KASPERSKY lab

Proteção Next Generation de endpoints

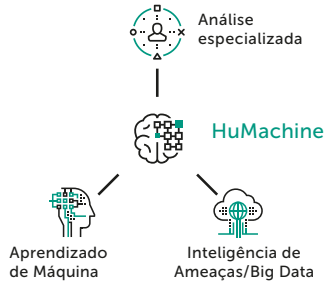
www.kaspersky.com/business
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

Proteção como parte da sua estratégia de continuidade de negócios

A tecnologia é uma força transformadora para empresas – acompanhe o ritmo ou fique para trás. Porém, a tecnologia também abre portas para criminosos, e os endpoints são os principais alvos e a fonte da maioria dos problemas. Apenas no último ano, mais de 38% das empresas sofreram algum ciberataque, e 39% dos ataques destinados a endpoints protegidos foram bem-sucedidos. Nesse contexto, as companhias precisam ser mais espertas que os cibercriminosos que as atacam.

Desde que existam pessoas por trás dos ciberataques, haverá uma necessidade por inteligência humana junto às tecno logias inovadoras para contê-los. A proteção da Kaspersky Lab se baseia em nossa inteligência de ameaças global combinada com algoritmos de aprendizado de máquina, movida à expertise humana dos maiores especialistas da indústria. Nomeamos essa combinação única de HuMachineTM, e ela está no DNA de todos os nossos produtos.



Em 2017, a Kaspersky Lab ganhou um dos principais prêmios da Gartner Peer Insights para plataformas de proteção de endpoints: o prêmio Platinum, por índices de satisfação do cliente. O prêmio é a mais alta distinção possível no competitivo mercado de plataformas de proteção de terminais. Nossos programas para endpoints alcançaram a porcentagem mais alta (90%) de presença entre os três primeiros lugares em testes independentes quando comparados a qualquer outro fornecedor.

Invista no futuro

El impacto financiero promedio de una perpetración para pequeñas y medianas empresas es de $ 86.5k y para las compañías grandes, de $ 992k. El antivirus de última generación ya no es suficiente: sólo una solución multidimensional que brinda seguridad en múltiples capas tecnológicas y capas funcionales de la infraestructura de TI corporativa puede brindar la protección que necesita. La verdadera seguridad de nodos combina una variedad de técnicas y tecnologías inteligentes para proteger a las empresas contra cualquier tipo de amenaza cibernética, en cualquier plataforma. Si puede proteger toda su red de TI, asegurará la continuidad de su negocio.

Proteja o que você mais valoriza com programas baseados em HuMachine™

Conforme o seu negócio amadurece, seu orçamento de segurança em TI talvez não cresça na mesma proporção. Os recursos devem ser otimizados para atender os desafios de hoje – e de amanhã. O Kaspersky Endpoint Security for Business, por meio da inteligência HuMachine™, protege contra ransomware, exploits e as mais avançadas ciberameaças. Com otimização de recursos, é equipado com controles de segurança poderosos, gerenciamento de vulnerabilidades e de correções automatizado, criptografia integrada e pode controlar toda a rede corporativa a partir de um único console.

Segurança ágil e adaptável

O produto foi desenvolvido para funcionar em qualquer ambiente de TI. Emprega as melhores e comprovadas tecnologias Next Generation. Sensores internos e integração com o sistema de detecção e resposta de endpoints (EDR) os quais permitem a captura e análise de grandes volumes de dados para garantir a descoberta dos mais obscuros e sofisticados ciberataques.

