KASPERSKY lab

LES SOLUTIONS DE SÉCURITÉ KASPERSKY LAB POUR LES ENTREPRISES

2015

«LE POUVOIR DE PROTÉGER VOTRE ENTREPRISE »

Le risque de cyber-menaces pèse sur toutes les entreprises, quelle que soit leur taille. Kaspersky Lab est très bien placé pour détecter et identifier nombre de ces menaces.

Le niveau de menace augmente. Les nouveaux programmes malveillants qui ciblent les particuliers et les entreprises comme la vôtre dépassent actuellement le seuil des 325 000 menaces par jour.

Chez Kaspersky Lab, nous nous inquiétons de ces menaces et des risques qu'elles présentent pour votre entreprise ; c'est pourquoi nous conseillons aux entreprises de s'assurer que leur stratégie de sécurité réponde à trois critères clés :

1. Vous devez pouvoir accéder à une veille stratégique de premier plan en matière de menaces. Celle-ci vous permettra de comprendre ce qu'est une menace et comment les menaces sont écrites et compilées. Il est important que votre système de sécurité soit alimenté en permanence par des informations spécialisées et que votre fournisseur analyse les zones à risque du monde entier pour savoir à quoi s'attendre.

2. Votre système de sécurité doit comprendre des outils et techniques capables de détecter et d'éliminer des programmes malveillants connus, inconnus et sophistiqués. En même temps, votre logiciel de sécurité doit peser au minimum sur vos systèmes et maintenir de courts délais d'analyse afin de ne pas perturber les activités de votre entreprise.

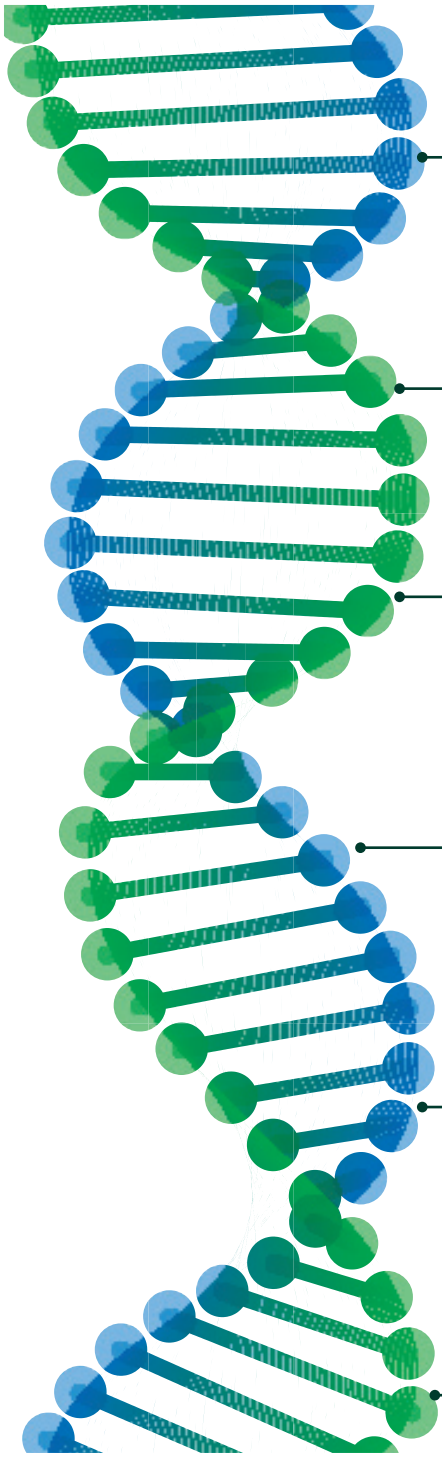
3. Puisque les environnements informatiques sont de plus en plus complexes, cette technologie doit pouvoir s'appliquer de façon souple et efficace aux terminaux physiques, mobiles et virtuels à travers une plate-forme unique, sans conflit de logiciels, sans avoir recours à plusieurs consoles et sans faille de sécurité.

Seul Kaspersky Lab peut offrir à votre entreprise la veille stratégique optimale en matière de menaces ainsi que la technologie permettant de la mettre en œuvre, intégrées en une seule plate-forme de sécurité.

Les solutions de Kaspersky Lab sont suffisamment souples pour s'adapter à vos objectifs. Ceci signifie que nous sommes toujours là pour protéger votre entreprise contre les menaces qui pèsent sur vos terminaux physiques et virtuels ainsi que sur vos appareils mobiles, vos systèmes de messagerie, serveurs, passerelles et portails SharePoint. Contactez-nous ou adressez-vous à votre fournisseur pour en savoir plus sur les produits, solutions et services évoqués dans ce document. Nous vous montrerons comment nous pouvons collaborer avec vous pour protéger votre entreprise contre les cyber-menaces.

NOTRE ADN : LA VEILLE TECHNOLOGIQUE EN MATIÈRE DE SÉCURITÉ

De nombreux éditeurs se disent à la pointe sur une technologie ou n°1 dans la détection de certaines menaces, mais un seul peut également le prouver : ces preuves sont dans notre ADN !



- Des technologies développées en interne.
- Reconnu comme leader par les 3 plus éminents et influents analystes mondiaux (Gartner, Forrester et IDC).
- Un réseau international d'experts (GREAT).
- La confiance des autorités de police et des administrations les plus respectées au monde.
- Le cloud Kaspersky Security Network (KSN) pour détecter des incidents de sécurité en temps réél.
- Plus de 130 fabricants OEM, dont Microsoft®, Cisco ® Meraki, Blue Coat, Juniper Networks, Alcatel Lucent et autres, intègrent nos technologies au sein de leurs propres produits et services.

SOMMAIRE

LA TECHNOLOGIE DE PROTECTION KASPERSKY LAB pages 6-7

PRODUITS, SOLUTIONS ET SERVICES page 8

Kaspersky Endpoint Security for Business

A propos page 9
Caractéristiques page 10
Version **CORE** page 11
Version **SELECT** page 12
Version **ADVANCED** page 13
Version **TOTAL** page 14

Solutions à la carte

Kaspersky Security for File Server page 15

Technologie de contrôle des terminaux pages 16-17

Kaspersky Security for Mobile pages 18-19

Chiffrement pages 20-21

Kaspersky Systems Management pages 22-23

Kaspersky Security for Mail Server page 24

Kaspersky Security for Internet Gateway page 25

Kaspersky Security for Collaboration page 26

Kaspersky Security for Storage page 27

Kaspersky Security for Virtualization pages 28-29

Services de veille stratégique page 30

Solutions de protection des environnements critiques page 31

Kaspersky Small Office Security page 32

Contrats de maintenance et support Kaspersky Lab page 33

KASPERSKY LAB A TRAVERS LE MONDE pages 34-35

LA TECHNOLOGIE DE PROTECTION KASPERSKY LAB CONTRE LES PROGRAMMES MALVEILLANTS

Gestion des correctifs, MDM, chiffrement, contrôle des appareils, anti-phishing : toutes ces technologies et bien d'autres encore fournissent des niveaux de sécurité précieux pour protéger les entreprises contre les menaces connues, inconnues et sophistiquées.

Le moteur de sécurité Kaspersky Lab est alimenté et renforcé en permanence par une veille stratégique constante. La priorité que nous accordons à la sécurité, alliée à notre expérience mondiale et notre veille stratégique en matière de sécurité, nous permettent de nous démarquer.

Les performances de pointe du moteur de protection contre les programmes malveillants intégré dans la plate-forme Kaspersky Endpoint Security for Business sont démontrées par de multiples tests indépendants réalisés de manière continue. Vos propres vérifications vous permettront de constater que la sécurité qu'offrent les solutions de Kaspersky Lab est inégalée.

CARACTÉRISTIQUES CLÉS DU PRODUIT

- **Détection des menaces connues, inconnues et sophistiquées**
- **Analyse comportementale et heuristique**
- **Kaspersky Security Network pour une protection dans le cloud**
- **Désinfection active**
- **Protection contre les programmes de chiffrement et ransomware**
- **Prévention automatique d'exploitation des failles**
- **HIPS et pare-feu personnel**
- **Blocage des attaques réseau**
- **Console de gestion simple et transparente**

BÉNÉFICES

UNE APPROCHE À PLUSIEURS NIVEAUX

L'approche à plusieurs niveaux de Kaspersky Lab est l'une des raisons pour lesquelles nous pouvons vous fournir les solutions de sécurité les plus efficaces du marché aujourd'hui. Puisque les technologies Kaspersky Lab sont développées en interne, les différents niveaux de protection se coordonnent simplement, avec un impact minimal sur la performance.

Chaque niveau de protection fait barrage aux cyber-menaces d'une manière différente, ce qui permet aux professionnels de l'informatique d'implémenter des technologies étroitement interdépendantes et de fournir une solution de sécurité complète.

LA MEILLEURE VEILLE STRATÉGIQUE EN MATIÈRE DE SÉCURITÉ DU MONDE : LA GARANTIE D'UNE PROTECTION CONTINUE

La veille stratégique mondiale en matière de sécurité de Kaspersky Lab est reconnue dans le monde entier et cette expertise alimente nos solutions de sécurité, qui sont conçues pour s'adapter à un monde en évolution constante.

FONCTIONNALITÉS

UNE SÉCURITÉ HEURISTIQUE, QUI PÈSE MOINS SUR VOS SYSTÈMES

L'identification des programmes malveillants basée sur l'étude des schémas de fonctionnement offre une détection améliorée, avec des fichiers de mise à jour plus petits et une sécurité renforcée.

ANALYSE COMPORTEMENTALE

Les solutions de protection contre les programmes malveillants de Kaspersky Lab comprennent deux composants spécifiques permettant d'analyser l'activité des programmes :

- **Émulateur** : reproduit et vérifie les activités du programme prévues.
- **Suivi du système** : suit les activités des programmes en cours d'exécution en discernant et en analysant les comportements caractéristiques des programmes malveillants.

DÉTECTION DE PROGRAMMES MALVEILLANTS DANS LE CLOUD : KASPERSKY SECURITY NETWORK (KSN)
Réponse en temps réel aux menaces de programmes malveillants nouvelles et déjà connues. Un flux constant de nouvelles données sur les tentatives d'attaques de programmes malveillants et les comportements suspects, fourni par plus de 60 millions d'utilisateurs de logiciels Kaspersky Lab, est utilisé pour aider à effectuer des diagnostics instantanés des fichiers, ce qui permet à tous les clients de bénéficier d'une protection en temps réel avec un faible taux de « faux positifs ».

PRÉVENTION AUTOMATIQUE D'EXPLOITATION DES FAILLES
La prévention automatique d'exploitation des failles vise spécifiquement les programmes malveillants qui exploitent les vulnérabilités logicielles des applications en reconnaissant leurs comportements typiques ou suspects. La technologie stoppe l'exploitation des failles et empêche tout code malveillant téléchargé de s'exécuter.

MESURES CONTRE LE RANSOMWARE DE CHIFFREMENT
Le système sauvegarde des copies des fichiers importants dans un espace de stockage temporaire, au cas où un processus suspect tenterait d'y accéder. Si un ransomware tentait de chiffrer les originaux, ces fichiers pourraient être restaurés à leur état non chiffré.

DÉSINFECTION ACTIVE
Utilise différentes techniques de « nettoyage » des infections détectées : empêche l'exécution des fichiers et des processus, y compris leur démarrage automatique, détruit les programmes malveillants et redéploie les fichiers stockés dans leur état d'origine.

SYSTÈME DE PRÉVENTION DES INTRUSIONS HÉBERGÉ SUR L'HÔTE (HIPS) ET PARE-FEU INDIVIDUEL
Certaines des activités des programmes sont associées à des risques suffisamment élevés pour rendre une obstruction souhaitable, même s'ils ne sont pas confirmés comme malveillants. Le système de prévention des intrusions hébergé sur l'hôte (HIPS) de Kaspersky Lab permet de limiter les activités du système en fonction du niveau de confiance de l'application à l'aide du pare-feu personnel de l'application, qui restreint l'activité réseau.

