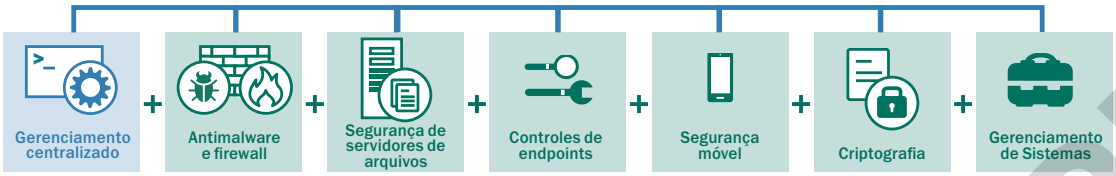
KASPERSKY ENDPOINT SECURITY FOR BUSINESS — ADVANCED



As ferramentas de gerenciamento de sistemas otimizam a eficiência e segurança de TI, enquanto a criptografia integrada protege dados sigilosos

O gerenciamento automatizado de correções e o gerenciamento de imagem do SO, a distribuição de software remoto e a integração SIEM ajudam a simplificar a administração, enquanto os inventários de hardware e software e o gerenciamento de licenças fornecem visibilidade e controle. A tecnologia de criptografia integrada adiciona uma camada poderosa de proteção de dados.

GERENCIAMENTO DE SISTEMAS

Gerenciamento de vulnerabilidades e correções — detecção e priorização automatizadas de vulnerabilidades do SO e de aplicativos, combinadas com a rápida distribuição automatizada de correções e atualizações.

Implementação do sistema operacional — fácil criação, armazenamento e implementação de imagens "golden" do SO a partir de um local centralizado, incluindo suporte a UEFI.

Distribuição e solução de problemas de software — implementação e aplicação remotas do software e atualização do SO disponível por demanda ou programada, incluindo suporte a Wake-on-LAN. A solução de problemas remota com economia de tempo e a distribuição eficiente de software são suportadas através da tecnologia Multicast.

Inventários de hardware e software e gerenciamento de licenças — a identificação, visibilidade e controle (incluindo bloqueio), juntamente com o gerenciamento de uso da licença, fornecem informações sobre todos os softwares e hardwares implementados por todo o ambiente, incluindo dispositivos removíveis. Estão disponíveis também: gerenciamento de licenças de software e hardware, detecção de dispositivos convidados, controles de privilégios e provisionamento de acesso.

Integração SIEM — suporte para sistemas IBM® QRadar e HP ArcSight SIEM.

Controle de acesso com base em função (Role Based Access Control — RBAC) — as responsabilidades administrativas podem ser atribuídas através de redes complexas, com exibição do console personalizada de acordo com as funções e direitos atribuídos

CRIPTOGRAFIA

Poderosa proteção de dados — a criptografia dos arquivos / pastas (FLE) e do disco completo (FDE) pode ser aplicada aos endpoints. O suporte para o "modo portátil" garante a administração de criptografia em todos os dispositivos que saem dos domínios administrativos.

Conexão flexível do usuário — autenticação pré-inicialização (Pre-boot authentication - PBA) para aumentar a segurança que inclui login único opcional para transparência do usuário. Também está disponível a autenticação com base em dois fatores ou em token.

Criação de políticas Integradas — integração única de criptografia com controles de aplicativos e dispositivos fornece uma camada adicional de segurança aprimorada e facilidade administrativa

O Kaspersky Endpoint Security for Business — ADVANCED também inclui todos os componentes dos NÍVEIS SELECT e CORE.