Segurança orientada para o futuro de TI terceirizada

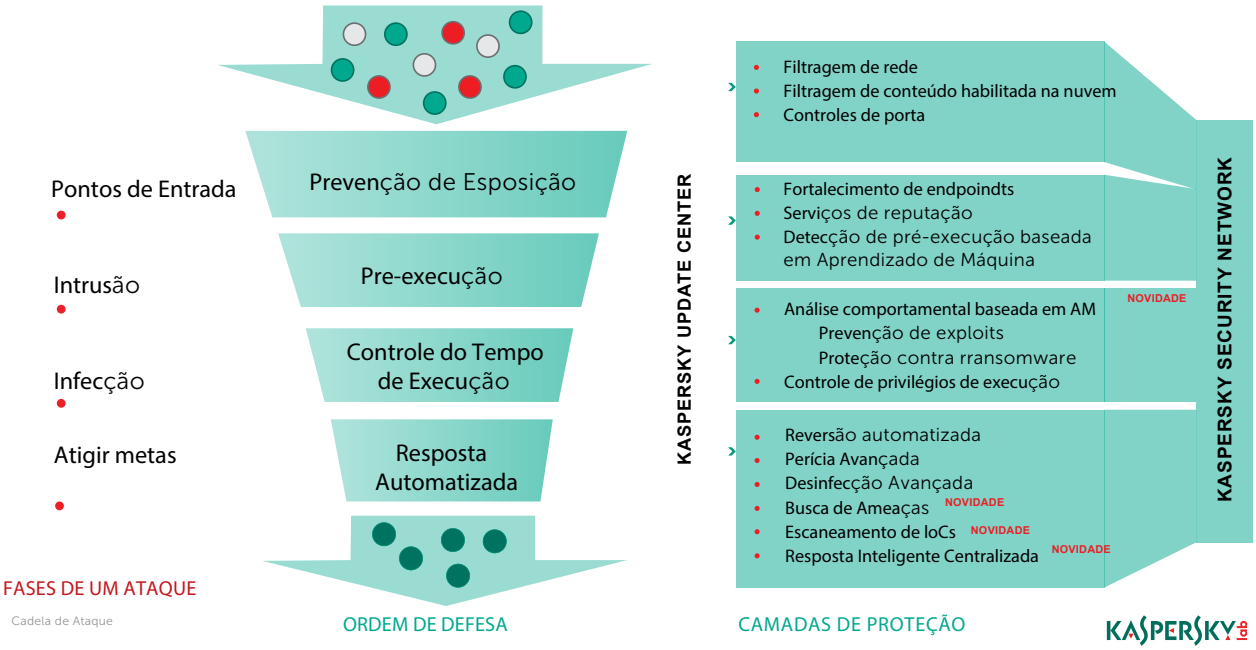
Modelo multitenancy (multi-inquilino) interno, com prevenção de ameaças, segurança móvel, criptografia de dados, gerenciamento de vulnerabilidades e correções, capacitam os provedores de serviços gerenciados (MSPs) a adicionar segurança de TI a suas ofertas.

Baixo consumo de memória: alta performance

A nossa mais testada e premiada segurança baseada em HuMachine entrega proteção otimizada com impacto mínimo nos recursos computacionais. Componentes sem assinatura garantem que ameaças sejam detectadas mesmo sem atualizações frequentes..

Proteção abrangente

O **Kaspersky Endpoint Security for Business** utiliza várias tecnologias Next Generation (como fortalecimento de terminais, análise comportamental baseada em aprendizado de máquina, prevenção de exploits, etc.) para neutralizer a maioria das ameaças antes que alcancem as camadas avançadas de proteção. Arquivos suspeitos que chegam até o endpoint são detectados e bloqueados.



Essa combinação de tecnologias avançadas com a nossa abordagem multicamadas alcança o equilíbrio perfeito entre performance e proteção eficiente. Desempenha um papel crítico em nossos produtos e alcança uma das mais altas taxas de detecção da indústria, como demonstrado continuamente por meio de testes independentes.

Múltiplas camadas de proteção para

- Windows, Linux ou Mac
- Android e outros dispositivos móveis
- Armazenamento removível
- Servidores Windows e Linux
- Servidores de e-mail
- Gateways web
- Servidores de colaboração

Defesa incomparável contra

- Exploits
- Ransomware
- Malware móvel
- Ameaças desconhecidas
- Ameaças sem arquivo
- PowerShell e outros ataques baseados em script
- Ameaças da web
- Ameaças distribuídas por e-mail
- Ataques de phishing
- Spam

Proteção Anti-Ransomware e Anti-Exploit

Baseada em fontes incomparáveis de inteligência de ameaças e aprendizado de máquina em tempo real, nossas tecnologias evoluem continuamente. Proteja seus endpoints dos últimos exploits e mantenha seus dados e pastas compartilhadas seguras e protegidas de ameaças avançadas e ransomware.

