KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Controles de endpoints

Ferramentas de controle de endpoints poderosas, fortemente integradas com tecnologia de ponta antimalware e o único laboratório exclusivo de listas brancas do setor ajuda a proteger a sua empresa do dinâmico ambiente de ameaças de hoje em dia.

PROTEGE, APLICA, CONTROLA

Vulnerabilidades em aplicativos confiáveis, malware com base na Web e falta de controle sobre os dispositivos periféricos formam parte de um cenário de ameaças cada vez mais complexo. As ferramentas de aplicativos, Web e Controle de dispositivos da Kaspersky Lab permitem total controle sobre seus edpoints, sem comprometer a produtividade.

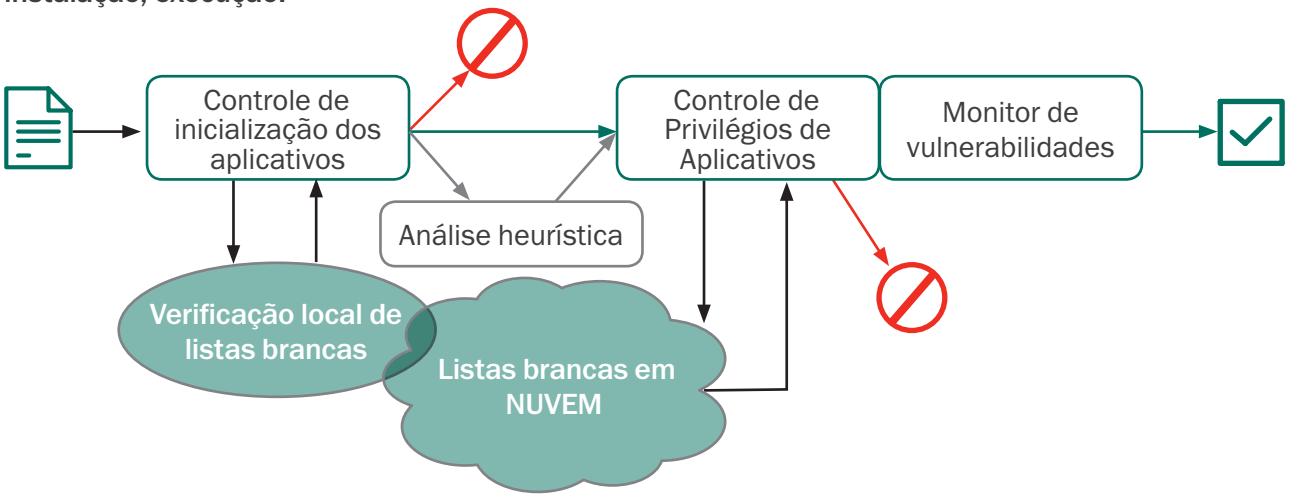
CONTROLE DE APLICATIVOS E LISTAS BRANCAS DINÂMICAS

Protege os sistemas contra ameaças conhecidas e desconhecidas, dando aos administradores controle total sobre os aplicativos e programas que podem ser executados em endpoints, independentemente do comportamento do usuário final. Além disso, permite o monitoramento da integridade dos aplicativos para avaliar comportamento e impedi-los de executar ações inesperadas que possam pôr em risco os edpoints ou a rede. A criação e aplicação de políticas simplificadas, personalizáveis ou automatizadas permitem:

- **Controle da inicialização de aplicativos**: Concessão, bloqueio, auditoria de inicialização de aplicativos. Orientar produtividade restringindo acesso a aplicativos não corporativos.
- **Controle de privilégio de aplicativos**: Regular e controlar o acesso de aplicativos aos recursos e dados do sistema. Classificar aplicativos como confiáveis, não confiáveis ou restritos. Gerenciar o acesso de aplicativos aos dados criptografados em endpoints, tais como informações postadas via navegadores da Web ou Skype.
- **Verificação de vulnerabilidades de aplicativos**: Defesa proativa contra ataques direcionados a vulnerabilidades em aplicativos confiáveis.

