences de tous les serveurs protégés.
- **Sauvegarde des fichiers modifiés** : en cas d'incident, les fichiers originaux peuvent être restaurés si nécessaire et les informations détaillées concernant la sauvegarde peuvent être utilisées dans le cadre d'enquêtes.
- **Intégration à Active Directory®** : permet l'authentification des utilisateurs Active Directory.

CONFIGURATION

Serveurs SharePoint :
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013
- Microsoft SharePoint 2016

Système d'exploitation (pour installer la solution)

Pour SharePoint Server 2010 :
- Windows Server 2008 x64/ 2008 R2/2012 R2

Pour SharePoint Server 2013 :
- Windows Server 2008 R2 x64 SP1/ 2012 x64/2012 R2

Pour SharePoint Server 2016 :
- Windows Server 2012 R2 x64

La liste complète de la configuration requise est disponible sur kaspersky.fr

Comment acheter le produit

La solution Kaspersky Security for Collaboration est incluse lorsque vous achetez la solution Kaspersky Total Security for Business. Elle est également vendue seule, en tant que solution « à la carte ».

Remarque ! Lorsque vous achetez ce produit, l'option de protection contre les fuites d'informations confidentielles est vendue séparément.

Kaspersky Security for Collaboration/Version 0.4/avr 16/Mondial