Bloqueio de roubo de contas

Detecção comportamental implementa um mecanismo de proteção de memória, que protege processos críticos para o sistema e evita o vazamento de credenciais de usuários e administradores.

Diminuição de exposição a ataques por meio de programas

Movido por listas brancas dinâmicas, o Controle de Programas reduz significativamente sua exposição a ataques de dia zero e fornece controle completo sobre quais softwares podem ser executados em desktops e servidores. O Controle de Programas intercepta o lançamento de arquivos executáveis, DLLS e controla scripts executados por uma variedade de intérpretes. A Detecção de Comportamento e Prevenção de Exploits monitora o comportamento do programa, bloqueia atividades potencialmente maliciosas e protege programas legítimos de exploração e utilização por malware. Seus programas aprovados e confiáveis continuam a rodar sem problemas.

Neutralização de rootkits

Criminosos usam rootkits e bootkits para esconder suas atividades das soluções de segurança. A tecnologia anti-rootkit, parte da proteção multicamadas Next Generation da Kaspersky Lab, favorece a detecção até mesmo de infecções mais silenciosas e as neutraliza.

Reconhecimento de ataques e intrusões – até os mais obscuros

Sensores internos e integração com o Kaspersky Endpoint Detection and Response permitem a captura e análise de grandes volumes de dados no local sem impacto na produtividade do usuário. Fornece avançada busca de ameaças por evidências de intrusão – como indicadores de comprometimento (IoC).

Evita exposição na rede

Malwares que utilizam um ataque de transbordamento de dados (buffer-overrun) podem modificar um processo que já está sendo executado na memória e dessa forma executar um código malicioso. A proteção contra ameaças na rede identifica ataques e exploits na rede e os interrompe no meio do caminho.

Mantenimiento y soporte

Operando en más de 200 países en 35 oficinas de todo el mundo, nuestro compromiso con el soporte global de 24 horas, los 7 días de la semana, se refleja en nuestros paquetes de soporte del Acuerdo de Servicio de Mantenimiento (MSA). Nuestros equipos Profesionales de Servicio están listos para garantizar que usted obtenga el máximo beneficio de su solución de Kaspersky Lab, brindándole asistencia con la implementación y soporte durante incidentes críticos.

Prueba gratuita

Descubra por qué solo True Cybersecurity combina la facilidad de uso, la agilidad y la inteligencia de **HuMachine ™** para proteger su negocio de todo tipo de amenazas. Visite la página y obtenga una versión de prueba gratuita de la versión completa de **Kaspersky Endpoint Security for Business** de 30 días. Al final de la prueba, si decide comprar, solo pagará las tarifas de la licencia. Como la aplicación ya se habrá ejecutado en sus nodos durante la prueba, no tendrá que hacer nada más.

Além da proteção de endpoints – agora e no futuro

Simplifica inventários e correções

Descobrir os detalhes para inventários de hardware e software e gerenciar a correção oportuna de vulnerabilidades é entediante e consome tempo. Explorar vulnerabilidades que não foram corrigidas é uma das maneiras mais comuns usadas pelos cibercriminosos para atacar a infraestrutura de TI a partir de um único endpoint. Além da implementação remota de novos softwares de terceiros, a avaliação de vulnerabilidades e gerenciamento de correções automatizada, baseada em inteligência ininterrupta em vulnerabilidades exploradas, mantém softwares potencialmente vulneráveis atualizados economiza tempo dos administradores de TI, o qual pode ser utilizado para outras tarefas.

Protege o compartilhamento de dados com criptografia

A criptografia transparente para usuário com certificação FIPS 140-2 protege completamente dados confidenciais em dispositivos portáteis e locais. A tecnologia integrada significa que você pode reforçar centralmente a criptografia de dados corporativos a nível de arquivo, disco ou dispositivo e permitir o compartilhamento seguro de dados por toda a sua rede.

