▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Technologie de chiffrement

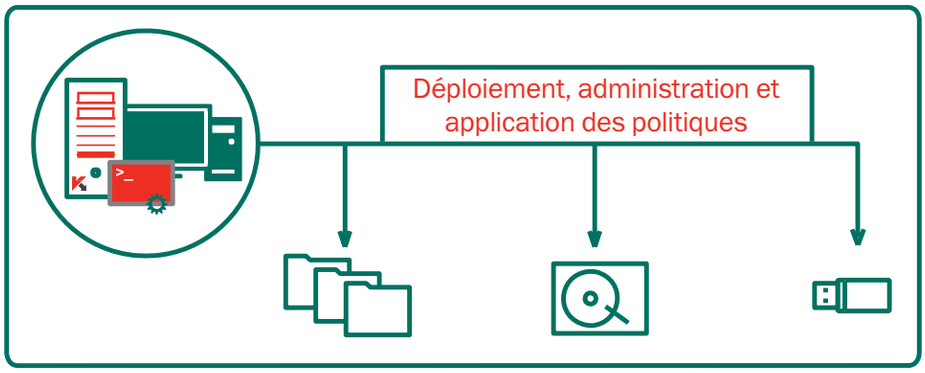
Empêche l'accès non autorisé à vos données en cas de perte ou de vol d'un appareil ou d'une attaque malveillante ciblant vos données.

La protection proactive des données et la conformité sont un impératif mondial. 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 au repos et en mouvement.

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

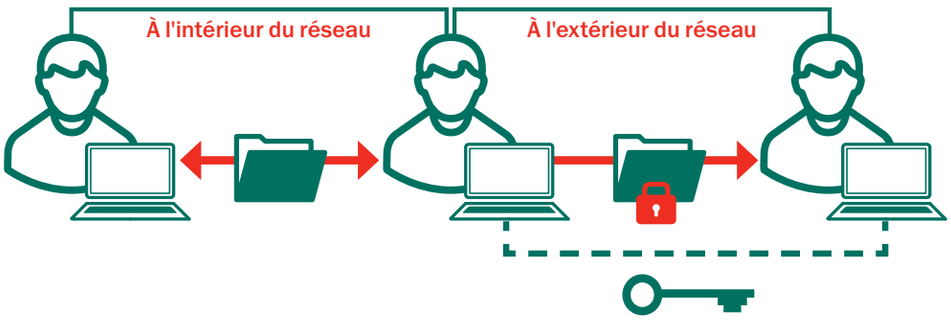
Kaspersky Lab utilise la norme Advanced Encryption Standard (AES) avec une longueur de clé de 256 bits, une gestion des clés et un entiercement simplifiés. Prend en charge les plateformes de technologie Intel® AES-NI, UEFI et GPT.

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 de Kaspersky Lab 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.

Comment vous procurer ce produit ?

La technologie de chiffrement de Kaspersky Lab n'est pas vendue séparément. Elle est disponible uniquement dans les versions Advanced et Total de Kaspersky Endpoint Security for Business, en tant que module d'une plateforme de sécurité complète, riche en fonctionnalités

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

Prend en charge l'authentification à deux facteurs via la création de 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.

Kaspersky Endpoint Security for Business/Chiffrement/

KASPERSKY lab