KASPERSKY lab

SEGURANÇA DA KASPERSKY PARA PORTFÓLIO EMPRESARIAL 2015

"O PODER DE PROTEÇÃO DE SUA ORGANIZAÇÃO"

Qualquer empresa, independentemente do tamanho, está em risco de ameaças de malware. A Kaspersky Lab está em uma posição única para ver e descobrir muitas destas ameaças.

E o nível de ameaça está aumentando. Novos malware visando indivíduos e empresas como a sua já ultrapassam 325.000 ameaças únicas a cada dia.

Na Kaspersky Lab, estamos preocupados com essas ameaças e os riscos que representam para a sua empresa - é por isso que estamos aconselhando organizações como a sua a garantir que a estratégia de segurança de TI atenda a três critérios fundamentais:

- **Em primeiro lugar,** você precisa ter acesso à inteligência de ameaças superior. Esta é uma profunda compreensão de como é uma ameaça - como está escrita e compilada. É importante que o seu sistema de segurança seja continuamente alimentado por informações especializadas e que seu fornecedor vasculhe zonas quentes de malware em todo o mundo para verificar o que está por vir.

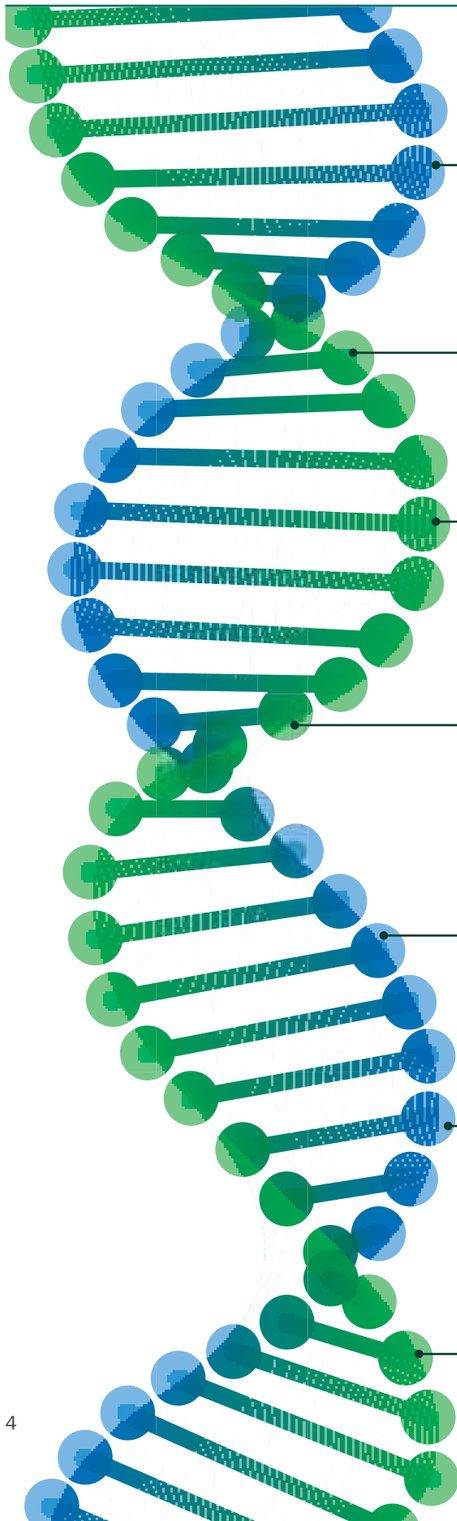
- **Em segundo lugar,** sua segurança deve incluir ferramentas e técnicas capazes de detectar e eliminar malware conhecido, desconhecido e avançado. Ao mesmo tempo, o seu software de segurança deve minimizar a carga em seus sistemas e manter tempos de verificação rápida, para que seu negócio não seja interrompido.

- **Em terceiro lugar,** como ambientes de TI corporativos têm se tornado cada vez mais complexos, essa tecnologia precisa estender seu alcance em todos endpoints físicos, móveis e virtuais, com perfeição e eficiência, através de uma única plataforma, sem conflitos de software, vários consoles ou falhas na segurança.