BLOCAGE DES ATTAQUES RÉSEAU
Surveille les activités suspectes sur votre réseau et vous permet également de préconfigurer la façon dont vos systèmes répondront en cas de détection d'un comportement suspect.

MISES À JOUR RÉGULIÈRES
Des mises à jour qui vous protègent contre les nouvelles menaces sont apportées à votre base de données de sécurité à l'issue du cycle de mise à jour le plus rapide du secteur, en même temps que les mises à jour continues des données sur les programmes malveillants nouvellement découverts dans le cloud, Kaspersky Security Network (KSN).

LA MEILLEURE PROTECTION DU SECTEUR : UN FAIT DÉMONTRÉ PAR DES TESTS INDÉPENDANTS

Au cours de l'année 2014, les produits Kaspersky Lab ont fait l'objet de **93 tests et études indépendants**. Nos produits ont été classés **66 fois parmi les trois meilleurs**, ce qui équivaut à **un score de 71 % dans le top 3**, et sont arrivés **en tête 51 fois**, c'est-à-dire dans bien plus de la moitié des tests.

Aucun produit ni aucune solution de nos principaux concurrents ne s'en approchent.

PRODUITS, SOLUTIONS ET SERVICES DE SÉCURITÉ POUR LES ENTREPRISES

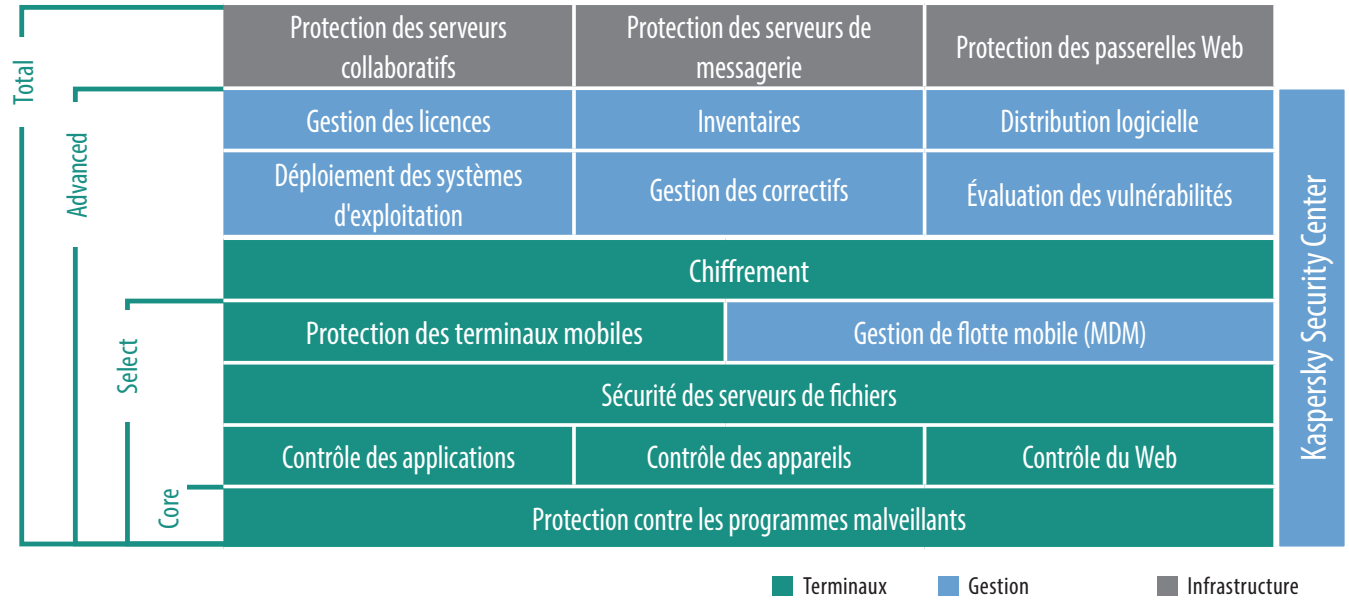
Kaspersky Endpoint Security for Business	Gamme de protection pour les entreprises de Kaspersky Lab. Elle comprend 4 niveaux de protection ainsi que des « solutions à la carte », le tout géré à partir d'une même console d'administration, Kaspersky Security Center. Kaspersky Total Security for Business intègre la protection des serveurs de messagerie, Web et collaboratifs, ce qui permet de préserver votre réseau périmétrique et de sécuriser complètement votre environnement informatique d'entreprise.
Solutions à la carte	Solutions indépendantes permettant de bénéficier de la sécurité Kaspersky Lab dans des domaines précis de votre système informatique. Certaines de ces solutions, telles que Kaspersky Security for Mobile, font également partie de Kaspersky Endpoint Security for Business. D'autres, telles que Security for Virtualization, sont disponibles séparément. Toutes les solutions de sécurité de terminaux physiques, mobiles, et virtuels sont gérées à travers Kaspersky Security Center.
Services de veille stratégique et solutions de protection des environnements critiques	La veille stratégique et l'expertise technique de Kaspersky Lab au service des entreprises. Ces services proposent des réponses à des problématiques de sécurité spécifiques (les attaques DDoS par exemple) ou encore des formations à la cyber-sécurité.
KASPERSKY SMALL OFFICE SECURITY	Une protection optimale, facile à installer et à utiliser, pour les très petites entreprises.
ACCORDS DE SERVICE ET DE MAINTENANCE	Une palette d'options d'assistance pour votre solution de sécurité Kaspersky Lab.

À PROPOS DE KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Kaspersky Endpoint Security for Business vous offre une solution de sécurité complète conçue par les meilleurs experts en sécurité informatique au monde : la protection la plus exhaustive et la plus avant-gardiste, une performance efficace et une gestion simple consolidées à travers des versions évolutives pour une sécurisation complète de votre entreprise.

Tous les composants ont été conçus en interne et rassemblés sous la forme d'une plate-forme de sécurité unique destinée à la satisfaction des besoins de votre entreprise. Le résultat obtenu est une solution stable et intégrée, ne présentant aucune faille, aucun problème de compatibilité et aucune charge de travail supplémentaire pour votre système.

Les administrateurs peuvent surveiller, gérer et protéger leur environnement informatique en s'appuyant sur Kaspersky Endpoint Security for Business. Les outils et technologies de Kaspersky Lab sont proposés sous forme de versions évolutives afin de répondre à vos nouveaux besoins au fur et à mesure qu'ils se présentent. Kaspersky Lab vous permet de simplifier votre quotidien.



Kaspersky Lab s'appuie sur des technologies développées à partir du même code source, utilisant le cloud Kaspersky Security Network, pour offrir à ses clients une protection de premier ordre.

En résumé, nous proposons la première plate-forme de sécurité du marché, développée en interne de A à Z, afin d'aider l'administrateur à surveiller, gérer et protéger votre environnement en toute simplicité.

▶ CARACTÉRISTIQUES DES SOLUTIONS

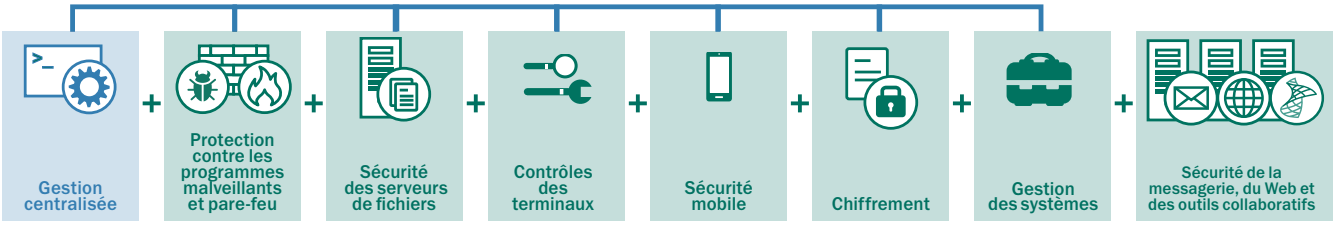
Quelle est la solution la mieux adaptée à vos besoins ?

		Core	Select	Advanced	Total	Géré via Security Center	Disponible dans une solution à la carte
	Protection contre les programmes malveillants	•	•	•	•	•	
	Pare-feu	•	•	•	•	•	
Outils de contrôle	Contrôle des applications		•	•	•	•	
Outils de contrôle	Contrôle des périphériques		•	•	•	•	
Outils de contrôle	Contrôle du Web		•	•	•	•	
	Sécurité des serveurs de fichiers		•	•	•	•	•
	Protection des terminaux mobiles		•	•	•	•	•
	Gestion de flotte mobile (MDM)		•	•	•	•	•
	Chiffrement			•	•	•	
Gestion des systèmes	Analyse des vulnérabilités			•	•	•	•
Gestion des systèmes	Gestion des correctifs (Patch management)			•	•	•	•
Gestion des systèmes	Inventaires			•	•	•	•
Gestion des systèmes	Gestion des licences			•	•	•	•
Gestion des systèmes	Déploiement d'applications			•	•	•	•
Gestion des systèmes	Déploiement des systèmes d'exploitation			•	•	•	•
	Protection des outils collaboratifs				•		•
	Protection des serveurs de messagerie				•	•	•
	Protection de la passerelle Internet				•		•
	Protection des infrastructures virtuelles					•	•
	Protection des serveurs de stockage					•	•

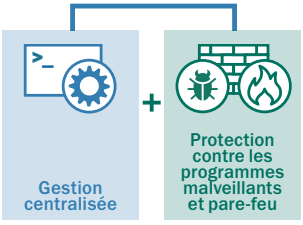
• Inclus • Inclus en partie (voir pages descriptives du produit)

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Protection puissante à plusieurs niveaux contre les menaces connues, inconnues et sophistiquées, conçue par les meilleurs experts en sécurité du secteur. La solution Kaspersky Endpoint Security for Business, alimentée par une veille stratégique en matière de sécurité de renommée mondiale, offre une sécurité et un contrôle informatiques inégalés.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS — CORE



Une protection optimale contre les programmes malveillants : la base de la plate-forme de sécurité Kaspersky Lab

Les technologies de protection à plusieurs niveaux de Kaspersky Lab sont développées en interne par des ingénieurs passionnés par la sécurité. Et comme le confirment des tests indépendants, le résultat est là : nous vous proposons la solution de sécurité la plus puissante et la plus efficace du marché, et donc la meilleure protection qui soit pour votre entreprise.

Protection contre les menaces connues, inconnues et sophistiquées : des technologies exclusives avancées identifient et éliminent les menaces nouvelles et existantes.

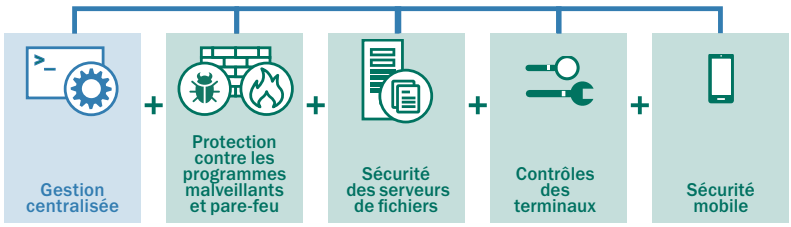
Prévention automatique d'exploitation des failles : cible et identifie proactivement les menaces inconnues et sophistiquées.

Protection dans le cloud : exploite les informations en temps réel du Kaspersky Security Network.

Suivi du système : fournit une fonction de restauration de fichier exclusive au cas où le système se trouverait affecté.

Le système de prévention des intrusions hébergé sur l'hôte (HIPS) avec pare-feu personnel permet de limiter les activités du système en fonction du niveau de confiance de l'application à l'aide du pare-feu personnel de l'application, qui restreint l'activité réseau.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — SELECT



Des outils pour répondre aux problématiques des équipes itinérantes, assurer le respect des politiques de sécurité informatique et bloquer les programmes malveillants.

