

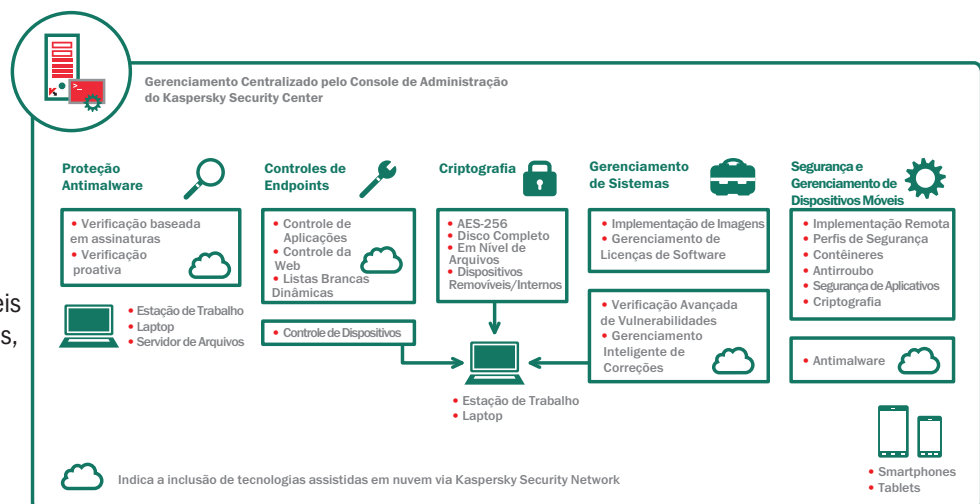
# ▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS Advanced

Este valioso conjunto de soluções da Kaspersky Lab está repleto de ferramentas de segurança combinadas com recursos de otimização de TI.

O nível Advanced da Kaspersky oferece a solução de proteção e gerenciamento de que sua organização precisa para impor políticas de TI, manter os usuários livres de malware, evitar a perda de dados e aprimorar a eficiência de TI.

## As Funcionalidades de Proteção e Gerenciamento de Que Você Precisa.

A Kaspersky criou avançados recursos corporativos nos níveis progressivos de nossas ofertas, mas tornamos a tecnologia descomplicada e simples para empresas de todos os tamanhos.



## Qual o Nível Certo para Você?

- CORE
- SELECT
- ADVANCED
- TOTAL

### RECURSOS INCLUÍDOS:

- ANTIMALWARE
- FIREWALL
- PROTEÇÃO ASSISTIDA EM NUVEM VIA KASPERSKY SECURITY NETWORK
- CONTROLE DE APLICATIVOS
- LISTAS BRANCAS DE APLICATIVOS
- CONTROLE DA WEB
- CONTROLE DE DISPOSITIVOS
- PROTEÇÃO DE SERVIDORES DE ARQUIVOS
- GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM)
- SEGURANÇA DE ENDPOINTS MÓVEIS (PARA TABLETS E SMARTPHONES)
- CRIPTOGRAFIA
- CONFIGURAÇÃO E IMPLEMENTAÇÃO DE SISTEMAS
- CONTROLE DE ADMISSÃO NA REDE
- VERIFICAÇÃO AVANÇADA DE VULNERABILIDADES
- GERENCIAMENTO DE CORREÇÕES

## ▶ A ÚNICA VERDADEIRA PLATAFORMA DE SEGURANÇA NO MERCADO

### Um Único Console de Gerenciamento

Em uma 'única exibição', o administrador pode ver e gerenciar todo o cenário da segurança: máquinas virtuais, computadores físicos e dispositivos móveis.

### Uma Única Plataforma de Segurança

A Kaspersky Lab desenvolveu nosso console, nossos módulos de segurança e nossas ferramentas internamente, em vez de adquiri-los de outras empresas. Isso significa que os mesmos programadores que trabalham na mesma base de código desenvolveram tecnologias que conversam e trabalham juntas. Isso resulta em estabilidade, políticas integradas, relatórios úteis e ferramentas intuitivas.

### Um Único Custo

Todas as ferramentas são de um único fornecedor, entregues em uma única instalação. Você não precisa de um novo processo de orçamento e uma nova justificativa para alinhar seus riscos de segurança com suas metas empresariais.

## CRIPTOGRAFIA E PROTEÇÃO DE DADOS:

### CRIPTOGRAFIA ABRANGENTE

Opções de disco completo ou em nível de arquivos, com o suporte do padrão AES (Advanced Encryption Standard) com criptografia de 256 bits para proteger informações corporativas críticas no caso de perda ou roubo do dispositivo.

### SUORTE PARA DISPOSITIVOS REMOVÍVEIS

Melhora sua segurança por meio de políticas que impõem a criptografia de dados em dispositivos removíveis.