Apenas a Kaspersky pode oferecer a inteligência de ameaça líder mundial que sua empresa precisa, e a tecnologia que a faz funcionar, construída em uma plataforma de segurança única e abrangente.

As soluções Kaspersky são projetadas com a flexibilidade para se alinhar com os objetivos de sua empresa. Isso significa que estamos sempre de prontidão para proteger sua organização contra ameaças aos seus endpoints físicos e virtuais, seus dispositivos móveis. seus sistemas de e-mail, servidores, gateways e portais SharePoint. Entre em contato com o seu revendedor de TI hoje para saber mais sobre os produtos, soluções e serviços constantes neste documento. Gostaríamos de lhe mostrar como podemos trabalhar em conjunto para proteger sua empresa de ameaças virtuais.

INTELIGÊNCIA DE SEGURANÇA ESTÁ EM NOSSO DNA



Especialidade do começo ao fim

Líder global em inteligência de ameaças, incluindo o GREAT team

Respeitados entre as melhores organizações de segurança

Movidos à tecnologia

Reconhecidos como líderes em testes independentes

Liderando a descoberta das ameaçasmais complicadas

Veja e preveja incidentes de segurança com a Kaspersky Security Network

SEGURANÇA COM UMA DIFERENÇA

A Kaspersky Lab oferece o mais poderoso antimalware do mercado, aproveitando o líder mundial em inteligência de segurança que está embutido no nosso DNA e influencia tudo o que fazemos – e como o fazemos.

- Somos uma empresa movida à tecnologia - do começo ao fim - começando pelo nosso CEO, Eugene Kaspersky.
- Nossa Equipe de Pesquisa & Análise Global (Our Global Research & Analysis Team - GReAT), um grupo de elite de especialistas em segurança de TI, foi a primeira a descobrir muitas das ameaças de malware e ataques direcionados mais perigosos do mundo.
- Muitas das organizações de segurança mais respeitadas do mundo e órgãos que aplicam as leis têm procurado ativamente a nossa assistência.
- Como a Kaspersky Lab desenvolve e aperfeiçoa todas as suas próprias principais tecnologias internamente, nossos produtos são naturalmente mais estáveis e eficientes.
- A cada ano, a Kaspersky Lab participa de testes mais independentes do que qualquer outro fornecedor - e nos destacamos em uma percentagem muito maior de testes do que qualquer outro fornecedor!
- Os analistas mais amplamente respeitados do setor – incluindo Gartner, Inc, Forrester Research e International Data Corporation (IDC) – classificam-nos como um líder em várias categorias principais de segurança de TI
- Mais de 130 OEMs – incluindo Microsoft®, Cisco® Meraki, Juniper Networks, Alcatel Lucent muitos outros – usam as nossas tecnologias em seus produtos e serviços.

Isso é o que faz a diferença!

SOBRE A NOSSA TECNOLOGIA ANTIMALWARE

O software de segurança de TI é tão eficaz quanto o mecanismo de segurança em seu núcleo. Gerenciamento de correções, MDM, criptografia, controles de dispositivos, antiphishing - todas essas tecnologias e muitas outras fornecem camadas de segurança adicionais e valiosas. As organizações não devem comprometer a segurança contra ameaças conhecidas, desconhecidas e avançadas.

O mecanismo de segurança da Kaspersky Lab é continuamente alimentado e aprimorado por nossa inigualável inteligência em ameaças dinâmicas. É o nosso foco único em segurança, combinado com a nossa inteligência em ameaças e experiência global, que nos destaca no mercado.

O desempenho do mecanismo antimalware líder do setor, construído na plataforma Kaspersky Endpoint Security for Business, é comprovado através de vários testes contínuos e independentes. Sua própria diligência confirmará que a segurança Kaspersky é incomparável.

Confira o que faz da proteção antimalware da Kaspersky Lab tão poderosa e tão mais eficaz do que o resto.