Suporta cenários remotos e móveis

Os dados ficaram disponíveis a qualquer hora, em livre circulação pelo perímetro. A segurança móvel protege contra ameaças direcionadas especificamente a dados em movimento, assim como contra as tentativas de utilizar fraquezas nos dispositivos como trampolins para infiltração subsequente na infraestrutura. O Controle de Dispositivos protege contra as consequências da perda de dados em dispositivos portáteis sem aprovação ou sem criptografia e o carregamento de dados infectados do dispositivo.

Otimiza a eficácia com gerenciamento para todas as plataformas

Um único console fornece visibilidade completa e controle sobre cada estação de trabalho, servidor e dispositivo móvel, independentemente de onde estiver e do que estiver fazendo. Quase infinitamente escalável, a solução fornece acesso ao licensiamento, resolução remota de problemas e controles de rede. O gerenciamento centralizado é complementado pela integração com diretórios ativos, modelo baseado em funções e painéis de controle integrados.

Regula o acesso a dados sensíveis e dispositivos de gravação

Nossa solução restringe os privilégios de programa de acordo com níveis de confiança atribuídos, limita o acesso a recursos como dados criptografados. Trabalha em sintonia com uma base de dados de reputação local e na nuvem (KSN), o sistema de prevenção de intrusão (HIPS) controla programas e restringe o acesso aos recursos críticos do sistema e dispositivos de gravação áudio e vídeo.

Interrompe ameaças da web antes que alcancem seus endpoints

Ao interromper a maioria das ameaças recebidas a nível de gateway, reduzimos significativamente o impacto do fator humano e das especificidades de segurança das estações de trabalho impede-se que alcancem os terminais.

Um gateway seguro continua como a primeira linha de defesa para a maioria dos cenários de segurança corporativa, apesar da penetração da mobilidade nos processos de trabalho. Nossas tecnologias de segurança filtram o fluxo de tráfego ao longo dos gateways, bloqueia automaticamente as ameaças recebidas antes que alcancem seus endpoints e servidores. Isso reduz significativamente o risco da exploração de vulnerabilidades e diminui consideravelmente as despesas operacionais para a equipe de segurança de TI.

Aumenta a produtividade e reduz as ameaças

O anti-spam Next Generation e assistido pela nuvem da Kaspersky Lab detecta até os mais sofisticados e desconhecidos spams com perda mínima de comunicação devido a falsos positivos. Reduzir o tempo perdido, os recursos e os riscos associados ao spam por meio da interrupção do seu caminho economiza recursos humanos e de sistema. A proteção incorpora múltiplas camadas de segurança proativa, o que inclui aprendizado de máquina e inteligência de ameaças assistida pela nuvem, a fim de filtrar anexos maliciosos, malwares conhecidos e previamente desconhecidos em mensagens recebidas.

Permite colaboração segura

Nossa segurança para o Microsoft SharePoint® inclui anti-malware, filtragem de conteúdo e de arquivos, para ajudar a sua empresa a aplicar as políticas de colaboração e evitar que conteúdos inapropriados sejam armazenados na sua rede corporativa.

O Kaspersky Endpoint Security for Business permite que os administradores vejam, monitorem, controlem e protejam seu ambiente de TI. As ferramentas e tecnologias Next Generation são inteligentemente equilibradas ao longo dos níveis progressivos a fim de atender suas novas necessidades de TI e de segurança a cada ponto da sua jornada de negócios.

Kaspersky® Total Security for Business

Empresas que possuem ambientes de TI maduros – com um mix de sistemas de legado e recentes – precisam afinar a sua segurança para diferentes sistemas. Nossa solução de segurança mais abrangente para endpoints, infraestrutura e servidores de colaboração permitem que você faça exatamente isso – com objetivo de obter segurança rigorosa que pode adequar à sua TI.