Contrôle des applications

Les administrateurs peuvent définir des politiques visant à autoriser, bloquer ou réglementer l'usage des applications (ou de catégories d'applications).

Contrôle des périphériques

Les administrateurs sont en mesure de définir, programmer et appliquer des procédures sur l'accès aux données avec un contrôle des supports de stockage amovibles ainsi que d'autres périphériques (port USB ou autre type de connexion).

Filtrage de contenu Web

Les règles liées à l'usage d'Internet suivent l'utilisateur, qu'il soit sur le réseau d'entreprise ou en déplacement.

Liste blanche dynamique

La réputation des fichiers en temps réel réalisée par le cloud Kaspersky Security Network permet de s'assurer que vos applications approuvées sont protégées contre des programmes malveillants tout en favorisant une productivité optimale de l'utilisateur.

CONTRÔLES DES TERMINAUX

- **Contrôle des applications**
- **Contrôle Web**
- **Contrôle des périphériques**

Tous les détails pages 16-17

PROTECTION DES SERVEURS DE FICHIERS

Gérée conjointement avec la sécurité des terminaux via le Kaspersky Security Center.

KASPERSKY SECURITY FOR FILE SERVER

Tous les détails page 15

PROTECTION DES TERMINAUX MOBILES :

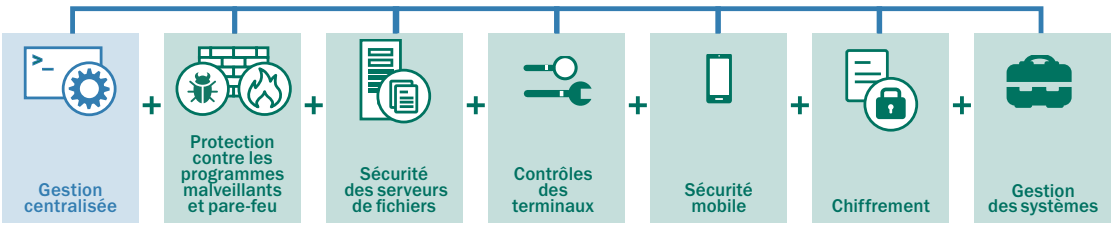
- **Anti-phising**
- **Antivol à distance**
- **Gestion des applications mobiles (MAM)**
- **Gestion de flotte mobile (MDM)**
- **Portail en libre service**

KASPERSKY SECURITY FOR MOBILE

Tous les détails pages 18-19

Kaspersky Endpoint Security for Business — SELECT comprend également tous les composants de la version CORE.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — ADVANCED



La version Advanced de Kaspersky Lab permet à votre entreprise de déployer et d'administrer ses procédures informatiques, de protéger ses utilisateurs des programmes malveillants et d'éviter la perte de données tout en optimisant les performances de l'environnement informatique.

Chiffrement des données

Possibilité de choisir un chiffrement complet du disque dur ou par fichier, en s'appuyant sur la norme de chiffrement AES (Advanced Encryption Standard) 256 bits pour sécuriser les données stratégiques de l'entreprise en cas de vol ou de perte des périphériques.

Partage sécurisé des données

Possibilité de créer facilement des paquets de données chiffrées et autoextractibles, pour protéger les données partagées via des périphériques amovibles, des e-mails, un réseau ou le Web.

Support des périphériques amovibles

Sécurité optimisée par le biais de politiques qui imposent le chiffrement des données sur les périphériques amovibles.

Transparence pour les utilisateurs finaux

La solution de chiffrement de Kaspersky est transparente pour les utilisateurs et n'a aucune incidence négative sur la productivité, aucun impact sur les paramètres, ni sur les mises à jour des applications

GESTION DES SYSTÈMES

- **Gestion des vulnérabilités et des correctifs**
- **Déploiement des systèmes d'exploitation**
- **Distribution de logiciels et dépannage**
- **Inventaires matériels et logiciels**
- **Gestion des licences**
- **Intégration SIEM**
- **Contrôle des accès basé sur les rôles**

Tous les détails pages 22-23

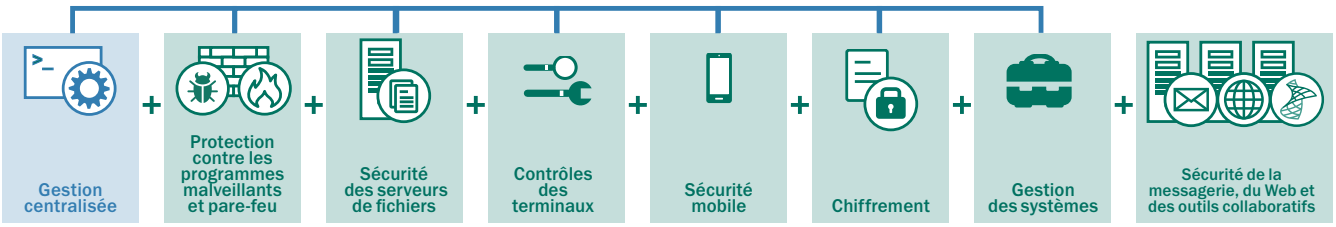
CHIFFREMENT

- **Chiffrement intégral de disques (FDE)**
- **Chiffrement au niveau des fichiers / dossiers (FLE)**
- **Chiffrement des périphériques amovibles**

Tous les détails pages 20-21

Kaspersky Endpoint Security for Business — ADVANCED comprend également tous les composants des versions SELECT et CORE.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Les entreprises qui ont besoin d'une sécurité complète pour l'ensemble de leur environnement informatique choisissent Kaspersky Total Security for Business

Kaspersky Total Security for Business est à ce jour la plate-forme de protection et d'administration la plus complète du marché. Elle protège toutes les couches de votre réseau et intègre des outils de configuration puissants afin de garantir que vos utilisateurs restent productifs et protégés contre les fichiers malveillants, indépendamment des appareils qu'ils utilisent et du lieu où ils se trouvent.

PROTECTION DES SERVEURS DE MESSAGERIE

Bloque efficacement les programmes malveillants associés aux e-mails, les attaques par phishing et les courriers indésirables grâce à des mises à jour en temps réel dans le cloud, pour un taux de détection exceptionnel et un nombre de faux positifs minimal. La protection contre les programmes malveillants est également possible pour IBM® Domino®. La fonctionnalité DLP pour Microsoft Exchange peut être achetée séparément.

KASPERSKY SECURITY FOR MAIL SERVER

Tous les détails page 24.

PROTECTION DES PASSERELLES INTERNET

Accès Internet sécurisé dans l'entreprise grâce à la suppression automatique des programmes malveillants et potentiellement dangereux contenus dans le trafic de données HTTP(S) / FTP / SMTP et POP3.

KASPERSKY SECURITY FOR INTERNET GATEWAY

Tous les détails page 25.

PROTECTION DES OUTILS COLLABORATIFS

Défend les serveurs et fermes Sharepoint® contre toutes les formes de programmes malveillants. La fonctionnalité DLP pour Sharepoint, disponible séparément, fournit des capacités de filtrage des fichiers et des contenus permettant d'identifier les données confidentielles et de protéger les systèmes contre les fuites de données.

KASPERSKY SECURITY FOR COLLABORATION

Tous les détails page 26.

Kaspersky Total Security for Business comprend également tous les composants des versions ADVANCED, SELECT et CORE.

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server fournit une sécurité évolutive, fiable et économique pour le stockage des fichiers partagés, sans impact perceptible sur les performances systèmes.

BÉNÉFICES

PUISSANTE PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS

Le moteur primé de protection contre les programmes malveillants de Kaspersky Lab protège efficacement les serveurs, empêchant même les menaces malveillantes connues les plus récentes d'entrer sur le réseau.

HAUTE PERFORMANCE ET FIABILITÉ

Vous avez la garantie que Kaspersky Security for File Server ne ralentira pas votre système de manière importante ni n'interfèrera avec vos activités, qui se déroulent même dans des conditions de réseau surchargé.

SUPPORT DE PLATES-FORMES MULTIPLES

Une solution de sécurité unique et efficace pour des réseaux de serveurs hétérogènes, entièrement compatible avec les plates-formes et serveurs les plus récents (par exemple serveurs de terminaux, en cluster et virtuels).

PUISSANCE DE GESTION ET DE CRÉATION DE RAPPORTS

Des outils d'administration efficaces et conviviaux, des informations sur l'état de protection des serveurs, des paramètres horaires flexibles pour les analyses et un système de création de rapports très complet garantissent un contrôle efficace de la sécurité des serveurs de fichiers.

FONCTIONNALITÉS

- **Protection en temps réel contre les programmes malveillants** pour les serveurs de fichiers dotés des dernières versions de Windows® (y compris Windows Server® 2012/R2), Linux® et FreeBSD (tous deux incluant Samba).
- **Protection des serveurs de terminaux Citrix et Microsoft®.**
- **Support des serveurs en cluster.**
- **Évolutivité** : support et protection sans effort, même pour les infrastructures hétérogènes les plus complexes.
- **Fiabilité, stabilité et haute tolérance aux pannes.**
- **Technologie d'analyse optimisée et intelligente** permettant l'analyse à la demande et par zone système critique.
- **Zones fiables** permettant de renforcer la sécurité tout en réduisant les niveaux de ressources nécessaires pour l'analyse.
- **Mise en quarantaine et sauvegarde** des données avant désinfection ou suppression.
- **Mise à l'écart** des postes de travail infectés.
- **Installation, gestion et mises à jour centralisées** avec des options de configuration souples.
- **Scénarios d'intervention flexibles en cas d'incidents.**
- **Rapports complets** sur l'état de la protection du réseau.
- **Système de notification de l'état des applications.**
- **Support des systèmes de gestion hiérarchique du stockage** (HSM).
- **Support de Hyper-V et Xen Desktop.**
- **Compatibilité avec VMware.**
- **Compatibilité avec ReFS.**

Kaspersky Security for File Server est inclus dans Kaspersky Endpoint Security for Business - SELECT et ADVANCED, ainsi que dans Kaspersky Total Security for Business. Il est également disponible séparément en tant que solution à la carte.

NOTRE TECHNOLOGIE DE CONTRÔLE DES TERMINAUX

Des outils puissants de contrôle des postes de travail, étroitement intégrés à un anti-malware particulièrement efficace et au seul laboratoire de liste blanche dédié du secteur, vous aident à protéger votre entreprise contre les menaces dynamiques actuelles.