PRINCIPAIS RECURSOS DO PRODUTO

- **Detecção de ameaças conhecidas, desconhecidas e avançadas**
- **Análise & Heurística comportamental**
- **Kaspersky Security Network: Proteção assistida em nuvem**
- **Desinfecção ativa**
- **Defesa de criptografia e ransomware**
- **Automatic Exploit Prevention**
- **Firewall HIPS & Pessoal**
- **Bloqueio de ataques de rede**
- **Console de gerenciamento simples e transparente**

DESTAQUES

UMA ABORDAGEM MULTICAMADAS

A abordagem multicamadas da Kaspersky Lab é uma das razões de sermos capazes de fornecer a segurança mais eficaz no mercado hoje. Como as tecnologias da Kaspersky Lab são desenvolvidas internamente, a sobreposição de camadas da poderosa e aprimorada proteção é capaz de trabalhar perfeitamente em conjunto, com um impacto mínimo no desempenho.

Cada camada de proteção lida com ameaças virtuais de uma perspectiva diferente, permitindo que os profissionais de TI implementem tecnologias fortemente interligadas, proporcionando segurança que é ao mesmo tempo profunda e ampla.

LÍDER MUNDIAL EM INTELIGÊNCIA DE AMEAÇAS — SUA GARANTIA DE PROTEÇÃO CONTÍNUA

A inteligência global de ameaças da Kaspersky Lab é reconhecida mundialmente e essa especialidade é retroalimentada diretamente em nossas soluções de segurança, criadas para evoluir constantemente em um mundo de TI em constante transformação.

RECURSOS

SEGURANÇA HEURÍSTICA — QUE REDUZ A CARGA EM SEUS SISTEMAS

Identificação de malware com base em padrões fornece uma detecção melhorada — entrega arquivos menores de atualização, bem como uma maior segurança.

ANÁLISE DE COMPORTAMENTO

O antimalware Kaspersky inclui dois componentes específicos para análise de atividade do programa:

- **Emulador** — reproduz e verifica as atividades planejadas do programa.
- **Inspetor do sistema** — rastreia as atividades dos programas já em execução, discriminando e analisando padrões de comportamento característicos de malware.

DETECÇÃO DE MALWARE ASSISTIDA EM NUVEM — KASPERSKY SECURITY NETWORK (KSN)

Resposta em tempo real às ameaças de malware novas e desconhecidas. O fluxo constante de novos dados sobre tentativas de ataques de malware e comportamento suspeito, fornecidos por mais de 60 milhões de usuários voluntários do software Kaspersky Lab, é usado para ajudar a criar veredictos instantâneos de arquivos, o que permite a todos os clientes beneficiarem-se da proteção em tempo real com baixos "falsos positivos".

AUTOMATIC EXPLOIT PREVENTION

A Prevenção automática contra exploits é direcionada especificamente a malware que explora vulnerabilidades de software em aplicativos populares reconhecendo padrões de comportamento típicos ou suspeitos. Em seguida, a tecnologia interrompe o exploit em suas trilhas, e impede que qualquer código malicioso baixado seja executado.

CONTRAMEDIDAS DE CRIPTOGRAFIA RANSOMWARE

O inspetor do Sistema salva cópias de arquivos importantes em armazenamento temporário, no caso de um processo suspeito tentar acessá-los. Caso o ransomware tente criptografar os originais, estes arquivos podem ser restaurados ao seu estado não criptografado.

DESINFECÇÃO ATIVA

Utiliza diferentes técnicas para "cura" de todas as infecções detectadas — impedindo a execução de arquivos e processos, incluindo autostart, destruindo malware e "revertendo" arquivos armazenados à sua condição original.

HIPS E FIREWALL PESSOAL

Algumas atividades de programas são suficientemente de altíssimo risco para receber apenas restrição, mesmo que eles não sejam confirmados como maliciosos. O HIPS (Host-Based Intrusion Prevention System, sistema de prevenção contra invasões com base em host) da Kaspersky Lab restringe atividades dentro do sistema de acordo com o nível de confiança do aplicativo — com a ajuda de um firewall pessoal no nível do aplicativo, restringindo a atividade de rede.

