KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Tecnología de cifrado

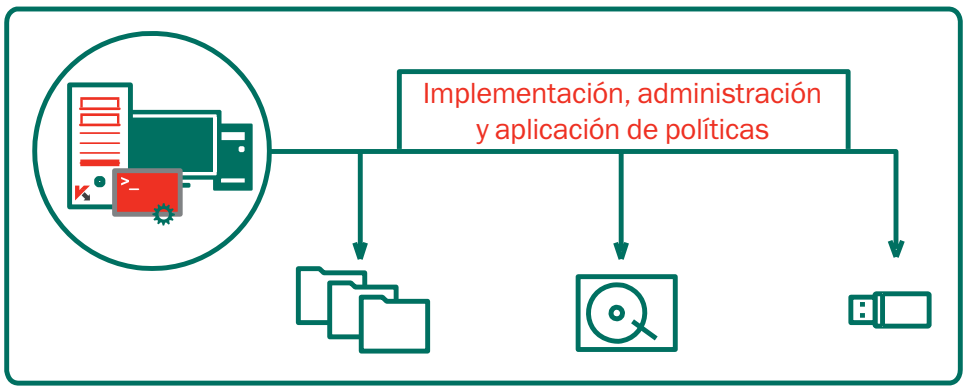
Evita el acceso no autorizado a los datos causado por pérdidas del dispositivo, robo o malware de robo de datos.

La protección proactiva de los datos y el cumplimiento es un imperativo mundial. La tecnología de cifrado de Kaspersky Lab protege los datos valiosos de la pérdida accidental, el robo del dispositivo y los ataques de malware. Gracias a que combina las sólidas tecnologías de cifrado con las tecnologías de protección de terminales líderes en la industria de Kaspersky Lab, nuestra plataforma integrada protege los datos en reposo y en movimiento.

Y puesto que es un producto de Kaspersky Lab, es fácil de implementar y administrar desde una consola de administración centralizada, mediante una única política.

Evite la pérdida de datos y el acceso no autorizado a la información con la tecnología de cifrado de Kaspersky Lab:

- **Cifrado del disco completo (FDE)**
- **Nivel de archivos/carpetas (FLE)**
- **Dispositivos extraíbles e internos**



ADMINISTRADO A TRAVÉS DE UNA ÚNICA CONSOLA DE ADMINISTRACIÓN

CRIPTOGRAFÍA SEGURA ESTÁNDAR DE LA INDUSTRIA

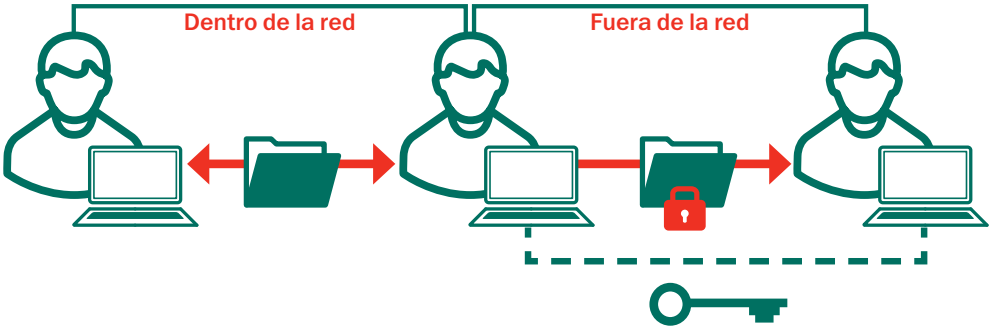
Kaspersky Lab utiliza el Estándar de cifrado avanzado (AES) con claves de 256 bits de longitud y administración y almacenamiento de claves simplificados. Es compatible con la tecnología de Intel® AES-NI y las plataformas UEFI y GPT.