Kaspersky® Endpoint Security for Business Advanced

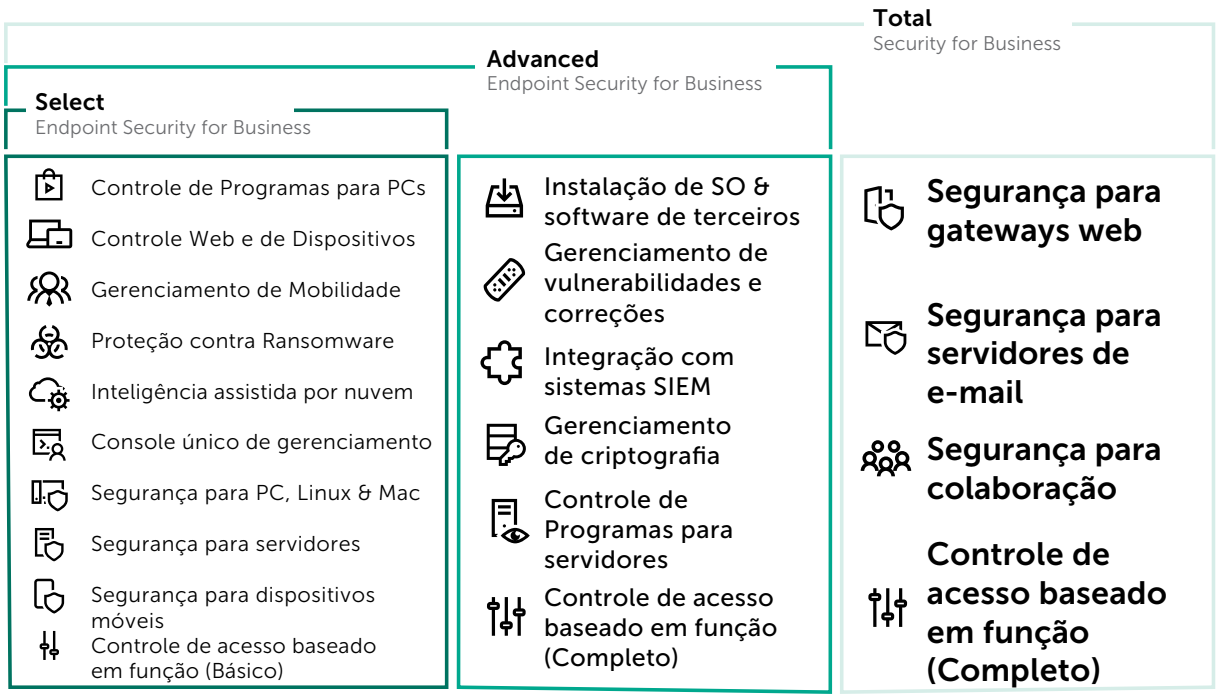
Para uma segurança que vai além para proteger sua empresa, escolha o **Kaspersky Endpoint Security for Business Advanced.** Além de proteger todos os seus endpoints e servidores, fornece camadas extras de segurança para proteção de dados sensíveis e eliminação de vulnerabilidades – além de auxiliar na simplificação do gerenciamento de sistemas.

Kaspersky® Endpoint Security for Business Select

Com mais operações de negócios em migração para plataformas digitais, você precisa proteger cada servidor, laptop e dispositivo móvel. Fornecemos segurança Next Generation que ajuda você a proteger cada endpoint gerido pela sua empresa, em uma única solução com um console de gerenciamento flexível.

Qual o nível certo para você?

Independentemente das especificidades da sua estrutura de TI em evolução precisa, o **Kaspersky Endpoint Security for Business** tem a solução ideal para você.



A segurança que você precisa

Automatizar e centralizar a descoberta de vulnerabilidades de softwares e gerenciamento de correções auxilia na proteção contra as mais perigosas ameaças, tais como o ransomware. Para clientes do Kaspersky Endpoint Security for Business Select, essa automação está disponível com o Kaspersky Vulnerability and Patch Management Add-on.

Para os clientes Select, o Kaspersky Encryption Add-on permite criptografia de arquivos e de disco completo, por meio de algoritmos fortes de encriptação, além de apresentar suporte de acesso único para abertura imediata de arquivos encriptados, o que se estende para cartões inteligentes/tokens voltados para autenticação de dois fatores. Permite a encriptação de arquivos e pastas armazenados em drives locais e removíveis.

Para ainda mais segurança sem qualquer complexidade adicional, basta ativar o conjunto de recursos necessários a partir do Kaspersky Security Center.

Por que aprimorar a sua proteção de endpoints atual?