BLOQUEIO DE ATAQUES DE REDE

Monitora a atividade suspeita em sua rede — e permite predefinir como seus sistemas responderão se qualquer comportamento suspeito for detectado.

ATUALIZAÇÕES FREQUENTES

Atualizações de proteção contra novas ameaças de malware são entregues ao seu banco de dados de segurança através do ciclo de atualização mais rápido do setor, em conjunto com a atualização contínua de dados sobre malwares recém-descobertos a partir da nuvem da Kaspersky Security Network (KSN).

LÍDER DO SETOR DE PROTEÇÃO — UM FATO COMPROVADO DE FORMA INDEPENDENTE

Durante 2014, os produtos da Kaspersky Lab participaram de **93 testes e análises independentes.** Nossos produtos ficaram **66 vezes entre os três primeiros**, o equivalente a **71%**, e **51 vezes em 1º lugar** — em bem mais da metade de todos os testes.

Nenhum produto ou solução de qualquer um dos nossos principais concorrentes chega próximo a isso.

PRODUTOS DE SEGURANÇA, SOLUÇÕES E SERVIÇOS PARA EMPRESAS

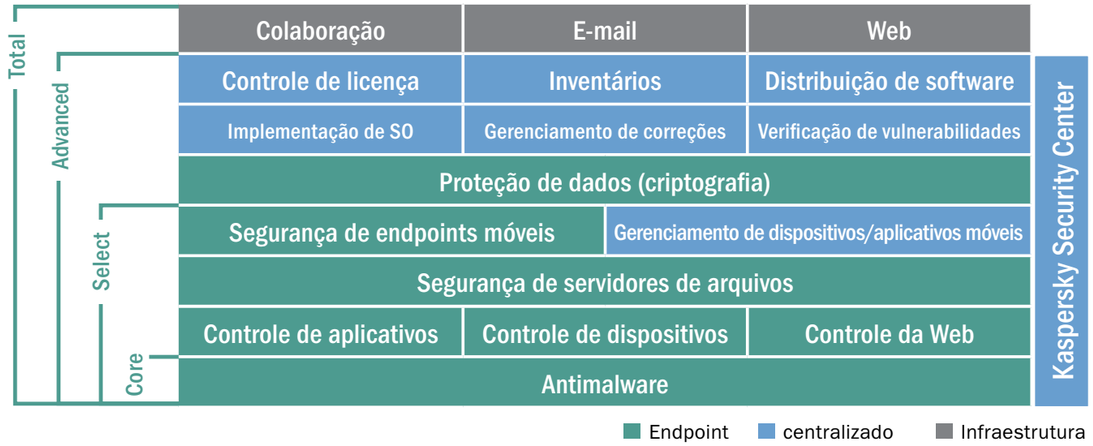
Kaspersky Endpoint Security for Business	Aproveitando a especialização do melhor ecossistema em inteligência de ameaças do mundo, o Kaspersky Endpoint Security for Business fornece uma abordagem de segurança em níveis com base em uma única plataforma integrada, incorporando recursos incluindo robustas ferramentas de aplicativos, dispositivos e controle da Web, criptografia de dados, segurança de endpoints móveis e MDM, e gerenciamento de sistemas e correções. Tudo é gerenciado a partir um console central — o Kaspersky Security Center. O Kaspersky Total Security for Business adiciona segurança de e-mail, Web e servidor de colaboração, salvaguardando seus perímetros e protegendo o ambiente de TI completo de sua empresa.
Kaspersky Targeted Solutions	Soluções autônomas que permitem a segurança Kaspersky Lab ser aplicada às áreas específicas do seu sistema de TI. Algumas soluções, como o Kaspersky Security for Mobile, também estão disponíveis como parte do Kaspersky Endpoint Security for Business. Outras, como o Kaspersky Security for Virtualization, estão disponíveis unicamente como soluções direcionadas. Todas foram desenvolvidas a partir das mesmas tecnologias e inteligência de ameaças de destaque, e todas as soluções de segurança de endpoints físicos, móveis e virtuais são gerenciadas de maneira centralizada através do Kaspersky Security Center.
Serviços de inteligência e Soluções empresariais do Kaspersky Security	Aproveita a inteligência em ameaças, a especialização técnica, os dados e habilidades de treinamento da Kaspersky para aumentar a segurança da sua marca, de sua organização e de seus funcionários As soluções empresariais lidam com problemas de segurança em setores e infraestruturas específicas e com formas específicas de ataques como o DDoS (Distributed Denial of Service - Negação de Serviço Distribuído).
KASPERSKY SMALL OFFICE SECURITY	Proteção de classe mundial facilitada para as empresas muito pequenas.
CONTRATOS DE MANUTENÇÃO E SERVIÇO	Uma gama de opções de suporte para a sua solução de segurança Kaspersky.

