

KASPERSKY TOTAL SECURITY FOR BUSINESS

Criptografia, ferramentas abrangentes de imposição de políticas e eficiência de TI, além de proteção de ponta a ponta contra malware.

O Kaspersky Total Security for Business fornece a mais completa plataforma de proteção e gerenciamento oferecida atualmente no mercado. O Total Security for Business protege todas as camadas de sua rede, incluindo ferramentas de configuração avançadas para garantir a produtividade de seus usuários e que eles estejam livres de ameaças de malware, independentemente do dispositivo ou do local.

As Funcionalidades de Proteção e Gerenciamento de Que Você Precisa.

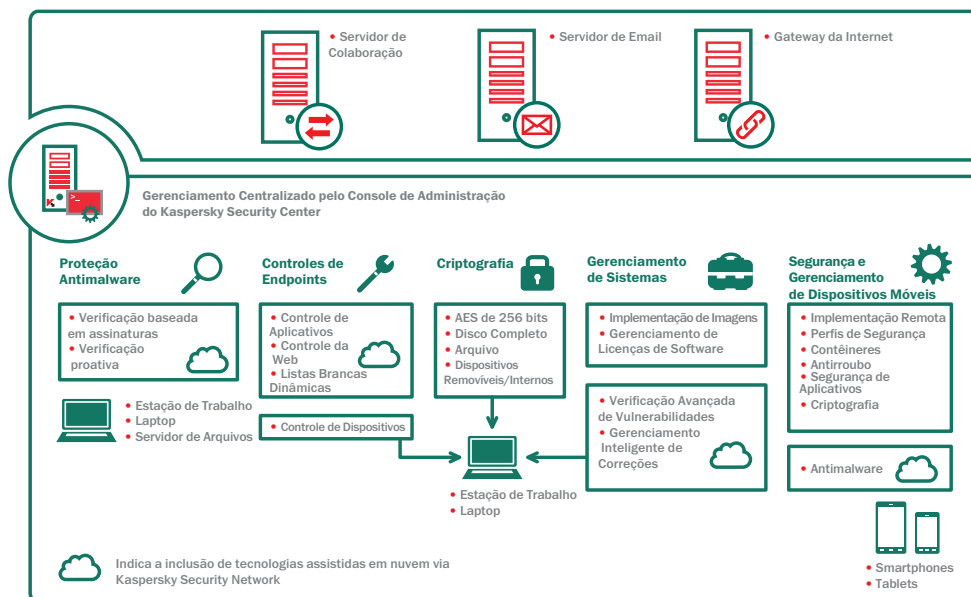
A Kaspersky criou avançados recursos corporativos nos níveis progressivos de nossas ofertas, mas tornamos a tecnologia descomplicada e simples para empresas de todos os tamanhos.

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
- VERIFICAÇÃO AVANÇADA DE VULNERABILIDADES
- CONTROLE DE ADMISSÃO NA REDE
- GERENCIAMENTO DE CORREÇÕES
- SEGURANÇA DE SERVIDORES DE E-MAIL
- PROTEÇÃO DE GATEWAYS DA WEB/INTERNET
- SEGURANÇA DE SERVIDORES DE COLABORAÇÃO



▶ 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.

RECURSOS DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS:

TECNOLOGIAS ANTIMALWARE INOVADORAS

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

SUPORTE 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.

IMPLEMENTAÇÃO COM PROVISIONAMENTO POR CONEXÃO SEM FIO

Pré-configurar e implementar aplicativos de forma centralizada por SMS, e-mail e do PC.

FERRAMENTAS ANTIRROUBO REMOTAS

Verificação do Chip, Bloqueio, Limpeza e Localização Remotas 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”.

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 de proteção tradicionais. O tempo de resposta da KSN a uma ameaça de malware pode ser de apenas 0,02 segundos!

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 DE 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.

NEM TODOS OS RECURSOS ESTÃO DISPONÍVEIS EM TODAS AS PLATAFORMAS.

Para obter detalhes, visite www.kaspersky.com

SEGURANÇA DE EMAIL, DE COLABORAÇÃO E DA WEB:

PROTEÇÃO DE SERVIDORES DE E-MAIL

Protege emails nas versões mais recentes das principais plataformas de e-mail e colaboração: servidores de e-mail baseados em Microsoft® Exchange, IBM®, Lotus® Domino® e Linux®.

SEGURANÇA PARA GATEWAYS DE INTERNET

Garanta um acesso seguro à Internet em toda a organização, removendo automaticamente programas maliciosos e possivelmente hosts do tráfego HTTP(S) / FTP / SMTP e POP3.

ELIMINAÇÃO VIRTUAL DE SPAM

Usando a tecnologia baseada em nuvem da Kaspersky, as atualizações são transferidas por push imediatamente, reduzindo a possibilidade dos spams se tornarem epidemias. Os e-mails suspeitos são retidos e verificados novamente, o que aumenta a taxa de detecção, além de reduzir falsos positivos.

SEGURANÇA DE COLABORAÇÃO

O Kaspersky defende seus servidores SharePoint® de malware, enquanto as funcionalidades de filtragem de conteúdo e arquivos ajudam a impedir o armazenamento de conteúdo impróprio.

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.

CRIOGRAFIA E PROTEÇÃO DE DADOS:

CRIOGRAFIA 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.

SUPORTE 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 email, 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.