Tenha sempre as últimas tecnologias – de maneira fácil e rápida: servidor, console e agente únicos

Suporte a qualquer processo de negócio por meio da mais profunda integração mais– base de código único, construído internamente

Evitar custos ocultos e licenças separadas – toda a funcionalidade que você precisa em uma única compra.

Capacidades de auditoria e controle aprimoradas; gerenciamento unificado com acesso baseado em função

Na Kaspersky Lab, desenvolvemos e aperfeiçoamos todas as nossas tecnologias internamente, o que torna nossos programas mais estáveis e eficientes. Estamos comprometidos com nossa própria P&D e a incorporar muitas inovações tecnológicas em nossos produtos. Apenas alguns exemplos:

- Aprendizado de Máquina multicamadas: métodos de aprendizado de máquina em diferentes estágios da cadeia de execução em endpoints e na nuvem.
- Busca de ameaças ativa como resultado da integração entre a proteção de endpoints e as soluções Endpoint Detection & Respose ou Anti Targeted Attack.
- Modo de nuvem único para proteção de componentes capaz de entregar proteção otimizada com impacto mínimo em recursos computacionais e no uso da internet.
- Suporte para recipientes do Microsoft Windows Server, segurança de tráfego externo e gerenciamento de firewall.
- Controle de Dispositivos e funcionalidade Anti-Bridging aprimorados.
- Controle de Programas aprimorado com categoria de certificados confiáveis e modo de teste para políticas.
- A nova e limpa interface de usuário que permite visualização da proteção multicamadas, exibe o status da proteção e a eficácia das últimas tecnologias da Kaspersky Lab em ação.

True Cybersecurity: está em nosso DNA

A Kaspersky Lab entrega soluções de cibersegurança poderosas por meio da utilização da inteligência de ameaças líder mundialmente, parte do nosso DNA e que influencia tudo o que fazemos. Como empresa independente, somos mais ágeis, pensamos diferente e agimos mais rápido.

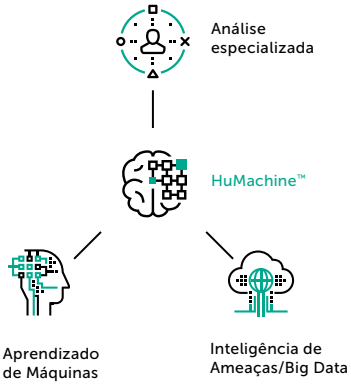
- **Nossa expertise é do topo para a base –** começando pelo nosso CEO, Eugene Kaspersky.
- **Nossa Equipe de Pesquisa e Análise Global (GReAT) –** grupo de elite de especialistas em segurança que descobriu muitos dos malwares, ameaças e ataques direcionados mais perigosos do mundo.
- Nossa inovadora **Iniciativa de Transparência Global** é mais uma evidência do nosso comprometimento em proteger clientes de ciberameaças, independentemente de suas origens ou propósito.

Fique em conformidade com o Regulamento Geral de Proteção de Dados (General Data Protection Regulation – GDPR) com a True Cybersecurity

A Kaspersky Lab promove a conscientização sobre os aspectos relacionados com segurança do GDPR. Nossas soluções ajudam os clientes a reduzir os riscos de violações de dados e evitar incidentes de segurança. Também auxiliamos o responsável pela proteção de dados (Data Protection Officer – DPO) de nossos clientes com uma melhor visibilidade da infraestrutura monitorada.

Panorama Geral – Soluções de Segurança de TI para empresas da Kaspersky

A proteção de endpoints, apesar de essencial, é apenas o início. Mesmo que você opere uma estratégia de segurança da melhor qualidade ou de um fornecedor único, a Kaspersky Lab oferece uma variedade de produtos que se conecta ou trabalha independentemente, para que você possa escolher sem sacrificar sua eficácia de performance ou liberdade de escolha. Saiba mais em nosso site.



Kaspersky Lab
Encontre um parceiro perto de você: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
Ciberseguridad verdadera: **www.kaspersky.com/true-cybersecurity**
idades sobre Segurança de TI: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com.br

KESB_Product_Datasheet_Next_Generation_Endpoint_Protection_Customer_0218_EN_GLB