SOBRE O KASPERSKY ENDPOINT SECURITY FOR BUSINESS

O Kaspersky Endpoint Security for Business oferece uma solução de segurança completa, desenvolvida pelos maiores especialistas em segurança do mundo. A proteção mais aprofundada e avançada, desempenho eficiente e gerenciamento direto desenvolvidos através de níveis progressivos para proteger totalmente a sua empresa.

Todos os componentes foram desenvolvidos e construídos para se interligarem internamente em uma única plataforma de segurança direcionada às suas necessidades comerciais. O resultado é uma solução estável e integrada sem brechas, sem problemas de compatibilidade e sem carga de trabalho adicional durante a fase de desenvolvimento do seu sistema.

Os administradores podem ver, controlar e proteger seu ambiente de TI com o Kaspersky Endpoint Security for Business. As ferramentas e tecnologias são distribuídas de forma exclusiva em níveis progressivos para atender às evoluções constantes de suas necessidades de segurança e TI. A Kaspersky pode tornar seu trabalho mais fácil.

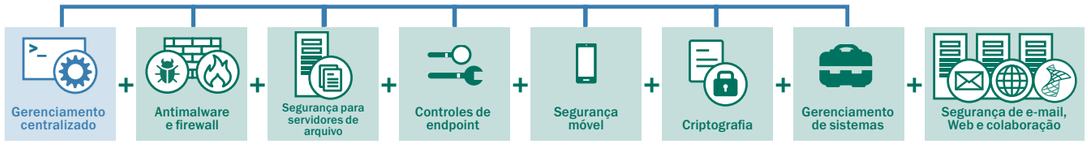


A Kaspersky apresenta uma lista completa de tecnologias - todas trabalhando em conjunto na mesma base de códigos e assistida pela Kaspersky Security Network com base na nuvem - para oferecer aos nossos clientes o nível de proteção de classe internacional de que necessitam.

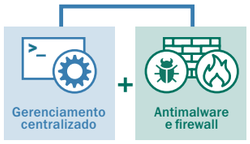
Resumindo, fornecemos a primeira plataforma de segurança do setor, desenvolvida do zero, facilitando ao administrador as tarefas de ver, controlar e proteger seu mundo.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Poderosa proteção em vários níveis contra ameaças conhecidas, desconhecidas e avançadas, criada e construída por especialistas líderes do setor em segurança. O Kaspersky Endpoint Security for Business, apoiado pela inteligência de ameaças de renome mundial, fornece segurança e controle de TI inigualável.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS — CORE



Proteção antimalware de última geração - a fundação da plataforma de segurança da Kaspersky Lab

As tecnologias de proteção em vários níveis da Kaspersky Lab são desenvolvidas internamente por pessoas apaixonadas por segurança. Testes independentes confirmam que o resultado é a solução de segurança mais poderosa e eficaz do setor - não há melhor proteção para a sua organização.

Proteção contra ameaças conhecidas, desconhecidas e avançadas — tecnologias sofisticadas e únicas identificam e eliminam as ameaças existentes e emergentes.

Prevenção automática contra exploits — direciona e identifica proativamente ameaças desconhecidas e avançadas.

Proteção assistida em nuvem — usa informações em tempo real da Kaspersky Security Network global.

Inspetor do sistema — No caso do sistema ser afetado, fornece uma função única de restauração de arquivo.