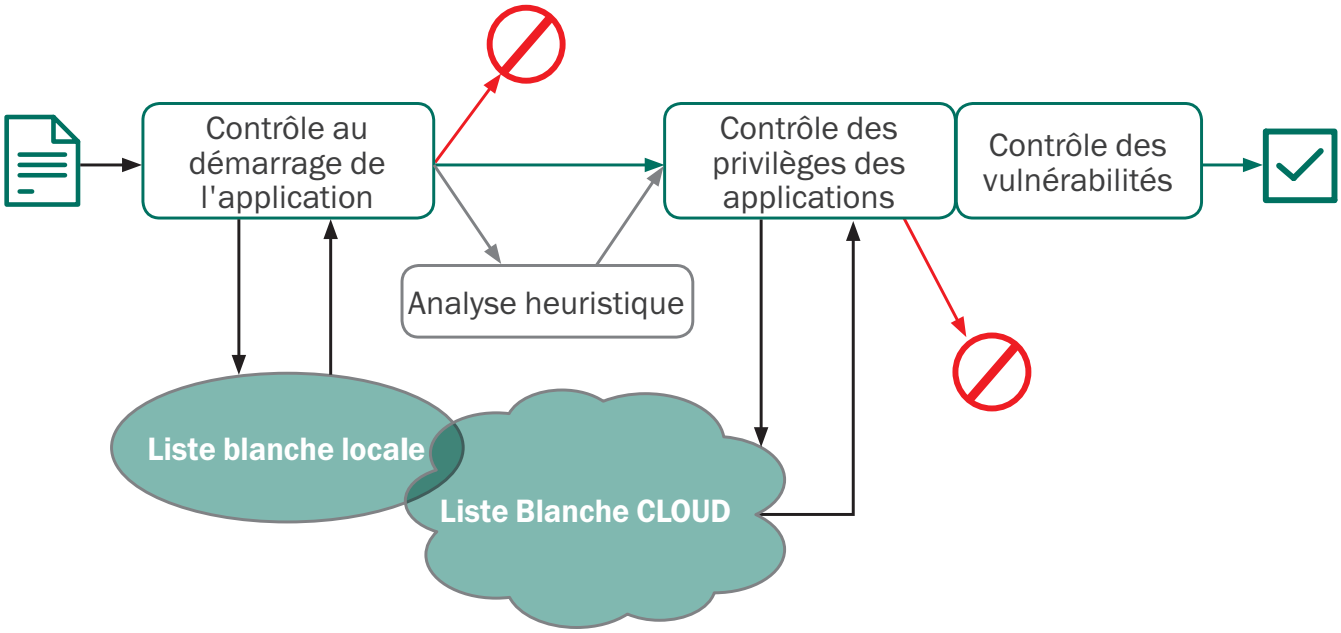
IDENTIFIER. CONTRÔLER. PROTÉGER.
Les vulnérabilités des applications de confiance, les programmes malveillants présents sur le Web et le manque de contrôle sur les périphériques font partie du paysage des menaces actuel, qui est de plus en plus complexe. Les outils de contrôle de Kaspersky Lab, appliqués au niveau des applications, du Web et des périphériques vous offrent un contrôle total sur l'ensemble de vos PC de bureau ou ordinateurs portables sous Windows sans nuire à la productivité.

CONTRÔLE DES APPLICATIONS ET LISTE BLANCHE DYNAMIQUE
Les systèmes sont protégés contre les menaces connues et inconnues grâce au contrôle total dont bénéficient les administrateurs sur les applications et les programmes autorisés à être exécutés sur les stations de travail, indépendamment du comportement de l'utilisateur. La technologie Kaspersky lab permet également de surveiller l'intégrité des applications afin d'évaluer leur comportement et d'éviter qu'elles n'exécutent des actions indésirables présentant des risques pour la station de travail ou le réseau. La création et l'application automatisées et simplifiées de politiques personnalisables offrent les avantages suivants :

- **Contrôle au démarrage de l'application** : autoriser, bloquer, vérifier les lancements d'applications. Améliore la productivité puisque l'accès aux applications non professionnelles est restreint.
- **Contrôle des privilèges au niveau des applications** : régule et contrôle l'accès de certaines applications aux ressources et données du système. Les applications sont classées en quatre catégories : confiance, restrictions faibles, restrictions élevées, douteuses.
- **Recherche de vulnérabilités au niveau des applications** : permet de remonter de façon centralisée les vulnérabilités de Microsoft Windows et des éditeurs tiers.

La plupart des solutions de contrôle proposent uniquement une fonction basique permettant d'autoriser ou de bloquer l'accès. Les outils de contrôle de Kaspersky Lab se distinguent par l'utilisation de bases de données de liste blanche dans le cloud, ce qui permet un accès presque en temps réel aux données les plus récentes relatives aux applications.

Les technologies de contrôle des applications de Kaspersky Lab utilisent des bases de données de liste blanche dans le cloud pour analyser et surveiller les applications à chaque étape : téléchargement, installation et exécution.



La liste blanche dynamique, qui peut être activée via une politique de blocage par défaut, bloque toutes les applications tentant de s'exécuter sur un poste de travail à moins qu'elles n'aient été explicitement autorisées par les administrateurs. Kaspersky Lab est la seule entreprise de sécurité informatique à posséder son propre laboratoire de liste blanche dédié, qui gère une base de données constamment surveillée et mise à jour et qui contient plus de 500 millions de programmes.

La politique de **blocage par défaut (Default Deny) de Kaspersky Lab peut être appliquée dans un environnement test**, afin d'établir la légitimité d'une application avant de la bloquer. Il est également possible de créer des catégories d'applications basées sur des signatures numériques, afin d'empêcher les utilisateurs de démarrer un logiciel légitime ayant été altéré par un programme malveillant ou provenant d'une source suspecte.

CONTRÔLES WEB
Cette fonction permet de surveiller, filtrer et contrôler les sites Web accessibles sur le lieu de travail, et ainsi d'améliorer la productivité tout en assurant une protection contre les programmes malveillants et attaques provenant du Web.

Les contrôles Web avancés de Kaspersky Lab sont intégrés à un répertoire de sites Web constamment mis à jour. Les sites y sont regroupés en catégories (adulte, jeux, réseaux sociaux, paris en ligne, etc.). Les administrateurs peuvent facilement créer des politiques pour interdire, limiter ou vérifier l'utilisation qui est faite d'un site ou de toute une catégorie de sites, ainsi que créer leurs propres listes. Les sites malveillants sont automatiquement bloqués.

En limitant leur utilisation, les contrôles Web de Kaspersky Lab aident à lutter contre les pertes de données survenant sur les réseaux sociaux et les services de messagerie instantanée. Des politiques flexibles permettent aux administrateurs d'autoriser la navigation Internet à certains moments de la journée. Grâce à l'intégration à Active Directory, les politiques peuvent être appliquées dans toute l'entreprise de manière simple et rapide.

Pour plus de sécurité, les contrôles Web de Kaspersky Lab sont activés directement sur la station de travail, ce qui signifie que les politiques s'appliquent même si l'utilisateur n'est pas sur le réseau.

CONTRÔLES DES APPAREILS
La désactivation d'un port USB ne résout pas toujours un problème de périphériques amovibles. Par exemple, un port USB désactivé a une incidence sur d'autres mesures de sécurité, comme l'accès VPN avec jeton.

Les contrôles de Kaspersky Lab sur les périphériques permettent une plus grande granularité de contrôle au niveau du port, du type et du périphérique, pour une productivité de l'utilisateur intacte et une sécurité optimisée. Le cas échéant, les contrôles peuvent être appliqués à un seul périphérique, en utilisant son numéro de série.

- Des autorisations de connexion, de lecture et d'écriture peuvent être définies pour les périphériques, ainsi que des heures de programmation pour l'application de ces contrôles.
- Les règles de contrôle des périphériques sont créées sur des masques, éliminant ainsi la nécessité de connecter physiquement les périphériques pour les placer sur liste blanche. Il est possible de placer sur liste blanche plusieurs périphériques en même temps.
- Contrôle l'échange de données entre l'entreprise et l'extérieur par les périphériques amovibles, ce qui réduit le risque de perte ou de vol de données.
- Intègre les technologies de chiffrement de Kaspersky Lab, afin d'appliquer les politiques de chiffrement à des types d'appareils spécifiques.

SIMPLICITÉ D'ADMINISTRATION
Tous les outils de contrôle de Kaspersky Lab s'intègrent avec Active Directory. L'élaboration des politiques est donc à la fois simple et rapide. Tous les contrôles au niveau des postes de travail sont gérés à partir de la même console, par le biais d'une seule interface.

La technologie de contrôle des terminaux est incluse dans Kaspersky Endpoint Security for Business – SELECT et ADVANCED et dans Kaspersky Total Security for Business.

KASPERSKY SECURITY FOR MOBILE

Les appareils mobiles sont devenus des cibles de choix pour les cyber-criminels. De plus, le BYOD (Bring Your Own Device) contribue à la diversification des appareils utilisés, ce qui complique le travail d'administration et de contrôle des services informatiques.

Avec Kaspersky Security for Mobile, vos appareils sont en sécurité, où qu'ils se trouvent. Protégez-vous des programmes malveillants en évolution constante et gagnez rapidement et facilement en visibilité et en contrôle pour tous les smartphones et tablettes de votre environnement, depuis une plateforme centralisée garantissant un minimum de perturbations.

CARACTÉRISTIQUES CLÉS DU PRODUIT

- **Puissant anti-malware**
- **Anti-phishing et filtrage des SMS et des appels entrants**
- **Protection Web**
- **Contrôle des applications**
- **Détection des terminaux 'jailbreakés'**
- **Mise en conteneur d'applications**
- **Protection contre le vol**
- **Gestion des appareils mobiles**
- **Portail libre-service**
- **Administration centralisée**
- **Console Web**
- **Plates-formes supportées :**
  - Android™
  - iOS
  - Windows Phone

POINTS FORTS

PROTECTION AVANCÉE CONTRE LES PROGRAMMES MALVEILLANTS POUR LA SÉCURITÉ DES APPAREILS MOBILES ET DES DONNÉES

Rien qu'en 2014, Kaspersky Lab a détecté près de 1,4 million d'attaques malveillantes différentes sur appareils mobiles. Kaspersky Security for Mobile lutte contre les menaces connues et inconnues visant les données stockées sur les appareils mobiles en associant une protection contre les programmes malveillants à diverses technologies de protection multi-niveaux.

GESTION DES APPAREILS MOBILES

L'intégration à l'ensemble des principales plateformes de gestion des appareils mobiles permet un déploiement et un contrôle à distance « Over the Air » (OTA) pour une plus grande simplicité d'utilisation et d'administration sous Android, iOS et Windows Phone.

GESTION DES APPLICATIONS MOBILES

Les fonctions de mise en conteneur et de suppression sélective permettent de séparer les données de l'entreprise et les données personnelles sur un même appareil, favorisant ainsi les initiatives en faveur du BYOD. Également doté de notre fonction de chiffrement et de notre protection contre les programmes malveillants, Kaspersky Security for Mobile ne se contente pas d'isoler un appareil et ses données, mais propose une solution proactive de protection pour mobiles.

ADMINISTRATION CENTRALISÉE

Gérez plusieurs plateformes et appareils depuis la même console que vos autres terminaux et gagnez en visibilité et en contrôle sans effort ou technologie d'administration supplémentaires.

FONCTIONS DE GESTION ET DE SÉCURITÉ POUR MOBILES

PUISSANT ANTI-MALWARE

Protection proactive dans le cloud, basée sur la reconnaissance de signatures (via Kaspersky Security Network, KSN), pour contrer les attaques malveillantes sur mobiles connues et inconnues. Des analyses programmées ou à la demande sont combinées à des mises à jour automatiques pour une protection supérieure.

ANTI-PHISHING ET FILTRAGE DE SMS /APPELS ENTRANTS

Des technologies puissantes anti-phishing avec création d'une liste blanche et liste noire personnelles protègent l'appareil et ses données des attaques de phishing et aident à filtrer les appels et les messages indésirables.

CONTRÔLE WEB/NAVIGATION WEB SÉCURISÉE

Des technologies gérées par Kaspersky Security Network (KSN) travaillent en temps réel pour empêcher l'accès à des sites Web malveillants et non autorisés. La fonction Safe Browser fournit une analyse de réputation constamment actualisée afin de garantir une navigation sécurisée sur appareil mobile.

CONTRÔLE DES APPLICATIONS

Des contrôles intégrés à KSN permettent de limiter l'utilisation d'applications aux logiciels approuvés, interdisant l'accès aux logiciels « grisés » ou non autorisés. Vous pouvez faire en sorte que l'appareil ne fonctionne qu'après installation de certaines applications. Le contrôle d'inactivité des applications permet aux administrateurs de demander à l'utilisateur de se reconnecter si une application est inactive pendant un certain temps. Cela permet de protéger les données même si une application est ouverte lors de la perte ou du vol de l'appareil.

DÉTECTION DES ACCÈS RACINE/'JAILBREAK'

Si un utilisateur ou une application tente de rooter le terminal Android ou jailbreaker les matériels sous iOS, ils seront détectés et consignés. Vous pouvez ensuite bloquer l'accès aux conteneurs, procéder à une suppression sélective ou supprimer toutes les données de l'appareil.