### COMPARTILHAMENTO SEGURO DE DADOS

Significa que os usuários podem facilmente criar pacotes criptografados e com extração automática para garantir que os dados estejam protegidos ao serem compartilhados por meio de dispositivos removíveis, de e-mail, da rede ou da Web.

### TRANSPARÊNCIA PARA OS USUÁRIOS FINAIS

A solução de criptografia da Kaspersky é integrada e invisível para os usuários. Além disso, não afeta a produtividade. Também não há qualquer impacto sobre as configurações ou atualizações de aplicativo.

## CONTROLES DE ENDPOINTS:

### CONTROLE DE APLICATIVOS

Permite que os administradores de TI definam políticas para permitir, bloquear ou restringir aplicativos (ou categorias de aplicativos).

### CONTROLE DE DISPOSITIVOS

Permite que os usuários definam, programem e imponham políticas de dados para armazenamentos removíveis e outros controles de dispositivos periféricos, conectados a USB ou qualquer outro tipo de barramento.

### CONTROLE DA WEB

Significa que os controles de navegação baseados no endpoint seguem o usuário, quer ele esteja na rede corporativa ou em trânsito.

### LISTAS BRANCAS DINÂMICAS

As reputações de arquivos fornecidas em tempo real pela Kaspersky Security Network garantem que os aplicativos aprovados estão isentos de malware, ajudando a maximizar a produtividade do usuário.

## RECURSOS DE PROTEÇÃO DE ENDPOINTS:

### AVANÇADO ANTIMALWARE DE ENDPOINTS

Métodos tradicionais baseados em assinaturas, proativos e baseados em nuvem comprovados para detectar ameaças de malware.

### PROTEÇÃO ASSISTIDA EM NUVEM

A Kaspersky Security Network (KSN) responde a ameaças suspeitas muito mais rápido que os métodos tradicionais de proteção. O tempo de resposta da KSN a uma ameaça de malware pode ser de apenas 0,02 segundos!

**NEM TODOS OS RECURSOS ESTÃO DISPONÍVEIS EM TODAS AS PLATAFORMAS.**

Para obter detalhes, visite [www.kaspersky.com](http://www.kaspersky.com)

## CONFIGURAÇÃO E GERENCIAMENTO DE CORREÇÕES DO SISTEMA:

### GERENCIAMENTO DE CORREÇÕES

Avançada verificação aprofundada de vulnerabilidades, combinada com a distribuição automatizada de correções.

### IMPLEMENTAÇÃO REMOTA DE SOFTWARE

Implementação centralizada de software em computadores cliente, até mesmo em outros escritórios.

### CONTROLE DE ADMISSÃO NA REDE (NAC)

Com o Controle de Admissão na Rede (NAC), você pode criar uma política para 'convidados' na rede. Os dispositivos convidados (inclusive dispositivos móveis) são automaticamente reconhecidos e direcionados para um portal corporativo onde a senha de identificação correta permite que usem os recursos aprovados por você.

### IMPLEMENTAÇÃO DE IMAGENS DO SISTEMA OPERACIONAL E DE APLICATIVOS

Criação, armazenamento e implementação fáceis de imagens do sistema, a partir de um local central. Perfeito para a migração para o Microsoft® Windows® 8.

### GERENCIAMENTO DE HARDWARE, SOFTWARE E LICENÇAS

Relatórios de inventário de hardware e software ajudam a manter o controle dos compromissos de licenças de software. Assim, você pode economizar com o provisionamento central de direitos de software.

## RECURSOS DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS:

### TECNOLOGIAS ANTIMALWARE INOVADORAS

A combinação de detecção baseada em assinaturas, proativa e assistida em nuvem resulta em proteção em tempo real. O navegador seguro e o antispam aumentam a segurança.

### IMPLEMENTAÇÃO COM PROVISIONAMENTO POR CONEXÃO SEM FIO

Pré-configurar e implementar aplicativos centralmente por SMS, e-mail e do PC.

### FERRAMENTAS ANTIRROUBO REMOTAS

Verificação do Chip, Bloqueio, Limpeza e Localização Remotos evitam o acesso não autorizado a dados corporativos, caso um dispositivo móvel seja roubado ou perdido.

### CONTROLE DE APLICATIVOS PARA DISPOSITIVOS MÓVEIS

Monitora os aplicativos instalados em um dispositivo móvel, de acordo com políticas de grupo predefinidas. Inclui um grupo de "Aplicativos Obrigatórios".

### SUORTE PARA DISPOSITIVOS DE FUNCIONÁRIOS

Iniciativas do tipo "traga seu próprio dispositivo"? Os aplicativos e dados corporativos são isolados em contêineres criptografados transparentes para o usuário. Esses dados podem ser apagados separadamente.