HIPS com firewall pessoal — o HIPS restringe atividades de acordo com o nível de confiança do aplicativo - apoiado por um firewall pessoal no nível do aplicativo, restringindo a atividade de rede.

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 às 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.

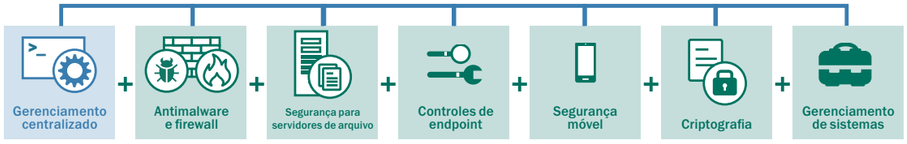
Gerenciamento de aplicativos móveis (Mobile Application Management - MAM) — Controla o limite do usuário ao executar aplicativos de listas brancas, impedindo a implementação de software indesejado ou desconhecido. '**Empacotamento de aplicativos**'isola dados corporativos em dispositivos pertencentes 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.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — ADVANCED



As ferramentas de gerenciamento de sistemas otimizam a eficiência e segurança de TI, enquanto a criptografia integrada protege dados sigilosos

O gerenciamento automatizado de correções e o gerenciamento de imagem do SO, a distribuição de software remoto e a integração SIEM ajudam a simplificar a administração, enquanto os inventários de hardware e software e o gerenciamento de licenças fornecem visibilidade e controle. A tecnologia de criptografia integrada adiciona uma camada poderosa de proteção de dados.

GERENCIAMENTO DE SISTEMAS

Gerenciamento de vulnerabilidades e correções — detecção e priorização automatizadas de vulnerabilidades do SO e de aplicativos, combinadas com a rápida distribuição automatizada de correções e atualizações.

Implementação do sistema operacional — fácil criação, armazenamento e implementação de imagens "golden" do SO a partir de um local centralizado, incluindo suporte a UEFI.

Distribuição e solução de problemas de software — implementação e aplicação remotas do software e atualização do SO disponível por demanda ou programada, incluindo suporte a Wake-on-LAN. A solução de problemas remota com economia de tempo e a distribuição eficiente de software são suportadas através da tecnologia Multicast.

Inventários de hardware e software e gerenciamento de licenças — a identificação, visibilidade e controle (incluindo bloqueio), juntamente com o gerenciamento de uso da licença, fornecem informações sobre todos os softwares e hardwares implementados por todo o ambiente, incluindo dispositivos removíveis. Estão disponíveis também: gerenciamento de licenças de software e hardware, detecção de dispositivos convidados, controles de privilégios e provisionamento de acesso.

Integração SIEM — suporte para sistemas IBM® QRadar e HP ArcSight SIEM.

Controle de acesso com base em função (Role Based Access Control - RBAC) — As responsabilidades administrativas podem ser atribuídas através de redes complexas, com exibição do console personalizada de acordo com as funções e direitos atribuídos

CRIPTOGRAFIA

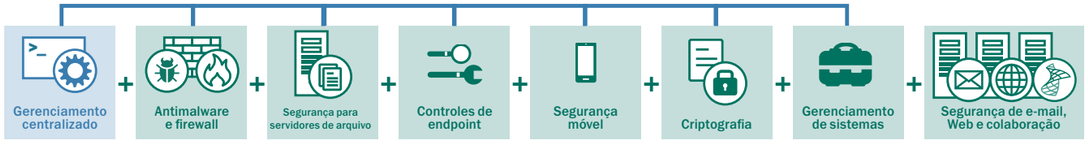
Poderosa proteção de dados — a criptografia dos arquivos / pastas (FLE) e do disco completo (FDE) pode ser aplicada aos endpoints. O suporte para o "modo portátil" garante a administração de criptografia em todos os dispositivos que saem dos domínios administrativos.

Conexão flexível do usuário — Autenticação pré-inicialização (Pre-boot authentication - PBA) para aumentar a segurança que inclui login único opcional para transparência do usuário. Também está disponível a autenticação com base em dois fatores ou em token.

