KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Tecnologia de Encriptação

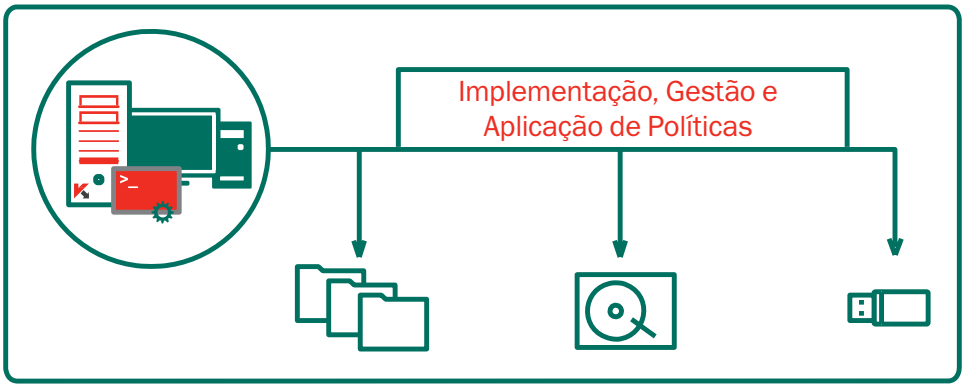
Impedir o acesso não autorizado aos dados em resultado de perda ou roubo do dispositivo ou de malware de roubo de dados.

A conformidade e proteção de dados proativa é um imperativo global. A tecnologia de encriptação da Kaspersky Lab protege dados valiosos contra perdas acidentais, roubo de dispositivos e ataques de malware direcionados. Combinando uma forte tecnologia de encriptação com as tecnologias de proteção de terminais líderes da indústria da Kaspersky Lab, a nossa plataforma integrada protege os dados em repouso e em movimento.

Como é da Kaspersky Lab, é fácil de implementar e administrar a partir de uma consola de gestão centralizada, utilizando uma única política.

Evite a perda de dados e o acesso a informações não autorizadas com a tecnologia de encriptação da Kaspersky Lab:

- Encriptação da totalidade do disco (FDE)
- Nível de ficheiros/pastas (FLE)
- Dispositivos amovíveis e internos



ADMINISTRADO ATRAVÉS DE UMA ÚNICA CONSOLA DE GESTÃO

ENCRIPTAÇÃO SEGURA PADRÃO NA INDÚSTRIA

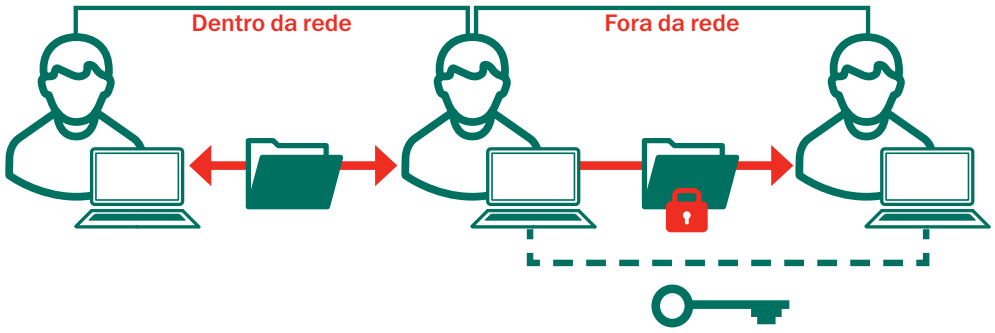
A Kaspersky Lab utiliza a Norma de encriptação Avançada (AES) com chave de 256 bits com depósito e gestão de chaves simplificadas. Suporta plataformas Intel® com tecnologia AES-NI, UEFI e GPT.

FLEXIBILIDADE TOTAL

A Kaspersky Lab oferece encriptação ao nível dos ficheiros/pastas (FLE) e encriptação da totalidade do disco (FDE), abrangendo todos os possíveis cenários de utilização. Os dados podem ser protegidos tanto em discos rígidos como em dispositivos amovíveis. O "modo portátil" permite a utilização e transferência de dados em suportes amovíveis encriptados, mesmo em computadores onde não esteja instalado software de encriptação, facilitando a troca de dados segura "fora do perímetro".

INÍCIO DE SESSÃO ÚNICO, TRANSPARÊNCIA PARA O UTILIZADOR FINAL

Desde a configuração à utilização diária, a tecnologia de encriptação da Kaspersky Lab funciona de forma transparente em todas as aplicações, sem afetar a produtividade do utilizador final. O início de sessão único garante uma encriptação simples – o utilizador final pode nem se aperceber de que a tecnologia está em execução.



A encriptação da Kaspersky Lab permite uma transferência simples e transparente de ficheiros entre utilizadores dentro e fora da rede.

FUNCIONALIDADES DE ENCRIPTAÇÃO

INTEGRAÇÃO PERFEITA COM AS TECNOLOGIAS DE SEGURANÇA DA KASPERSKY LAB

Integração completa com as tecnologias de gestão, anti-malware e controlo de terminais da Kaspersky Lab, para uma segurança realmente multicamadas construída sobre uma base de código comum. Por exemplo, uma política única pode forçar a encriptação em dispositivos amovíveis específicos. Aplicação de definições de encriptação com a mesma política que o anti-malware, controlo de dispositivos e outros elementos de segurança de terminais. Não é necessário implementar e gerir soluções separadas. A compatibilidade do hardware de rede é verificada automaticamente antes de a encriptação ser implementada; o suporte para plataformas UEFI e GPT é fornecido de série.

CONTROLO DE ACESSO COM BASE EM FUNÇÕES

Em empresas maiores, opte por delegar a gestão da encriptação utilizando a funcionalidade de controlo de acessos com base em funções. Isso permite uma gestão menos complexa da encriptação.

Como adquirir

A tecnologia de encriptação da Kaspersky não é vendida em separado. É ativada apenas nas camadas "Advanced" e "Total" do Kaspersky Endpoint Security for Business, como componente de uma plataforma de segurança abrangente e completa

AUTENTICAÇÃO PRÉ-ARRANQUE (PBA)

As credenciais do utilizador são necessárias antes de o sistema operacional arrancar, o que fornece uma camada adicional de segurança, com um início de sessão único opcional. A PBA da tecnologia de encriptação da Kaspersky Lab também está disponível em esquemas de teclados não QWERTY.

AUTENTICAÇÃO POR CARTÃO INTELIGENTE E TOKENS

Suporta a autenticação de dois fatores através de formas populares de cartões inteligentes e tokens, eliminando a necessidade de outros nomes de utilizador e palavras-passe e melhorando a experiência do utilizador.

RECUPERAÇÃO DE EMERGÊNCIA

Os administradores podem desencriptar dados em caso de falha de hardware ou software. A recuperação de palavras-passe para acesso por PBA ou dados encriptados é implementada através de um simples mecanismo de pergunta/resposta.

IMPLEMENTAÇÃO OTIMIZADA, CONFIGURAÇÕES PERSONALIZÁVEIS

Para facilitar a implementação, a funcionalidade de encriptação da Kaspersky Lab apenas é ativada nas camadas "Advanced" e "Total" do Kaspersky Endpoint Security for Business, sem que sejam necessárias instalações separadas. As definições de encriptação são predefinidas, mas podem ser personalizadas para pastas comuns como Os meus documentos, Ambiente de trabalho, pastas novas, extensões de ficheiros e grupos, como documentos do Microsoft Office ou arquivos de mensagens.

Kaspersky Endpoint Security for Business/Encriptação/

KASPERSKY lab