MISE EN CONTENEUR

Séparez les données de l'entreprise et les données personnelles en « empaquetant » vos applications dans des conteneurs. Vous pouvez appliquer d'autres politiques en complément, par exemple une fonctionnalité de chiffrement, pour protéger vos données sensibles. La suppression sélective permet de supprimer les données stockées dans les conteneurs sur un appareil lorsqu'un employé quitte la société, sans avoir à toucher à ses données personnelles.

PROTECTION CONTRE LE VOL

En cas de perte ou de vol d'un appareil, vous pouvez activer à distance des fonctions antivol, notamment la suppression des données, le verrouillage et la localisation de l'appareil, la surveillance SIM, le mugshot* et l'alarme. Selon la situation, ces commandes antivol seront appliquées avec une grande souplesse. Par exemple, les commandes sont envoyées immédiatement grâce à l'intégration à Google Cloud Messaging (GCM) pour un temps de réaction optimal et une sécurité accrue, et l'administrateur n'a pas à intervenir puisque les commandes sont envoyées sur le portail libre-service.

GESTION DES APPAREILS MOBILES

Le support de Microsoft Exchange ActiveSync, Apple MDM, Samsung KNOX 2.0 et tout matériel Android, permet d'appliquer un grand nombre de politiques sur une interface unifiée, quelle que soit la plate-forme (ex : appliquer un chiffrement et des mots de passe ou contrôler l'utilisation de l'appareil photo, restreindre les politiques à des individus ou des groupes, gérer les paramètres APN**/VPN, etc.).

PORTAIL LIBRE-SERVICE

Déléguez les tâches courantes d'administration de sécurité à vos employés et autorisez l'autoenregistrement des appareils approuvés. Lors de la procédure d'enregistrement d'un nouvel appareil, tous les certificats requis sont automatiquement mis à disposition sur le portail, sans que l'administrateur ait à intervenir. En cas de perte de l'appareil, l'employé peut activer toutes les commandes antivol disponibles depuis le portail.

ADMINISTRATION CENTRALISÉE

Administrez tous vos appareils mobiles depuis une seule et même console, qui vous permettra également de gérer la sécurité informatique de tous les autres terminaux.
La console Web permet aux administrateurs de contrôler et d'administrer les appareils à distance depuis n'importe quel ordinateur.

*cliché du voleur capturé à l'aide de l'appareil photo frontal du périphérique mobile
** Point d'accès réseau (Access Point Name)

Kaspersky Security for Mobile est inclus dans Kaspersky Endpoint Security for Business - SELECT et ADVANCED, ainsi que Kaspersky Total Security for Business. Il est également disponible séparément en tant que solution à la carte.

TECHNOLOGIE DE CHIFFREMENT

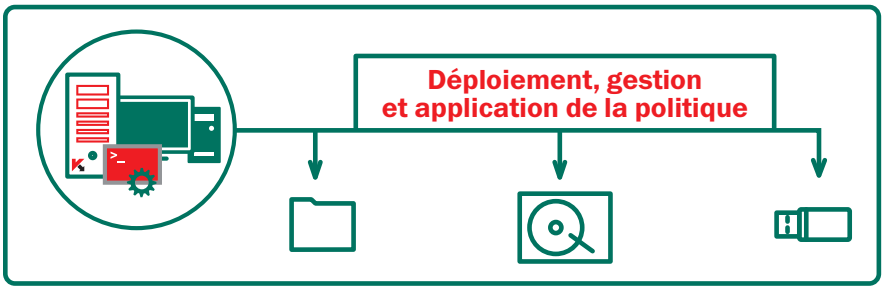
Empêche l'accès non autorisé à vos données en cas de perte ou de vol d'un appareil ou d'une attaque malveillante ciblant vos données.

La protection proactive des données et la conformité sont un impératif. La technologie de chiffrement de Kaspersky Lab protège les données importantes en cas de perte ou de vol d'un appareil ou d'attaques malveillantes ciblées. Associant une technologie puissante de chiffrement aux technologies de protection des terminaux de Kaspersky Lab, notre plateforme intégrée protège vos données quand elles sont stockées et quand elles circulent.

Cette solution a été développée intégralement par Kaspersky Lab : le déploiement et l'administration s'effectuent donc en toute simplicité à partir d'une unique console via une seule politique.

Protégez-vous contre la perte de données et l'accès non autorisé à certaines informations avec la technologie de chiffrement de Kaspersky Lab:

- **Chiffrement intégral de disque (FDE)**
- **Chiffrement au niveau des fichiers/ dossiers (FLE)**
- **Périphériques amovibles (clés USB, disques durs externes)**



ADMINISTRATION DEPUIS UNE SEULE CONSOLE DE GESTION

CHIFFREMENT SÉCURISÉ CONFORME À LA NORME DU SECTEUR

Kaspersky Lab utilise la norme Advanced Encryption Standard (AES) avec une longueur de clé de 256 bits, une gestion des clés et une autorité de séquestre simplifiées. Supporte les plateformes de technologie Intel® AES-NI, UEFI et GPT.

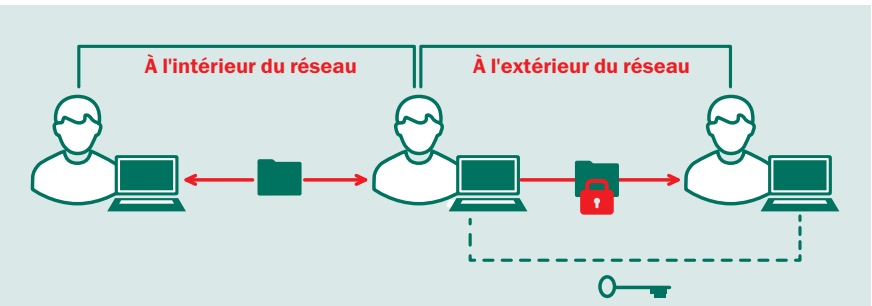
FLEXIBILITÉ TOTALE

Kaspersky Lab propose un chiffrement au niveau des fichiers et des dossiers (FLE) ainsi qu'un chiffrement intégral de disque (FDE), afin de couvrir tous les scénarios d'utilisation possibles. Les données peuvent être protégées sur disques durs et appareils amovibles. Le « mode portable » permet l'utilisation et le transfert des données sur des supports amovibles chiffrés, y compris sur des ordinateurs sur lesquels le logiciel de chiffrement n'est pas installé, ce qui facilite l'échange sécurisé de données « en dehors du périmètre ».

AUTHENTIFICATION UNIQUE ET TRANSPARENCE POUR L'UTILISATEUR FINAL

De la configuration à l'utilisation quotidienne, la technologie de chiffrement de Kaspersky Lab travaille de manière transparente sur l'ensemble des applications, sans compromettre la productivité de l'utilisateur final. L'authentification unique permet un chiffrement en toute transparence, l'utilisateur final n'ayant peut-être même pas conscience que la technologie fait son travail.

Le chiffrement de Kaspersky Lab permet de transférer des fichiers de manière transparente entre différents utilisateurs présents à l'intérieur et à l'extérieur du réseau.



FONCTIONNALITÉS DE CHIFFREMENT

INTÉGRATION TRANSPARENTE AUX TECHNOLOGIES DE SÉCURITÉ DE KASPERSKY LAB

Intégration totale aux technologies de protection contre les programmes malveillants, de contrôle des terminaux et de gestion pour une sécurité à plusieurs niveaux reposant sur un code de base commun. Par exemple, une seule politique suffit pour appliquer le chiffrement à certains appareils amovibles. Les paramètres de chiffrement peuvent s'appliquer sous la même politique que l'anti-malware, le contrôle des appareils et d'autres éléments de sécurité des terminaux. Il n'est pas nécessaire de déployer et d'administrer plusieurs solutions distinctes. La compatibilité du matériel réseau est automatiquement vérifiée avant l'application du chiffrement ; les plateformes UEFI et GPT bénéficient d'une prise en charge standard.

CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES

Dans les grandes entreprises, vous pouvez choisir de déléguer la gestion du chiffrement à l'aide de la fonction de contrôle d'accès basé sur les rôles. Cela permet une gestion du chiffrement moins complexe.

AUTHENTIFICATION AVANT DÉMARRAGE (PBA)

Les identifiants de l'utilisateur sont requis avant même le démarrage du système d'exploitation pour un niveau de sécurité supplémentaire, avec possibilité d'authentification unique.

AUTHENTIFICATION PAR CARTE À PUCE ET JETON

Supporte l'authentification à deux facteurs via les cartes à puce et jetons parmi les plus répandus. L'utilisateur n'a plus à saisir de nom d'utilisateur ni de mot de passe supplémentaires, ce qui améliore son expérience.

RÉCUPÉRATION D'URGENCE

Les administrateurs peuvent déchiffrer les données en cas de panne matérielle ou logicielle. La récupération du mot de passe pour l'authentification PBA ou l'accès aux données chiffrées est mise en place par un mécanisme simple de défi/réponse.

DÉPLOIEMENT OPTIMISÉ, PARAMÈTRES PERSONNALISABLES

Pour un déploiement aisé, la fonction de chiffrement de Kaspersky Lab n'est disponible que dans les versions Advanced et Total de Kaspersky Endpoint Security for Business. Aucune autre installation n'est nécessaire. Les paramètres de chiffrement sont prédéfinis mais personnalisables pour des dossiers couramment utilisés, notamment Mes Documents, le Bureau, les nouveaux dossiers, les extensions de fichiers et les groupes comme Documents Microsoft Office ou archives de messages.

Le chiffrement des données est inclus dans Kaspersky Endpoint Security for Business – ADVANCED et Kaspersky Total Security for Business.

KASPERSKY SYSTEMS MANAGEMENT

Les vulnérabilités non corrigées dans les applications largement utilisées représentent l'une des plus grandes menaces pour la sécurité informatique des entreprises. Ce risque est aggravé par la complexité croissante des environnements informatiques : si vous ne savez pas de quoi est composé votre parc, comment faire pour le sécuriser ?

La centralisation et l'automatisation des principales tâches de sécurité, de configuration et de gestion, telles que l'évaluation des vulnérabilités, la distribution des correctifs et mises à jour, la gestion des inventaires et le déploiement d'applications, permettent de gagner du temps mais aussi de gagner en sécurité.

Kaspersky Systems Management aide à réduire les risques relatifs à la sécurité informatique ainsi que la complexité de l'administration afin de donner aux responsables une visibilité et un contrôle complets et en temps réel sur les différents appareils, applications et utilisateurs, et ce, depuis un seul et même écran.

CARACTÉRISTIQUES CLÉS DU PRODUIT

- **Évaluation des vulnérabilités et gestion des correctifs**
- **Inventaires matériels et logiciels**
- **Installation logicielle et prise de contrôle à distance, y compris pour les sites distants**
- **Déploiement des systèmes d'exploitation**
- **Intégration SIEM**
- **Contrôle d'accès multi-administrateurs basé sur des rôles**
- **Administration centralisée**

SÉCURITÉ RENFORCÉE

Renforcez la sécurité informatique et réduisez la quantité de tâches courantes grâce à des correctifs et mises à jour distribués automatiquement et au bon moment. La découverte et la hiérarchisation automatisées des vulnérabilités soutiennent la productivité et réduisent la charge de travail des ressources concernées. Des tests indépendants[1] révèlent que Kaspersky Lab propose la couverture automatisée de correctifs et de mises à jour la plus complète et la plus rapide.

CONTRÔLE AVEC VISIBILITÉ TOTALE

Grâce à une visibilité totale du réseau depuis une console unique, les administrateurs sont au fait de chaque application et appareil entrant sur le réseau, y compris des appareils des visiteurs. Cette visibilité permet un contrôle centralisé de l'accès aux données et aux applications de l'entreprise par utilisateur ou appareil, conformément aux politiques informatiques de l'entreprise.

