KASPERSKY SECURITY FOR WINDOWS SERVER™

Développé spécifiquement pour les serveurs d'entreprise haute performance

À mesure que les réseaux informatiques d'entreprise deviennent plus complexes, des niveaux de protection des serveurs supérieurs sont nécessaires. Un seul fichier infecté sur votre serveur d'entreprise peut contaminer tous les ordinateurs de votre réseau et créer des dommages importants. Une solution de sécurité des serveurs dédiée appropriée permet de s'assurer non seulement que vos données critiques sont protégées contre les derniers programmes malveillants, mais également que le risque d'intrusion des programmes malveillants dans des copies de sauvegarde des fichiers n'entraînent pas d'épidémies à répétition.

Kaspersky Security for Windows Server offre une sécurité économique, fiable et évolutive pour le stockage des fichiers partagés, avec un impact minimal sur les ressources.

Points fort de l'application

PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS CONNUS, INCONNUS ET SOPHISTIQUÉS

Notre moteur de protection contre les programmes malveillants, référence du secteur, garantit des analyses plus rapides et moins d'impact sur les ressources système, ce qui permet des taux de détection supérieurs rendus possibles par la sécurité basée sur le cloud (Kaspersky Security Network).

SÉCURITÉ AVANCÉE POUR LES SERVEURS CRITIQUES

Un module puissant de Contrôle du lancement des applications, combiné à la veille mondiale sur la sécurité et à la fonctionnalité Anti-Cryptor (protection contre le chiffrement), ajoute d'autres couches de protection avancée à vos systèmes de stockage et à vos serveurs d'entreprise.

SOLUTION CERTIFIÉE

L'application est certifiée compatible avec les plateformes de virtualisation et les systèmes d'exploitation.

Fonctionnalités de l'application

PROTECTION EFFICACE CONTRE LES PROGRAMMES MALVEILLANTS

Protection permanente contre les programmes malveillants et analyse à la demande. L'application analyse chaque fichier lancé ou modifié et traite, supprime ou met en quarantaine les objets suspects. Si un nouveau logiciel est installé ou en cas de suspicion d'infection d'un fichier, l'administrateur peut également lancer une analyse contre les programmes malveillants ciblant les zones suspectes.

Protection des serveurs assistée par le cloud. Kaspersky Security Network (KSN) offre une réponse plus rapide que jamais aux nouvelles menaces, améliorant ainsi la protection des composants et réduisant le risque de faux positifs.

Contrôle du lancement des applications sur les serveurs. Apporte une sécurité inégalée en utilisant des règles configurées pour autoriser ou bloquer le démarrage de fichiers exécutables, de scripts et de packages MSI ou le chargement de modules DLL sur les serveurs.

Protection des dossiers partagés contre les programmes malveillants de type CryptoLocker (fonction Anti-Cryptor de protection contre le chiffrement) Lorsqu'une activité de chiffrement est détectée, l'application empêche à l'ordinateur d'origine d'accéder aux fichiers ressources du réseau.

Blocage de l'accès des hôtes présentant des activités suspectes. Fonctionnalité de blocage des ordinateurs aux dossiers réseau d'un serveur protégé lors de la détection d'une activité malveillante en provenance de ces machines dans le cadre des tâches de Protection des fichiers en temps réel et de Protection contre le chiffrement.

Protection proactive contre les programmes malveillants. Technologies avancées de protection contre les programmes malveillants, dont un analyseur heuristique capable d'identifier des programmes malveillants à un très haut degré de précision même si sa signature n'a pas encore été ajoutée aux bases de données des programmes malveillants.

Analyse des zones critiques du système d'exploitation. Vous pouvez exécuter une tâche dédiée pour analyser les zones de votre système d'exploitation les plus exposées aux infections. Par exemple, l'analyse des fichiers qui s'exécutent automatiquement peut empêcher le lancement des programmes malveillants au démarrage du système et peut détecter des processus cachés.

Paramètres d'analyse flexibles. Les paramètres d'analyse des fichiers permettent à l'administrateur :

- d'exclure certains processus de l'analyse ;
- de définir le niveau de la protection ;
- de spécifier les types de fichiers qui doivent toujours être analysés et devraient être exclus ;
- de prédéfinir des réponses en cas d'infection d'objets en fonction du type de menace.

Cette approche permet d'optimiser la charge sur le serveur et garantit une gestion flexible de la sécurité du réseau d'entreprise.

Protection des serveurs de terminaux et virtuels. L'application protège les services Microsoft Terminal Server et les serveurs Citrix XenApp, en s'assurant que les utilisateurs finaux qui travaillent dans des modes de publication de bureau/d'application restent protégés et soient informés des événements. Hyper-V, XenDesktop et les environnements VMware™ sont eux aussi pris en charge.