A maioria das soluções de controle oferece apenas a funcionalidade básica de bloqueio/acesso. As ferramentas de controle da Kaspersky Lab são únicas na sua utilização de bancos de dados de listas brancas com base em nuvem, possibilitando o acesso quase em tempo real aos dados de aplicativos mais recentes.

As tecnologias de controle de aplicativos da Kaspersky Lab usam bancos de dados de listas brancas com base em nuvem para analisar e monitorar aplicativos em todas as fases: download, instalação, execução.



Listas brancas dinâmicas, que podem ser ativadas por "Negação Padrão" abrangente, bloqueiam todos os aplicativos que tentam executar em qualquer estação de trabalho, a menos que explicitamente permitido pelos administradores. A Kaspersky Lab é a única empresa de segurança com um laboratório exclusivo de listas brancas que mantém um banco de dados constantemente monitorado e atualizado de mais de 500 milhões de programas.

A Negação Padrão **da Kaspersky Lab pode ser aplicada em um ambiente de teste**, permitindo que os administradores estabeleçam a legitimidade do aplicativo antes do bloqueio. Além disso, as categorias de aplicativos com base em assinaturas digitais podem ser criadas, impedindo que os usuários executem software legítimo que foi modificado por malware ou originário de uma fonte suspeita.

CONTROLES DA WEB

Monitora, filtra e controla os sites da Web que os usuários finais podem acessar no local de trabalho, aumentando a produtividade enquanto protege contra malware e ataques com base na Web.

Os avançados controles da Web da Kaspersky Lab são construídos em um diretório constantemente atualizado de sites da Web, agrupados em categorias (por exemplo, adultos, jogos, redes sociais, apostas). Os administradores podem facilmente criar políticas para proibir, limitar ou auditar o uso pelo usuário final de quaisquer sites individuais ou categorias de site, bem como criar suas próprias listas. Sites maliciosos são bloqueados automaticamente.

Com essa restrição, os controles da Web da Kaspersky Lab ajudam a impedir a perda de dados através de redes sociais e serviços de mensagens instantâneas. Políticas flexíveis possibilitam aos administradores que permitam navegar em determinadas horas do dia. A integração com o Active Directory faz com que políticas possam ser aplicadas em toda a organização de forma rápida e fácil.

Para maior segurança, os controles da Web da Kaspersky Lab são ativados diretamente nos endpoints, ou seja, as políticas são executadas mesmo quando o usuário não está conectado à rede.

CONTROLE DE DISPOSITIVOS

A desativação de uma porta USB nem sempre resolve os seus problemas de dispositivos removíveis. Por exemplo, uma porta USB desativada impacta outras medidas de segurança, como o acesso VPN com base em token.

Os controles de dispositivos da Kaspersky Lab permitem um nível mais granular de controle no nível do barramento, do tipo e do dispositivo – mantendo a produtividade do usuário final, ao mesmo tempo em que otimiza a segurança. Os controles podem ser aplicados ao número de série específico do dispositivo.

- Conecta/lê/escreve permissões para dispositivos bem como programação de tempo.
- Cria regras de controle de dispositivos com base em máscaras, eliminando a necessidade de conectar fisicamente os dispositivos para verificação de lista branca. Verificação simultânea de lista branca em diversos dispositivos.
- Controle de troca de dados através de dispositivos removíveis dentro e fora da organização, reduzindo o risco de perda ou roubo de dados.
- Integração com as tecnologias de criptografia da Kaspersky Lab para reforçar as políticas de criptografia em tipos específicos de dispositivo.

FÁCIL ADMINISTRAÇÃO

Todas as ferramentas de controle da Kaspersky Lab são integradas com o Active Directory, portanto, configurar políticas de bloqueio é simples e rápido. Todos os controles de edpoints são gerenciados a partir do mesmo console, através de uma única interface.

Como comprar

As ferramentas de controle de endpoints da Kaspersky Lab não são vendidas separadamente. Elas são ativadas nos níveis "Select", "Advanced" e "Total" do Kaspersky Endpoint Security for Business.

KASPERSKY lab