ADMINISTRATION CENTRALISÉE

La solution de gestion des systèmes de Kaspersky Lab est un composant géré depuis la console Kaspersky Security Center, à l'aide de commandes et d'interfaces homogènes et intuitives, la finalité étant d'automatiser les tâches informatiques courantes.

FONCTIONNALITÉS

ÉVALUATION DES VULNÉRABILITÉS ET GESTION DES CORRECTIFS

Les analyses logicielles automatisées permettent une détection, une hiérarchisation et une correction rapides des vulnérabilités. Les correctifs et mises à jour peuvent être fournis automatiquement, dans des délais très courts[2], pour les logiciels Microsoft et non Microsoft. L'administrateur reçoit une notification sur le statut d'installation du correctif. L'application des correctifs non essentiels peut être repoussée après les heures de bureau, et pourra se faire même si les ordinateurs sont éteints grâce à la

1&2. Test sur les solutions de gestion des correctifs effectué par AV-TEST GmbH (juillet 2013) à la demande de Kaspersky Lab

fonction de réveil à distance, Wake-on-LAN. La diffusion Multicast permet une distribution locale des correctifs et mises à jour sur les sites distants, réduisant ainsi les besoins en bande passante.

INVENTAIRES MATÉRIELS ET LOGICIELS
Grâce à la découverte, l'inventaire, la notification et le suivi automatiques des matériels et logiciels, y compris des appareils amovibles, les administrateurs ont une vue détaillée de chaque ressource présente sur le réseau de l'entreprise. Les appareils des visiteurs peuvent être détectés et un accès Internet peut leur être attribué. Le contrôle des licences offre une visibilité sur le nombre de noeuds et la date d'expiration.

DÉPLOIEMENT D'APPLICATIONS ET DE SYSTÈMES D'EXPLOITATION
Création, stockage, clonage et déploiement simples et centralisés d'images systèmes sécurisées de manière optimale. Déploiement en dehors des heures de bureau via Wake-on-LAN avec modification après installation pour une plus grande flexibilité. Support UEFI.

DISTRIBUTION LOGICIELLE
Déploiement/mise à jour à distance, depuis une seule console. Plus de 100 applications parmi les plus répandues, identifiées via Kaspersky Security Network, peuvent être automatiquement installées, après les heures de bureau si vous le souhaitez. Complète prise en charge du dépannage à distance, avec une sécurité renforcée par les audits et journaux de sessions et l'autorisation des utilisateurs. Trafic réduit vers les sites distants grâce à la technologie Multicast pour la distribution logicielle en local.

INTÉGRATION SIEM
Les événements sont directement consignés et transférés vers les principaux systèmes SIEM (IBM® QRadar® et HP ArcSight). Les journaux et autres données de sécurité sont récupérés pour analyse, afin de réduire la charge de travail des administrateurs et le nombre d'outils utilisés, tout en simplifiant la création de rapports au niveau de l'entreprise.

CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES
Permet de distinguer les rôles et responsabilités d'administration sur les réseaux complexes. Possibilité de personnaliser les éléments affichés sur la console selon les rôles et les droits.

ADMINISTRATION CENTRALISÉE
Une console d'administration intégrée, Kaspersky Security Center, permet de gérer la sécurité des systèmes pour les postes de travail, les appareils mobiles et les terminaux virtuels sur l'ensemble du réseau, depuis une seule et même interface.

Kaspersky Systems Management est inclus dans Kaspersky Endpoint Security for Business - ADVANCED et dans Kaspersky Total Security for Business, et peut également être acheté séparément en tant que solution ciblée.

KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server assure une protection de haut niveau du trafic qui transite par les serveurs de messagerie contre les courriers indésirables, les phishing et les menaces liées à des programmes malveillants simples ou élaborés, et ce même si votre infrastructure est hétérogène et des plus complexes.

La protection contre les fuites de données confidentielles dans les e-mails et les pièces jointes est également disponible pour les environnements Microsoft® Exchange Server.

BÉNÉFICES

PROTECTION CONTRE LES MENACES LIÉES AUX PROGRAMMES MALVEILLANTS

Le moteur de protection contre les programmes malveillants primé de Kaspersky assure une protection efficace, avec le soutien en temps réel de la protection dans le cloud Kaspersky Security Network, d'une protection proactive contre l'exploitation des failles et d'un filtrage des URL malveillantes.

PROTECTION ANTISPAM

Pour les serveurs de messagerie Microsoft Exchange et Linux®, le moteur antispam dans le cloud de Kaspersky Lab parvient à bloquer jusqu'à 99,92 % des courriers indésirables avec un nombre minime de faux positifs.

CONTRÔLES ET PROTECTION CONTRE LES FUITES DE DONNÉES (SERVEURS MICROSOFT EXCHANGE)*

Kaspersky Security for Microsoft Exchange Server identifie les données commerciales, financières, personnelles et autres informations sensibles contenues dans les e-mails sortants et les pièces jointes sur les serveurs Microsoft Exchange. Cette solution contrôlant la circulation de ces informations, elle garantit ainsi la confidentialité de vos données et de celles de vos employés conformément à la législation sur la protection des données. Des techniques d'analyse sophistiquées telles que les recherches de données structurées et les glossaires propres à chaque activité, permettent d'identifier les e-mails suspects, qui sont alors bloqués. Le système peut même avertir le responsable de l'expéditeur d'une possible atteinte à la sécurité des données.

ADMINISTRATION SIMPLE ET FLEXIBLE

Grâce à une administration et des outils de création de rapports intuitifs et des paramètres d'analyse flexibles, vous pouvez contrôler efficacement la sécurité de votre messagerie et de vos documents.

FONCTIONNALITÉS

- Protection contre les programmes malveillants, en temps réel et grâce au cloud avec Kaspersky Security Network.
- Protection instantanée contre l'exploitation des failles encore inconnues et même les vulnérabilités « zero-hour » avec ZETA Shield.
- Protection antispam avancée : le moteur antispam de Kaspersky Lab bloque plus de 99 % du trafic de courriers indésirables.
- Protection contre les fuites de données (serveurs Microsoft Exchange)*. Détection des informations confidentielles dans les e-mails et les pièces jointes par catégorisation (notamment les coordonnées personnelles et les données de cartes de paiement), glossaires et analyse approfondie à l'aide de données structurées.
- Analyse basée sur le cloud et en temps réel de tous les messages sur les serveurs Microsoft® Exchange, y compris dans les dossiers publics, via Kaspersky Security Network.
- Analyse programmée des e-mails et des bases de données Lotus Domino.
- Analyse des messages, bases de données et autres objets présents sur les serveurs IBM® Domino®.
- Filtrage des messages par reconnaissance du format, de la taille et du nom des pièces jointes.
- Processus simple et pratique de mise à jour des bases de données contre les programmes malveillants et les courriers indésirables.
- Sauvegarde des données avant désinfection ou suppression.
- Évolutivité et tolérance aux pannes.
- Installation simple et administration flexible.
- Système de notification avancé.
- Rapports complets sur l'état de la protection du réseau.

*Lorsque vous achetez ce produit, l'option de protection contre les pertes ou les fuites de données confidentielles est vendue séparément.

KASPERSKY SECURITY FOR INTERNET GATEWAY

L'accès sécurisé à Internet pour l'ensemble des collaborateurs est l'un des piliers centraux de toute stratégie de sécurité d'une entreprise. Kaspersky Security for Internet Gateway est une solution de haut niveau dédiée à la protection contre les programmes malveillants, qui garantit à l'ensemble de vos effectifs un accès Internet sûr et sécurisé en toutes circonstances.

BÉNÉFICES

PROTECTION ÉLEVÉE, RÉDUCTION DES PANNES ET DES PERTURBATIONS RÉSEAUX

Le moteur primé de protection contre les programmes malveillants de Kaspersky Lab empêche les menaces d'entrer sur le réseau local par le biais de programmes malveillants ou dangereux. Bénéfice de cette solution : un nombre minime de perturbations des activités de l'entreprise liées aux menaces malveillantes et la réduction des coûts associés.

EFFICACITÉ ET PERFORMANCE

La technologie d'analyse intelligente et optimisée et l'équilibrage de la charge permettent de réduire la sollicitation des ressources afin de préserver la bande passante sans compromettre la sécurité.

SUPPORT DE PLATES-FORMES MULTIPLES

Prenant en charge les derniers serveurs et plates-formes, y compris les serveurs proxy, Kaspersky Security for Internet Gateway est une solution à forte valeur ajoutée pour les entreprises gérant d'importants volumes de trafic réseau dans des environnements disparates. Le support de Microsoft Forefront TMG s'étend à la messagerie d'entreprise ainsi qu'à la protection de la passerelle Web.

SIMPLICITÉ D'ADMINISTRATION ET DE CRÉATION DE RAPPORTS

Grâce à des outils d'administration simples et conviviaux, des paramètres d'analyse flexibles et des systèmes de création de rapports relatifs à l'état de protection, vos administrateurs et vous êtes certains de pouvoir contrôler votre sécurité de manière simple et efficace.

FONCTIONNALITÉS

- **Protection proactive et permanente** contre les menaces malveillantes connues et émergentes.
- **Excellents taux de détection des programmes malveillants** et peu de faux positifs.
- **Technologie d'analyse optimisée et intelligente.**
- **Analyse en temps réel** du trafic HTTP, HTTPS et FTP depuis des serveurs publiés.
- **Protection pour Squid**, le serveur proxy Linux le plus utilisé.
- **Outils pratiques** d'installation, d'administration et de mise à jour.
- **Outils d'analyse flexibles et différents scénarios d'intervention en cas d'incidents**.
- **Équilibrage de la charge** des processeurs de serveurs.
- **Évolutivité et tolérance aux pannes.**
- **Rapports complets** sur l'état de la protection du réseau.

FONCTIONNALITÉS SPÉCIFIQUES AUX SERVEURS MICROSOFT® FOREFRONT® TMG ET ISA :

- Surveillance en temps réel de l'état des applications.
- Analyse des connexions VPN.
- Analyse en temps réel du trafic HTTPS (TMG uniquement).
- Protection du trafic de messagerie (via les protocoles POP3 et SMTP).
- Copie de sauvegarde des objets traités (TMG)

Les solutions Kaspersky Security for Mail Server et Kaspersky Security for Internet Gateway sont incluses dans Kaspersky Total Security for Business et peuvent également être achetées séparément en tant que solutions à la carte.

KASPERSKY SECURITY FOR COLLABORATION

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

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 cyber-menaces.

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 INTERNE
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.

FONCTIONNALITÉS

PROTECTION ANTIVIRUS
- **Analyse en temps réel** - les fichiers sont analysés en temps réel, lors du 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 basée sur le cloud et en temps réel contre les menaces zero day.

SUPPORT 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 des 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 confidentielless** : 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 »..

- **Recherche de données structurées :** si des informations présentées dans des structures spécifiques se trouvent 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.

Kaspersky Security for Collaboration est inclus dans Kaspersky Total Security for Business et peut également être acheté séparément en tant que solution à la carte.

*Lorsque vous achetez ce produit, l'option de protection contre les pertes ou les fuites de données confidentielles est vendue séparément.

KASPERSKY SECURITY FOR STORAGE

Protection haute performance pour les systèmes de stockage EMC, NetApp, Hitachi, Oracle et IBM®.

BÉNÉFICES

PUISSANTE PROTECTION EN TEMPS RÉEL CONTRE LES PROGRAMMES MALVEILLANTS

Protection proactive permanente pour les solutions de stockage en réseau. Le puissant moteur contre les programmes malveillants de Kaspersky Lab analyse chaque fichier lancé ou modifié à la recherche de programmes malveillants de tout type, tels que virus, vers et chevaux de Troie. Une analyse heuristique avancée permet d'identifier les nouvelles menaces encore méconnues.

