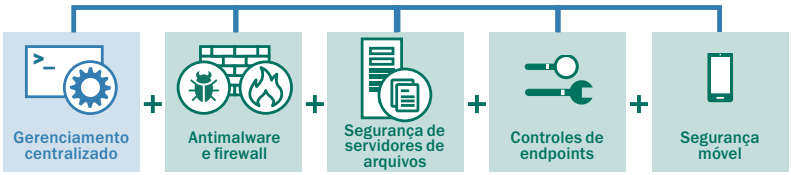
KASPERSKY ENDPOINT SECURITY FOR BUSINESS — SELECT



Poderosos controles de endpoints granulares combinados com segurança e gerenciamento proativos de dados e dispositivos móveis

Controles de aplicativos, da Web e de dispositivos, incluindo listas brancas dinâmicas suportadas pelo exclusivo laboratório interno da Kaspersky, adicionam uma nova dimensão para aprofundar a segurança de endpoints. Dispositivos móveis pertencentes à empresas e funcionários (BYOD) também são protegidos, e as plataformas são unificadas para gerenciamento juntamente com todos os endpoints protegidos através do console do Kaspersky Security Center. A proteção de servidores de arquivos garante que infecções não se disseminem para os endpoints protegidos por meio dos dados armazenados.

CONTROLES DE ENDPOINTS

Controle de Aplicativos com as Listras Brancas Dinâmicas — que usam as reputações de arquivos em tempo real entregues pela Kaspersky Security Network, os administradores de TI podem permitir, bloquear ou controlar aplicativos, incluindo a operação de um cenário de listas brancas de 'Negação Padrão' em um ambiente real ou de teste. O Controle de privilégios de aplicativos e a Verificação de vulnerabilidades monitoram aplicativos e restringem aqueles que operam de forma suspeita.

Controle da Web — políticas de navegação podem ser criadas com base em categorias predefinidas ou personalizáveis, garantindo supervisão abrangente e eficiência administrativa.

Controle de dispositivos — políticas de dados granulares que controlam a conexão de armazenamento removível e outros dispositivos periféricos podem ser definidas, programadas e aplicadas usando-se máscaras para implementação simultânea de diversos dispositivos.

SEGURANÇA DE SERVIDORES DE ARQUIVOS

Gerenciados juntamente com segurança de endpoints através do Kaspersky Security Center.

SEGURANÇA MÓVEL:

Poderosa segurança para dispositivos móveis — tecnologias avançadas, proativas e assistidas em nuvem combinam-se para entregar proteção em multicamadas de endpoints móveis em tempo real.

Componentes de proteção da Web, de antispam e de antiphishing aumentam ainda mais a segurança do dispositivo.

Antirroubo remoto — Bloqueio, Limpeza, Localização, Verificação do Chip, Alarme, Retrato e Limpeza total ou seletiva, todos impedem o acesso não autorizado a dados corporativos caso um dispositivo móvel seja perdido ou roubado. A habilitação do administrador e do usuário final, juntamente com o suporte do Google Cloud Management, oferece rápida ativação, se necessário.

Gerenciamento de aplicativos móveis (Mobile Application Management - MAM) — controla o limite do usuário ao executar aplicativos de listas brancas, impedindo a implementação de software indesejado ou desconhecido. '**Empacotamento de aplicativos**'isola dados corporativos em dispositivos pertencentes aos funcionários. Criptografia adicional ou "Limpeza seletiva" podem ser remotamente aplicadas.

Gerenciamento de dispositivos móveis (Mobile Device Management — MDM) — uma interface unificada para dispositivos **Microsoft® Exchange ActiveSync** e **iOS MDM** com implementação de políticas OTA (Over The Air, por conexão sem fio). **Samsung KNOX** com base em dispositivos Android™ também é compatível.

Portal de autoatendimento — permite o auto registro na rede de dispositivos aprovados de propriedade dos funcionários com instalação automática de todos os certificados e chaves necessários e a ativação de emergência por usuários / proprietários de recursos antirroubo, reduzindo a carga de trabalho administrativa de TI.

O Kaspersky Endpoint Security for Business - SELECT também inclui todos os componentes do nível CORE.