KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Contrôles des terminaux

Les outils de contrôle des terminaux de Kaspersky sont intégrés à notre technologie haut de gamme de protection contre les programmes malveillants de façon à permettre à votre entreprise de garder une longueur d'avance sur les nouvelles menaces.

CONTRÔLE DES APPLICATIONS ET LISTE BLANCHE DYNAMIQUE

Le **contrôle des applications** de Kaspersky basé sur une liste blanche dynamique renforce le niveau de sécurité en permettant aux administrateurs d'établir des politiques pour autoriser, bloquer ou réglementer l'utilisation des applications (ou des catégories d'applications).

En s'appuyant sur ces technologies, les sociétés peuvent mettre en œuvre une politique de blocage par défaut (default deny), sans effort. Dans ce scénario, toutes les applications sont bloquées par défaut. L'administrateur définit ensuite une liste d'applications dont il autorise l'exécution. Kaspersky facilite le travail de l'administrateur en regroupant des centaines de millions d'applications par catégories afin de créer simplement des règles d'utilisation. La base d'applications autorisées peut être créée localement par l'administrateur ou développée à partir des catégories prédéfinies par Kaspersky Lab.

Cette technologie intègre le module de **contrôle des privilèges des applications** qui surveille et contrôle en permanence l'activité des applications. Kaspersky peut imposer des restrictions au niveau des capacités d'une application à écrire dans des registres, à accéder à des ressources telles que le stockage, à contrôler et à modifier des données utilisateur, et bien plus.

Pour finir, la **liste blanche** créée par Kaspersky recense des programmes dont la légitimité est examinée et garantie en permanence. En réalité, nous sommes le seul éditeur de solutions de sécurité qui crée une liste blanche en s'appuyant sur son propre laboratoire d'experts !

FILTRAGE DE CONTENU WEB

Un grand nombre de sites Web contiennent des documents inappropriés sur le lieu de travail. C'est pour cela, entre autres, qu'il est essentiel d'utiliser des fonctionnalités de filtrage de contenu Web avancées.

Kaspersky maintient en permanence à jour une liste de sites Internet regroupés dans des catégories (jeux d'argent, sites pour adultes, recherche, etc.). Les administrateurs peuvent facilement définir des politiques de navigation selon ces catégories ou les personnaliser pour créer leurs propres listes. Les sites malveillants sont automatiquement bloqués.

Les politiques peuvent être établies selon un planning autorisant la navigation à certaines périodes de la journée et appliquées rapidement et en toute simplicité au sein de la société dans la mesure où la fonctionnalité du filtrage de contenu Web de Kaspersky s'intègre à votre architecture Active Directory.

L'approche innovante de Kaspersky permet à cette technologie de s'appliquer directement sur le terminal. En d'autres termes, toute politique configurée sera ainsi appliquée même lorsque l'utilisateur n'est pas connecté au réseau.

CONTRÔLE DES PÉRIPHÉRIQUES

La désactivation d'un port USB ne permet pas toujours de résoudre vos problèmes relatifs aux périphériques amovibles. Souvent, un niveau de contrôle plus granulaire est nécessaire pour garantir la productivité et la sécurité de l'utilisateur. Par exemple, si un utilisateur doit connecter une clé USB cryptographique pour accéder au réseau via un VPN, mais qu'il n'est pas supposé utiliser de périphériques de stockage amovibles, on ne peut pas imposer une politique désactivant l'usage des ports USB.

Kaspersky permet à l'administrateur d'établir des politiques et de contrôler, à tout moment, tout périphérique connecté sur chacun des ports de connexion (et pas uniquement ceux de type USB). L'administrateur est ainsi en mesure de réglementer les périphériques autorisés à se connecter, à lire ou à écrire des données, mais aussi de définir l'heure d'application d'une politique ainsi que les types de périphérique autorisés. Pour une sécurité optimale, ces contrôles peuvent être appliqués sur un périphérique spécifique à l'aide de son numéro de série.

SIMPLICITÉ D'ADMINISTRATION

Dans la mesure où Kaspersky a été conçu pour l'administrateur, tous les contrôles des périphériques s'intègrent à Active Directory. L'élaboration des politiques est donc à la fois simple et rapide. Tous ces contrôles sont effectués à partir d'une unique console : l'administrateur dispose ainsi d'une seule interface intuitive qui ne nécessite aucune formation supplémentaire.

Comment acheter

Les **outils de contrôle** de Kaspersky ne sont pas vendus séparément mais sont activés dans les versions suivantes de **Kaspersky Security for Business** :

- Endpoint Security, Select
- Endpoint Security, Advanced
- Kaspersky Total Security for Business

LES FONCTIONNALITÉS NE SONT PAS TOUTES DISPONIBLES SUR L'ENSEMBLE DES PLATES-FORMES.
Pour en savoir plus, rendez-vous sur **www.kaspersky.com/fr**

KASPERSKY LAB FRANCE
IMMEUBLE L'EUROPÉEN, BÂT C
2 RUE JOSEPH MONIER
92859 RUEIL-MALMAISON CEDEX
FRANCE
commercial@kaspersky.fr
www.kaspersky.fr

KESB-CONTROL/Version 0.2/NOV12/Mondial