PERFORMANCES OPTIMISÉES

Une analyse haute performance, basée sur une technologie optimisée et des paramètres d'exclusion flexibles, offre une protection maximale tout en minimisant l'impact sur les performances système.

FIABILITÉ

Une architecture directe utilisant des composants unifiés conçus pour travailler parfaitement ensemble permet d'atteindre une remarquable tolérance aux pannes. Vous bénéficiez ainsi d'une solution stable et résistante qui, en cas d'arrêt forcé, redémarrera automatiquement afin d'assurer une protection fiable et continue.

SIMPLICITÉ D'ADMINISTRATION

Les serveurs sont installés et protégés à distance dès la mise en service, sans nécessiter de redémarrage, et sont administrés ensemble depuis une console centralisée simple et intuitive, Kaspersky Security Center, complétée par d'autres solutions de sécurité de Kaspersky Lab.

FONCTIONNALITÉS

SÉCURITÉ PROACTIVE PERMANENTE

Référence en la matière, le moteur de protection contre les programmes malveillants de Kaspersky Lab, développé par nos experts, offre une protection proactive contre les nouvelles menaces et les menaces éventuelles, basée sur des technologies intelligentes de détection avancée.

MISES À JOUR AUTOMATIQUES

Les bases de données des programmes malveillants sont mises à jour automatiquement sans interruption d'analyse afin de garantir une protection continue et de minimiser la charge de travail pour l'administrateur.

ZONE DE CONFIANCE ET EXCLUSION DE PROCESSUS

La configuration des performances d'analyse peut être affinée en créant des « zones de confiance » qui, au même titre que des formats de fichiers et des processus définis tels que des sauvegardes de données, pourront être exclues des analyses.

ANALYSE AUTOMATIQUE D'OBJETS

Pour une protection accrue des serveurs, des analyses de démarrage automatique au niveau des fichiers et des systèmes d'exploitation peuvent être exécutées afin d'éviter que des programmes malveillants ne se lancent au démarrage du système.

ANALYSE FLEXIBLE POUR DES PERFORMANCES OPTIMISÉES

Réduit les temps d'analyse et de configuration et favorise l'équilibrage de la charge, pour des performances serveur optimales. L'administrateur peut spécifier et contrôler la profondeur, l'ampleur et le moment de l'activité d'analyse, et définir les types de fichiers et les zones à analyser. Il est également possible de programmer des analyses à la demande sur des périodes de faible activité des serveurs.

PROTECTION DES SOLUTIONS HSM ET DAS

Supporte les modes d'analyse hors ligne pour la protection efficace des systèmes HSM de gestion hiérarchique du stockage. La protection du stockage à connexion directe permet également d'utiliser des solutions de stockage à faible coût.

SUPPORT DE TOUS LES PRINCIPAUX PROTOCOLES

Kaspersky Security for Storage supporte les principaux protocoles utilisés par différents systèmes de stockage : CAVA agent, RPC et ICAP.

PROTECTION DES SYSTÈMES VIRTUELS ET DES SERVEURS DE TERMINAUX

Cette sécurité flexible inclut une protection pour les systèmes d'exploitation virtuels (invités) dans les environnements Hyper-V et VMware, et pour les infrastructures de terminaux Microsoft® et Citrix.

ADMINISTRATION

INSTALLATION ET GESTION CENTRALISÉES

L'installation, la configuration et l'administration se font à distance depuis la console intuitive Kaspersky Security Center, y compris les notifications, les mises à jour et la création de rapports flexibles. Vous pouvez également opter pour une administration par lignes de commande si vous le souhaitez.

CONTRÔLE DES PRIVILÈGES ADMINISTRATEUR

Différents niveaux de privilèges peuvent être affectés à chaque administrateur de serveur afin de respecter les politiques de sécurité informatique propres à l'entreprise.

RAPPORTS FLEXIBLES

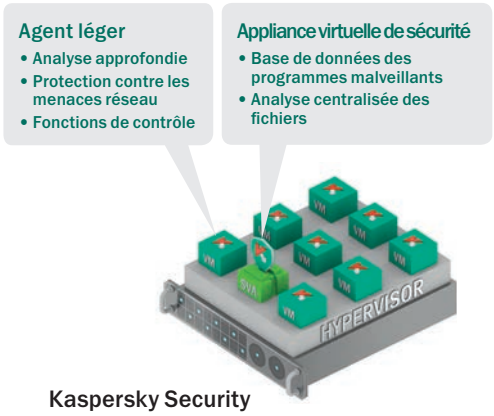
La création de rapports peut se faire à l'aide de rapports graphiques ou en consultant les journaux d'événements de Microsoft Windows® ou de Kaspersky Security Center. Les outils de recherche et de filtrage permettent d'accéder rapidement aux données recherchées dans des journaux volumineux.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization est une solution flexible qui garantit une protection et des performances exceptionnelles pour vos environnements virtuels.

UN AGENT LÉGER POUR UNE PROTECTION AVANCÉE

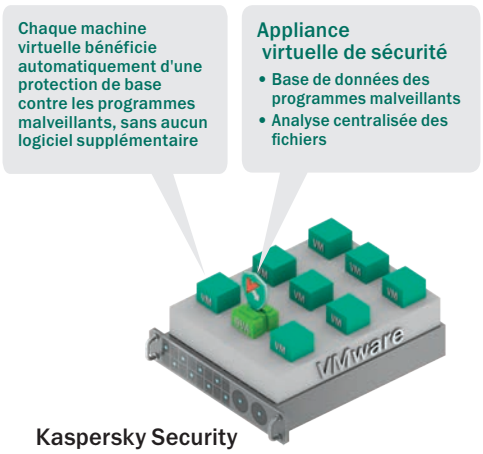
Kaspersky Security for Virtualization comprend un agent léger puissant qui est déployé sur chaque machine virtuelle. Cela permet l'activation des fonctionnalités avancées de sécurité pour les terminaux. Ces fonctions incluent la surveillance des vulnérabilités, le contrôle des applications, des périphériques et du Web, la protection antivirus pour la messagerie instantanée, la messagerie et le Web, et des méthodes heuristiques avancées. Résultat : une solution de sécurité puissante, multi-niveaux et ultra-performante.



Kaspersky Security for Virtualization
Configuration avec agent léger

CONFIGURATION FACULTATIVE SANS AGENT POUR LES ENVIRONNEMENTS VMWARE*

Grâce à une intégration étroite et aux technologies VMware, Kaspersky Security for Virtualization peut également être facilement déployé et géré sur cette plate-forme, dans une configuration de sécurité sans agent. Toute l'activité de sécurité est concentrée dans l'appliance virtuelle de sécurité et s'interface avec vShield pour une protection instantanée et automatique des machines virtuelles, et avec vCloud pour la protection réseau.



Kaspersky Security for Virtualization
Configuration sans agent

FONCTIONNALITES CLES DE LA SOLUTION

- Administration centralisée avec Kaspersky Security Center
- Protection de machines virtuelles basée sur une appliance virtuelle de sécurité centralisée
- Protection avancée contre les programmes malveillants
- Système de prévention des intrusions hébergé sur l'hôte (HIPS) et pare-feu
- Contrôle des applications, des périphériques et de l'accès au Web
- Sécurité basée sur le cloud via Kaspersky Security Network
- Blocage des attaques réseau
- Protection contre le phishing
- Anti-virus pour messagerie instantanée (IM), messagerie et trafic Internet
- Pas d'installation ni de redémarrage supplémentaire pour les nouvelles machines virtuelles**

SYSTÈME DE LICENCES FLEXIBLE

Selon vos besoins, plusieurs options de licence sont disponibles pour Kaspersky Security for Virtualization :

- Licences liées aux machines :
  - par poste de travail
  - par serveur
- Licences liées aux ressources :
  - par cœur.

PLUSIEURS PLATES-FORMES : UN TARIF UNIQUE

Une seule licence Kaspersky Security for Virtualization comprend le support des environnements virtuels Citrix, Microsoft® et VMware.

APPLIANCE VIRTUELLE DE SÉCURITÉ

Kaspersky Lab offre deux solutions performantes dans ce domaine, reposant sur une appliance virtuelle de sécurité.

L'appliance virtuelle de sécurité (SVA) Kaspersky Lab analyse de manière centralisée toutes les machines virtuelles de l'environnement hôte. Cette architecture fournit une protection efficace des machines virtuelles sans sacrifier les ressources des terminaux, en éliminant les « blitz de mise à jour », les « blitz antivirus » et en permettant un plus grand ratio de consolidation.

INTÉGRATION AVEC LA PLATE-FORME DE L'ARCHITECTURE

Kaspersky Security for Virtualization supporte les plates-formes VMware, Microsoft® Hyper-V® et Citrix Xen ainsi que leurs principales technologies.

VMWare	Microsoft Hyper-V	Citrix Xen
Haute disponibilité	Mémoire dynamique	Contrôle dynamique de la mémoire
Intégration avec vCenter	Volumes partagés de cluster	Protection et récupération de machine virtuelle (VMPR)
vMotion – DRS hôte	Sauvegarde instantanée	XenMotion (migration en direct)
Horizon view (clones entiers et clones liés)	Migration en direct	Multi-stream ICA
		Citrix Receiver
		Personal vDisk

* Les fonctionnalités de sécurité avancées [mise en quarantaine des fichiers, système de prévention des intrusions hébergé sur l'hôte (HIPS), analyse automatique des vulnérabilités, contrôles des terminaux, etc.] ne sont pas disponibles dans cette configuration.

** Pour les machines virtuelles non-persistantes, la protection instantanée est disponible dès l'installation de l'agent léger dans l'image de la machine virtuelle. Pour les machines virtuelles persistantes, l'administrateur doit déployer l'agent léger manuellement au cours de l'installation.

SERVICES DE VEILLE STRATÉGIQUE KASPERSKY LAB

En tant que responsable de la sécurité informatique, il est de votre responsabilité de protéger votre société contre les menaces actuelles, et d'anticiper les dangers auxquels elle pourrait être confrontée dans les années à venir. Ceci exige un niveau de veille stratégique en matière de sécurité que très peu d'entreprises sont en mesure de développer en interne.

Kaspersky Lab est un partenaire précieux, toujours disponible pour partager, via différents canaux, ses données de veille stratégique mises à jour minute par minute, pour vous aider à protéger votre entreprise.

FORMATION À LA CYBER-SÉCURITÉ
Le programme de formation à la cyber-sécurité de Kaspersky Lab a été développé spécifiquement pour les entreprises qui cherchent à développer leurs connaissances en interne sur la cyber-sécurité pour mieux protéger leurs infrastructures et leur propriété intellectuelle.

Le programme porte sur de nombreux sujets, des principes de sécurité de base à l'analyse avancée des programmes malveillants et investigations numériques pour aider les clients à améliorer leurs connaissances en matière de cyber-sécurité dans trois domaines principaux :

- Sensibilisation à la cyber-sécurité
- Principes généraux du cyber-diagnostic
- Analyse avancée des programmes malveillants et reverse engineering

FLUX D'INFORMATION SUR LES MENACES
Les flux d'informations sur les menaces de Kaspersky Lab sont conçus pour s'intégrer minute par minute dans les Security Information et Event Management (SIEM) existants pour fournir un niveau de protection supplémentaire.

ANALYSE DES PROGRAMMES MALVEILLANTS ; INVESTIGATION NUMÉRIQUE ; INTERVENTION EN CAS D'INCIDENT
Les services d'investigation de Kaspersky Lab peuvent aider les entreprises à élaborer des stratégies de défense en fournissant des analyses approfondies des menaces et en offrant des conseils sur les mesures appropriées à mettre en œuvre pour résoudre les incidents.