Prise en charge des clusters. L'application est idéalement adaptée à une architecture de cluster de serveurs complexes, protégeant à la fois les disques locaux et les disques partagés du cluster appartenant au noeud protégé.

Haute performance

Évolutivité. Pour les serveurs à plusieurs processeurs, l'administrateur peut spécifier le nombre de processus anti-programmes malveillants pour permettre un traitement plus rapide des demandes.

Équilibrage de la charge. Les ressources peuvent être allouées à Kaspersky Security for Windows Server et aux autres applications en fonction des priorités : les analyses anti-programmes malveillants peuvent également être exécutées en arrière-plan.

Sélection des processus fiables. L'administrateur peut exclure des processus sécurisés, comme les sauvegardes de données ou la défragmentation du disque dur, de l'analyse à des fins d'optimisation des performances.

Fonctionnement ininterrompu des serveurs. Kaspersky Security for Windows Server n'implique pas de redémarrer le serveur à chaque installation ou mise à jour de la protection contre les programmes malveillants.

Administration flexible

Sélection des outils de gestion. L'application peut être gérée directement ou à distance par le biais de la console MMC (Microsoft Management Console), de Kaspersky Security Center ou en utilisant la ligne de commande. La dernière version du produit fournit une interface graphique intuitive pour la console MMC (Microsoft Management Console).

Outils d'installation et de gestion faciles d'emploi. Kaspersky Security Center est une console de gestion prenant en charge l'installation et la configuration à distance de l'application simultanément sur différents serveurs et facilitant la gestion de son fonctionnement et la réception des mises à jour et des notifications.

Contrôle des privilèges administrateur. L'application permet d'affecter différents niveaux de droits à chaque administrateur du serveur, ce qui permet de répondre aux exigences de conformité internes ou spécifiques à un service informatique.

Définition flexible des heures d'analyse. Pour réduire les interruptions et accroître la disponibilité des ressources des serveurs, vous pouvez définir facilement l'heure de début et de fin des analyses.

Système de notification. L'application prend en charge les notifications destinées aux administrateurs par le biais du service de messagerie ou des courriers électroniques pour une liste étendue d'événements. L'application est intégrée au protocole SNMP (Simple Network Management Protocol) et peut fonctionner avec Microsoft Operations Manager (MOM). L'administrateur peut également surveiller le fonctionnement de l'application en consultant les journaux d'événements Microsoft Windows ou Kaspersky Security Center.

Comment acheter

Kaspersky Security for Windows Server peut être acheté avec :
- Kaspersky Endpoint Security for Business – Select (en dehors du contrôle de lancement des applications)
- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

Il peut également être vendu en tant que solution ciblée :
Kaspersky Security for File Server et Kaspersky Security for Storage.

La liste des partenaires de Kaspersky Lab est disponible à l'adresse suivante :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

Pour en savoir plus : www.kaspersky.fr

CONFIGURATION SYSTÈME REQUISE

- Kaspersky Security for Windows Server est conçu pour les serveurs exécutant des versions de Microsoft Windows 32 bits ou 64 bits :
  - Microsoft Windows Server 2008/2008 R2 x86/x64 Standard/ Enterprise/Datacenter SP1 ou version ultérieure (dont le mode Core)
  - Microsoft Windows Hyper-V Server 2008 R2 SP1 ou version ultérieure
  - Microsoft Windows Server 2012/2012 R2 Essentials/Standard/Foundation/ Datacenter (dont le mode Core)
  - Microsoft Windows Hyper-V® Server 2012/2012 R2

- Kaspersky Security for Windows Server peut être installé sur les serveurs de terminaux suivants :
  - Microsoft Remote Desktop Services basé sur Windows 2008 Server
  - Microsoft Remote Desktop Services basé sur Windows 2008/2012/2012 R2 Server
  - Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6
  - Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6

Console de gestion :
- Microsoft Windows XP SP2/Vista® /7/8/10 Enterprise/Professionnel x86/x64
- Microsoft Windows Server 2008/2008 R2 Édition Standard/Enterprise/Datacenter SP1 x64 ou version ultérieure
- Microsoft Windows Server 2012/2012 R2 Édition Essentials/Standard/Foundation/ Datacenter x64
- Microsoft Windows Hyper-V Server 2008 R2 SP1/2012/2012 R2 x64 ou version ultérieure

Configuration matérielle minimale :
- Processeur : Intel® Pentium® IV
- Vitesse de traitement : 2,4 GHz
- RAM : 512 Mo
- Sous-système de disque dur : 1 disque IDE

Kaspersky Security for Windows Server/Version 3/Février 2016/Mondial