▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Tecnologia de criptografia

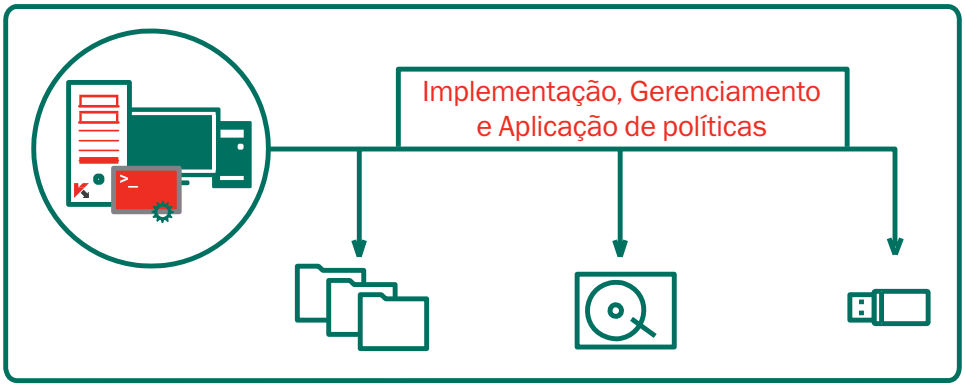
Impede o acesso não autorizado a dados causado pela perda ou roubo do dispositivo, ou malware para roubo de dados.

Proteção de dados e conformidade proativos são um imperativo global. A tecnologia de criptografia da Kaspersky Lab protege os dados valiosos contra perda acidental, roubo do dispositivo e ataques de malware direcionados. Ao combinar a poderosa tecnologia de criptografia com as tecnologias líderes do setor de proteção de endpoints da Kaspersky Lab, a nossa plataforma integrada protege os dados em repouso e em movimento.

Por ser da Kaspersky Lab, é fácil de implementar e administrar a partir de um console de gerenciamento centralizado, utilizando uma única política.

Impede a perda de dados e o acesso não autorizado as informações com a Tecnologia de criptografia da Kaspersky Lab:

- Criptografia do disco completo (FDE)
- Arquivo/Nível de pasta (FLE)
- Dispositivos removíveis e internos



ADMINISTRADO ATRAVÉS DE UM ÚNICO CONSOLE DE GERENCIAMENTO

CRIPTOGRAFIA SEGURA PADRÃO DO SETOR

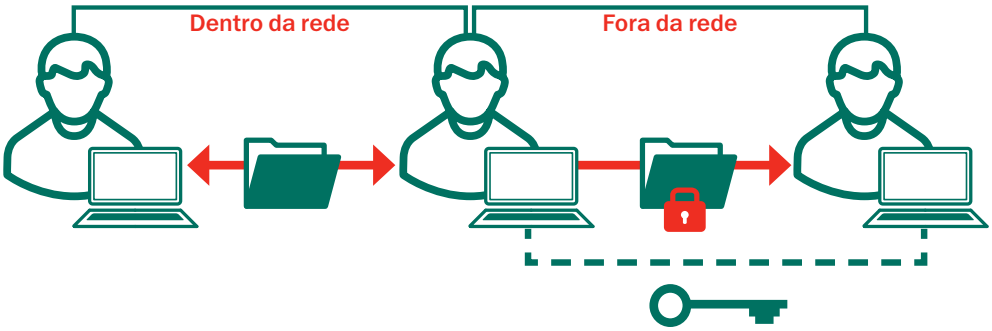
A Kaspersky Lab utiliza criptografia AES (Advanced Encryption Standard) de tamanho de chave de 256 bits com gerenciamento e garantia principais simplificados. É compatível com tecnologia Intel® AES-NI, plataformas UEFI e GPT.

FLEXIBILIDADE COMPLETA

A Kaspersky Lab oferece criptografia em nível de arquivo e pasta (FLE) e criptografia do disco completo (FDE), que abrange todos os possíveis cenários de uso. Os dados podem ser protegidos tanto nos discos rígidos como nos dispositivos removíveis. O "Modo portátil" permite o uso e transferência de dados em mídias removíveis criptografadas, mesmo em computadores sem o programa de criptografia - facilitando troca segura de dados "fora do perímetro".

LOGIN ÚNICO, TRANSPARÊNCIA DE USUÁRIO FINAL

Da configuração ao uso diário, a tecnologia de criptografia da Kaspersky Lab funciona de forma transparente em todos os aplicativos, sem impedir a produtividade do usuário final. O login único garante criptografia integrada - o usuário final não percebe que a tecnologia está sendo executada.



A criptografia da Kaspersky Lab permite a transferência de arquivos transparente e integrada entre os usuários dentro e fora da rede.

RECURSOS DE CRIPTOGRAFIA

INTEGRAÇÃO PERFEITA COM AS TECNOLOGIAS DE SEGURANÇA DA KASPERSKY LAB

Integração completa com antimalware da Kaspersky Lab, controles de edpoints e tecnologias de gerenciamento para uma verdadeira segurança multicamadas construída sobre uma base de código comum. Por exemplo, uma única política poderia aplicar a criptografia em dispositivos removíveis específicos. Aplica configurações de criptografia sob a mesma política como antimalware, controle de dispositivos e outros elementos de segurança de endpoints. Não há necessidade de implementar e gerenciar soluções distintas. A compatibilidade de hardware de rede é automaticamente verificada antes da implementação da criptografia; suporte padrão para as plataformas UEFI e GPT.

CONTROLE DE ACESSO COM BASE EM FUNÇÃO

Em organizações maiores, opte por delegar o gerenciamento de criptografia usando a funcionalidade de controle de acesso com base em função. Isso permite o gerenciamento de criptografia menos complexo.

Como comprar

A tecnologia de criptografia Kaspersky não é vendida separadamente. Ela é ativada apenas nos níveis "Advanced" e "Total" do Kaspersky Endpoint Security for Business como um componente de uma plataforma de segurança completa e abrangente

AUTENTICAÇÃO PRÉ-INICIALIZAÇÃO (PBA)

As credenciais do usuário são necessárias antes que o sistema operacional inicialize, proporcionando uma camada adicional de segurança, com login único opcional. A tecnologia de criptografia PBA da Kaspersky Lab também está disponível para layouts de teclado diferentes do QWERTY.

AUTENTICAÇÃO POR CARTÃO INTELIGENTE E TOKEN

Compatível com autenticação de dois fatores através de marcas populares de cartões inteligentes e tokens, eliminando a necessidade de nomes de usuários e senhas adicionais e melhorando a experiência do usuário final.

RECUPERAÇÃO DE EMERGÊNCIA

Os administradores podem descriptografar os dados em caso de falha de hardware ou software. A recuperação de senha do usuário para PBA ou o acesso aos dados criptografados são implementados através de um mecanismo simples de desafio/resposta.

IMPLEMENTAÇÃO OTIMIZADA, CONFIGURAÇÕES PERSONALIZÁVEIS

Para facilitar a implementação, a funcionalidade de criptografia da Kaspersky Lab está habilitada somente dentro dos níveis "Advanced" e "Total" do Kaspersky Endpoint Security for Business, sem necessidade de instalação separada. As configurações de criptografia são pré-definidas, mas podem ser personalizadas para pastas comuns, como Meus Documentos, Área de Trabalho, novas pastas, extensões de arquivos e grupos, tais como documentos do Microsoft Office ou arquivos comprimidos de mensagens.

KASPERSKY lab