KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Technologie de chiffrement

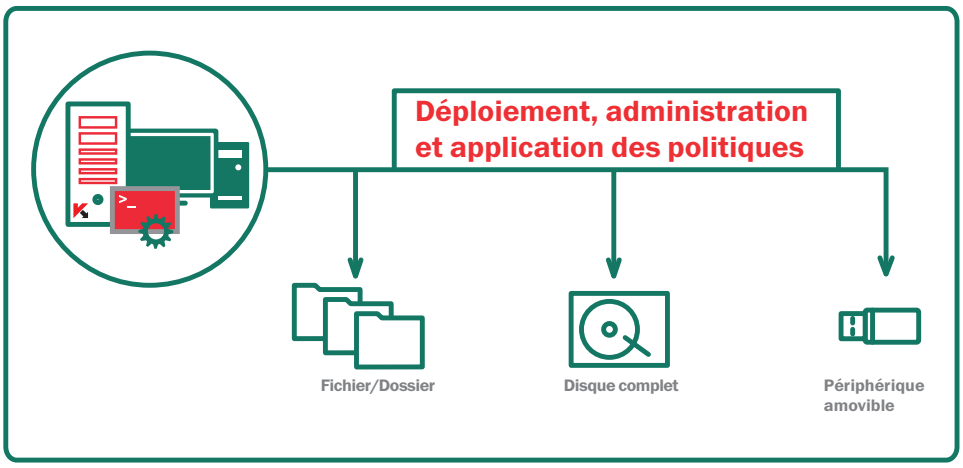
Le chiffrement empêche tout accès non autorisé en cas de perte d'un PC ou d'un autre support contenant des données.

La technologie de chiffrement de Kaspersky Lab protège les données sensibles en cas de perte ou de vol des périphériques. La solution allie des fonctions de chiffrement intégrées aux solutions de protection de Kaspersky. Cette solution a été développée intégralement par Kaspersky : le déploiement et l'administration s'effectuent donc en toute simplicité à partir d'une unique console via une seule politique.

Protégez vos données en toute simplicité et de manière sécurisée grâce à la technologie de chiffrement de Kaspersky :

- DISQUE COMPLET
- AU NIVEAU DES FICHIERS ET DES DOSSIERS
- PÉRIPHÉRIQUES AMOVIBLES ET INTERNES

ADMINISTRATION VIA UNE CONSOLE UNIQUE



CHIFFREMENT SÉCURISÉ ET ÉPROUVÉ

Kaspersky utilise un algorithme de chiffrement reposant sur la norme de cryptage AES avec une clé de 256 bits.

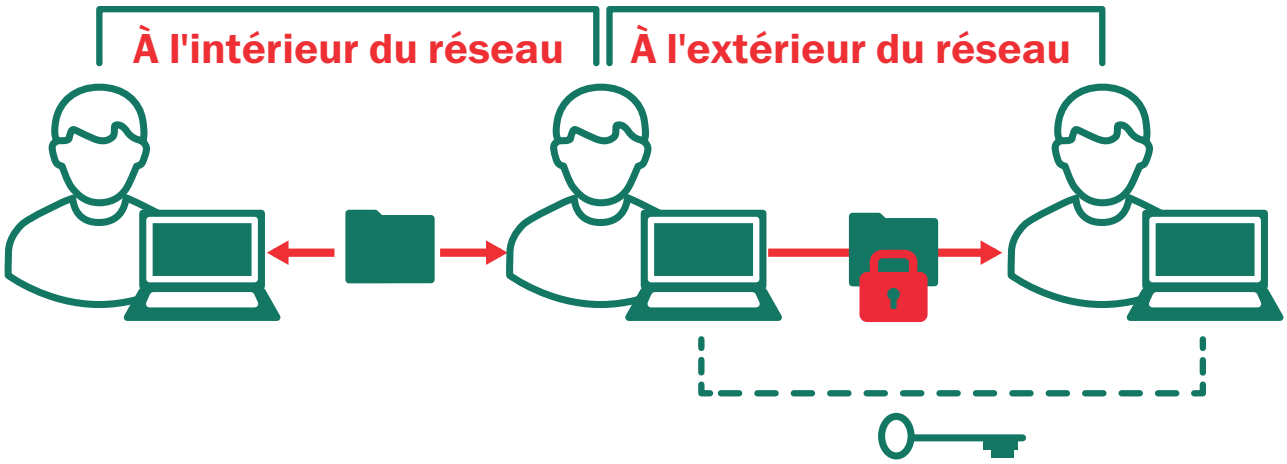
CHOIX DE LA MÉTHODE DE CHIFFREMENT

Pour couvrir tous les cas de figure, le chiffrement au niveau des fichiers et des dossiers et celui du disque complet peuvent être utilisés pour protéger les données sur les disques durs ou les périphériques amovibles.

TRANSPARENCE POUR LES UTILISATEURS FINAUX

La technologie de chiffrement de Kaspersky Lab reste transparente pour les applications, y compris lors de la configuration. Les informations sont protégées à la volée ce qui permet de préserver la productivité de l'utilisateur. L'authentification au système de chiffrement se fait en toute transparence grâce à un mécanisme de SSO (Single Sign On).

Lors du transfert d'un fichier, la solution de chiffrement de Kaspersky est transparente pour l'utilisateur au sein du réseau. Les données destinées à des utilisateurs externes peuvent être regroupées dans des conteneurs protégés par un mot de passe. Le mot de passe peut être envoyé au destinataire à des fins de déchiffrement via un canal séparé.



FONCTIONNALITÉS DE CHIFFREMENT :

CODE SOURCE INTÉGRÉ
Kaspersky intègre toutes ces solutions de protection dans un logiciel unique afin que vous n'ayez pas à déployer et administrer des solutions différentes pour la protection contre les programmes malveillants, le contrôle des terminaux et le chiffrement.

POLITIQUES INTÉGRÉES NATURELLEMENT ET INTERCONNECTÉES
Le code source intégré permet à l'administrateur de créer des politiques uniques. Par exemple, le service informatique peut approuver uniquement la connection de certains supports amovibles et leur imposer une politique de chiffrement en associant ainsi les fonctionnalités de contrôle des périphériques et de chiffrement.

PARAMÈTRES PERSONNALISABLES « PRÊTS À L'EMPLOI »
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 d'extensions de fichiers (Documents Microsoft Office, archives de messages électroniques).

CLÉ ADMINISTRATEUR CENTRALISÉE EN CAS D'URGENCE
L'administrateur de la sécurité est en mesure de déchiffrer des données sur les lecteurs en cas de défaillance matérielle ou logicielle.

RÉCUPÉRATION DES MOTS DE PASSE
L'utilisateur peut récupérer le mot de passe de pré-démarrage (pre-boot) ou accéder à des données chiffrées via un mécanisme de challenge/response.

Comment acheter

La technologie de chiffrement de Kaspersky n'est pas vendue séparément et est activée dans les versions suivantes **Kaspersky Security for Business** :

- 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**

KESB-ET/Version 0.1/Nov12/Global

KASPERSKY lab