FLEXIBILIDAD TOTAL

Kaspersky Lab ofrece cifrado a nivel de archivos y carpetas (FLE) y cifrado de disco completo (FDE), para abarcar todas las posibles situaciones de uso. Los datos pueden estar protegidos en las unidades de disco duro y los dispositivos extraíbles. El modo "portátil" permite la utilización y la transferencia de datos en medios extraíbles cifrados, incluso en equipos donde el software de cifrado no está instalado, facilitando el intercambio de datos "fuera del perímetro".

INICIO DE SESIÓN ÚNICO, TRANSPARENCIA PARA EL USUARIO FINAL

Desde la configuración al uso diario, la tecnología de cifrado de Kaspersky Lab funciona de forma transparente en todas las aplicaciones, sin que ello impida la productividad del usuario final. El inicio de sesión único garantiza cifrado sin problemas, el usuario final puede incluso no saber que la tecnología se está ejecutando.



El cifrado de Kaspersky Lab permite una transferencia de archivos sin problemas y transparente entre los usuarios de dentro y fuera de la red.

CARACTERÍSTICAS DE CIFRADO

INTEGRACIÓN SIN PROBLEMAS CON LAS TECNOLOGÍAS DE SEGURIDAD DE KASPERSKY LAB

Integración completa con las tecnologías antimalware, de control de terminales y de administración de Kaspersky Lab para una verdadera seguridad de varios niveles, construida sobre una base de código común. Por ejemplo, una sola política puede aplicar el cifrado en determinados dispositivos extraíbles. Aplicación de configuraciones de cifrado bajo la misma política antimalware, de control de dispositivos y otros elementos de seguridad de terminales. No hay necesidad de implementar y administrar soluciones independientes. La compatibilidad con el hardware de red se activa de forma automática antes de que se implemente el cifrado; admite de forma estándar las plataformas UEFI y GPT.

CONTROL DE ACCESO BASADO EN FUNCIONES

En las grandes organizaciones, elija delegar la administración de cifrado mediante el control de acceso basado en funciones. Esto permite una administración de cifrado menos compleja.

Cómo comprar

La tecnología de cifrado de Kaspersky no se vende por separado. Solo está disponible en los niveles "Advanced" y "Total" de Kaspersky Endpoint Security for Business, como un componente de una plataforma de seguridad completa e integral.

AUTENTICACIÓN PREVIA AL ARRANQUE (PBA)

Las credenciales de usuario se exigen incluso antes de que se inicie el sistema operativo, ofreciendo una capa adicional de seguridad, con inicio de sesión único opcional. La PBA de tecnología de cifrado de Kaspersky Lab también está disponible para las distribuciones de teclado diferentes a QWERTY.

TARJETA INTELIGENTE Y AUTENTICACIÓN DE TOKEN

Admite autenticación de dos factores mediante conocidas tarjetas inteligentes y tokens, eliminando la necesidad de nombres de usuario y contraseñas adicionales y mejorando experiencia del usuario final.

RECUPERACIÓN DE EMERGENCIA

Los administradores pueden descifrar los datos en caso de una falla de hardware o software. La recuperación de contraseña de usuario para PBA o acceso a datos cifrados se implementa a través de un sencillo mecanismo de desafío/respuesta.

IMPLEMENTACIÓN OPTIMIZADA, CONFIGURACIÓN PERSONALIZABLE

Para facilitar la implementación, la funcionalidad de cifrado de Kaspersky Lab solo se habilita en los niveles "Advanced" y "Total" de Kaspersky Endpoint Security for Business, sin necesidad de una instalación independiente. La configuración de la codificación es predefinida, pero se puede personalizar para las carpetas comunes como Mis documentos, Escritorio, carpetas nuevas, extensiones de los archivos y grupos, como documentos de Microsoft Office o archivos de mensajes.

© 2015 Kaspersky Lab ZAO. Todos los derechos reservados. Las marcas registradas y marcas de servicio son propiedad de sus respectivos propietarios.
Microsoft, Windows Server y SharePoint son marcas comerciales registradas o marcas comerciales de Microsoft Corporation en los Estados Unidos y otros países.

KASPERSKY lab