Trois niveaux d'investigation sont proposés :

- Analyse des programmes malveillants : pour vous aider à comprendre le comportement et les objectifs des fichiers de logiciels malveillants spécifiques ciblant votre entreprise.
- Investigation numérique : fournit une image complète de l'incident et de la manière dont votre entreprise est affectée.
- Réaction en cas d'incident : cycle complet d'investigation des incidents qui comprend une visite des experts de Kaspersky Lab sur le site de l'incident.

REPÉRAGE DES MENACES BOTNET
La solution experte de Kaspersky Lab surveille l'activité des botnets et donne rapidement (en 20 minutes) une notification des menaces associées à des utilisateurs individuels de systèmes bancaires et de paiement en ligne. Vous pouvez utiliser ces notifications pour alerter votre clientèle, vos fournisseurs de services de sécurité et les autorités locales des menaces en cours.

RAPPORTS DE VEILLE STRATÉGIQUE
Les rapports de veille stratégique de Kaspersky Lab vous donnent accès à des informations pertinentes mises à jour minute par minute et fondées sur plus de 80 millions de statistiques utilisateur recueillies dans 200 pays, ce qui augmente votre connaissance des menaces qui pèsent sur votre entreprise.

Les connaissances et l'expérience approfondies de Kaspersky Lab en font le partenaire de choix des plus grandes autorités de police et administrations au monde, notamment Interpol et de nombreux organismes CERT. Votre entreprise peut tirer parti dès aujourd'hui de ces renseignements.

SOLUTIONS DE PROTECTION DES ENVIRONNEMENTS CRITIQUES

PROTECTION CONTRE LES ATTAQUES DDOS

Prend en charge toutes les étapes nécessaires pour défendre votre entreprise contre les attaques de déni de service distribuées.

Kaspersky DDoS Protection défend votre entreprise contre tous les types d'attaques DDoS et atténue leurs effets. Ceci comprend l'analyse continue de l'ensemble de votre trafic en ligne, qui permet de vous alerter de la présence d'attaques potentielles puis de rediriger votre trafic, de le nettoyer et de vous renvoyer un trafic propre.

KASPERSKY FRAUD PREVENTION : POUR LES BANQUES ET INSTITUTIONS FINANCIÈRES

Une plate-forme complète, hautement personnalisée et facile d'utilisation qui répond aux risques de fraude liés aux transactions financières en ligne et sur mobiles.

Kaspersky Fraud Prevention protège les clients des établissements financiers, qu'ils accèdent à ces services à partir de PC, d'ordinateurs portables, de smartphones ou de tablettes. La plate-forme comprend également un composant logiciel côté banque qui détecte les programmes malveillants et identifie automatiquement les schémas comportementaux inhabituels dans les différentes transactions des clients. Kaspersky Fraud Prevention Clientless Engine peut empêcher les transactions frauduleuses même si Kaspersky Fraud Prevention for Endpoints n'a pas été installé.

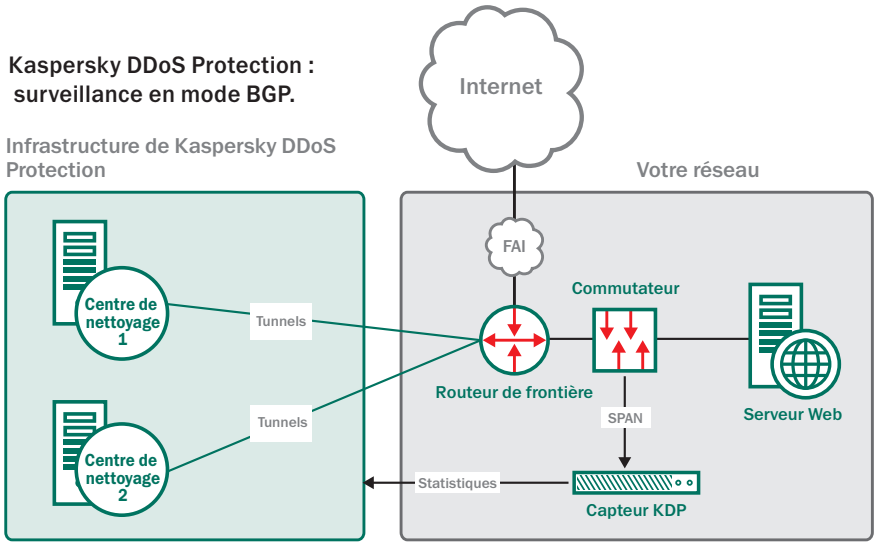
PROTECTION DES INFRASTRUCTURES CRITIQUES

Protection des systèmes de contrôle et réseaux industriels

Kaspersky Endpoint Security for Business offre une protection « en mode industriel » qui protège vos terminaux ICS/SCADA contre les menaces et les vulnérabilités qui constituent la porte d'entrée privilégiée pour de nombreux criminels qui ciblent les systèmes les plus importants.

Collaborant avec de grands fournisseurs industriels de systèmes automatiques tels qu'Emerson, Rockwell Automation et Siemens, Kaspersky Lab a mis en place de nombreuses procédures spécialisées pour assurer la validation et la compatibilité avec les technologies opérationnelles du client. Ceci nous permet de garantir une protection efficace des infrastructures essentielles sans impact sur la production.

Kaspersky DDoS Protection : surveillance en mode BGP.



SERVICES PROFESSIONNELS DE KASPERSKY LAB

Pour les clients équipés d'installations informatiques complexes, les services professionnels de déploiement et de mise à jour, de formation et de vérification Kaspersky Lab sont conçus pour s'assurer que les solutions Kaspersky Security for Business sont correctement configurées, déployées et gérées afin d'offrir des performances optimales.

KASPERSKY SMALL OFFICE SECURITY

Une protection optimale spécialement pensée pour les petites entreprises.

Une protection puissante, plus rapide et plus simple que jamais à utiliser.
- Solution spécialement conçue pour les petites entreprises jusqu'à 25 utilisateurs.
- Facile à installer et à utiliser : aucune formation requise
- Console Web pour une administration à distance basée sur Internet.

FAIBLE EXPERTISE TECHNIQUE REQUISE
La solution Kaspersky Small Office Security a été conçue pour que même les personnes qui n'ont pas la fibre technique puissent l'installer et l'utiliser facilement. Elle est dotée d'assistants d'installation pratiques qui vous guident automatiquement à travers des étapes telles que :

- La configuration, y compris la suppression de solutions de protection existantes contre les programmes malveillants
- Le réglage des commandes et le choix des politiques les mieux adaptées pour vous et votre entreprise
- Le téléchargement automatique de ces modifications sur plusieurs ordinateurs à la fois

Tout est administré par un tableau de bord basé sur le Web pour que vous ou une personne de votre choix puissiez gérer votre sécurité informatique à distance via Internet.

Kaspersky Small Office Security offre une sécurité exceptionnelle, transparente et efficace, si bien que vous oublierez presque sa présence.

PLUSIEURS NIVEAUX DE PROTECTION
Kaspersky Small Office Security protège vos PC et Mac, serveurs, tablettes et smartphones.

- Protection en temps réel basée sur le cloud contre les cyber-menaces (connues ou nouvelles).
- Le module « Safe Money » protège les transactions financières en ligne contre les pirates et l'usurpation d'identité.
- Des contrôles pour vous permettre de gérer la navigation de vos employés sur Internet et les réseaux sociaux.
- Le chiffrement pour protéger la confidentialité de vos activités et des données personnelles de vos clients.
- Des technologies anti-phishing pour vous protéger contre les sites Internet frauduleux.
- Filtrage puissant des courriers indésirables.
- Gestion sécurisée des mots de passe.*
- Sauvegarde automatique de vos données via Dropbox

FACTEUR D'ÉCONOMIES
En plus de vous protéger contre les attaques de pirates informatiques visant à voler votre argent, Kaspersky Small Office Security vous aide à maintenir la productivité de vos employés en régulant leur accès au Web et en définissant les moments où ils peuvent surfer ou envoyer des messages. Des fonctionnalités de protection avancées comme le chiffrement garantissent à vos clients que leurs données sont en sécurité entre vos mains, ce qui permet d'accroître votre potentiel commercial et la satisfaction de vos clients.

* Efficace pour les applications 32 bits uniquement. Comprend les appareils Android et iOS.

CONTRATS DE MAINTENANCE ET SUPPORT KASPERSKY LAB (MSA)

Une assistance de qualité en cas d'incident, de problèmes de configuration, d'incompatibilité et autre est essentielle pour les entreprises qui recherchent la tranquillité d'esprit et une disponibilité optimale.

Les contrats d'Assistance et de Maintenance Kaspersky Lab (MSA) offrent l'assurance de la continuité de vos services, ainsi qu'une assistance de qualité pour le maintien du niveau de sécurité de vos infrastructures. Ces contrats prévoient une assistance optimale en cas d'incident, allant du conseil à la configuration à la gestion des infections par des programmes malveillants, contribuant ainsi à maintenir la stabilité et l'efficacité de votre entreprise.

Les contrats de maintenance et d'assistance Kaspersky Lab couvrent les problèmes suivants :

- Épidémies mondiales de virus
- Pannes importantes en raison de la complexité des infrastructures
- Optimisation du déploiement et correctifs personnalisés
- Problèmes d'incompatibilité du réseau
- Processus de mise à niveau du produit Kaspersky Lab
- Analyse des logiciels malveillants
- Assistance pour la configuration et l'installation du produit*
- Déploiement des correctifs et autres mises à jour*

À chaque fois que votre équipe aura besoin d'aide, les spécialistes Kaspersky Lab seront disponibles par le biais de lignes téléphoniques prioritaires dédiées en langue locale, dans des délais d'intervention adaptés aux besoins de votre entreprise. Le schéma ci-dessous décrit les options d'assistance disponibles.

	Assistance standard		Assistance supérieure	
	MSA Starter	MSA Plus	MSA Business	MSA Enterprise
Ligne téléphonique prioritaire	Oui	Oui	Oui	Oui
Responsable technique du compte	Non	Non	Oui	Oui, dédié
Assistance en langue locale	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Assistance, niveau de gravité 1	8 x 5	8 x 5	24 x 7 x 365	24 x 7 x 365
Délai d'intervention, niveau de gravité 1	8 heures de travail	6 heures de travail	4 heures	30 minutes
Assistance, niveau de gravité 2	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Services professionnels Consultation	Non	Non	Coût additionnel	Bilan technique et rapports personnalisés
Nombre d'incidents	6	12	36	Illimité

*Options payantes pour MSA Business non disponibles pour MSA Starter et MSA Plus.

KASPERSKY LAB DANS LE MONDE

Kaspersky Lab opère dans 200 pays et territoires et possède des bureaux dans 30 pays.

Nous intégrons et respectons les cultures et traditions locales des entreprises en leur apportant des solutions d'envergure internationale.

www.kaspersky.fr

APAC

1. Australie
2. Chine
3. Hong Kong
4. Inde
5. Corée
6. Malaisie

Europe

7. Autriche
8. France
9. Allemagne
10. Italie
11. Pays-Bas
12. Portugal
13. Espagne
14. Norvège
15. Suisse
16. Royaume-Uni

Marchés émergents

17. Lettonie
18. Pologne
19. Roumanie
20. Slovénie
21. Afrique du Sud
22. Turquie
23. Ukraine
24. Émirats arabes unis

Japon

25. Japon (Tokyo)

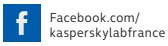
Amérique du Nord

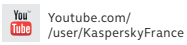
26. Canada
27. États-Unis d'Amérique (Boston)
28. États-Unis d'Amérique (Miami)

Russie et CEI

29. Russie
30. Kazakhstan


Twitter.com/
kasperskyfrance


Facebook.com/
kasperskylabfrance


Youtube.com/
/user/KasperskyFrance

Kaspersky Lab ZAO, Moscou, Russie
www.kaspersky.fr

Tout savoir sur la sécurité sur Internet :
www.securelist.com

Trouver un partenaire près de chez vous :
www.kaspersky.fr/partners

Catalog_SP1/mai15/Global

KASPERSKY lab