Criação de políticas Integradas — Integração única de criptografia com controles de aplicativos e dispositivos fornece uma camada adicional de segurança aprimorada e facilidade administrativa

O Kaspersky Endpoint Security for Business — ADVANCED também inclui todos os componentes dos NÍVEIS SELECT e CORE.

KASPERSKY TOTAL SECURITY FOR BUSINESS



As organizações que exigem segurança abrangente para todo o seu ambiente de TI escolhem o Kaspersky Total Security for Business

O Kaspersky Total Security for Business apresenta a mais completa plataforma de proteção e gerenciamento oferecida atualmente no setor. O Kaspersky Total Security for Business protege todos os níveis de sua rede e inclui ferramentas de configuração avançadas para garantir que os usuários sejam produtivos e estejam livres das ameaças de malware, independentemente do dispositivo ou do local.

SEGURANÇA PARA SERVIDORES DE E-MAIL

Impede de maneira eficaz ameaças de malware, ataques de phishing e spams com base em e-mails por meio de atualizações em tempo real e com base na nuvem para proporcionar taxas de captura excepcionais e o mínimo de falsos positivos. Proteção antimalware para IBM® Domino® também incluída. A funcionalidade DLP para Microsoft Exchange está disponível separadamente.

SEGURANÇA PARA GATEWAYS DA INTERNET

Garante acesso seguro à Internet na organização, removendo automaticamente programas maliciosos e potencialmente hostis do tráfego HTTP(S) / FTP / SMTP e POP3.

SEGURANÇA PARA COLABORAÇÃO

Defende servidores e farms SharePoint® contra todas as formas de malware. A funcionalidade DLP para Sharepoint, disponível separadamente, permite que as funcionalidades de filtragem de conteúdo e arquivo identifiquem dados confidenciais e protejam contra o vazamento de dados.

O Kaspersky Total Security for Business também inclui todos os componentes dos níveis ADVANCED, SELECT e CORE.

▶ RECURSOS DO PRODUTO

Qual é a solução certa para você?

	Core	Select	Advanced	Total	Gerenciado pelo Security Center	Disponível em uma solução específica
Antimalware	•	•	•	•	•	
Firewall	•	•	•	•	•	
Controle de aplicativos		•	•	•	•	
Controle de dispositivos		•	•	•	•	
Controle da Web		•	•	•	•	
Segurança de servidores de arquivos		•	•	•	•	•
Proteção de endpoints móveis	•	•	•	•	•	
Gerenciamento de dispositivos móveis / aplicativos	•	•	•	•	•	
Criptografia			•	•	•	
Verificação de vulnerabilidades			•	•	•	•
Gerenciamento de correções			•	•	•	•
Inventários			•	•	•	•
Controle de licença			•	•	•	•
Distribuição de software			•	•	•	•
Implementação de sistemas operacionais			•	•	•	•
Segurança de servidores de colaboração				•		•
Segurança para servidores de e-mail				•	•	•
Segurança de gateways da Internet				•		•
Segurança da infraestrutura virtual					•	•
Segurança de servidores de armazenamento					•	•

• Incluso • Parcialmente incluso — consulte as páginas sobre o produto para obter mais detalhes

▶ KASPERSKY SECURITY FOR FILE SERVER

O Kaspersky Security for File Server fornece segurança confiável e escalonável e com ótimo custo-benefício para o armazenamento compartilhado de arquivos, sem impacto perceptível sobre o desempenho do sistema.

DESTAQUES

PROTEÇÃO ANTIMALWARE AVANÇADA
O mecanismo antimalware premiado da Kaspersky proporciona proteção poderosa para o servidor e impede que possíveis ameaças de malware mais recentes entrem na rede local por meio de programas maliciosos ou perigosos.

ALTO DESEMPENHO E CONFIABILIDADE
Saiba que o Kaspersky Security for File Server não deixará seu sistema mais lento nem interferirá nas operações de negócios, mesmo sob condições pesadas de carga da rede.

SUPORTE A VÁRIAS PLATAFORMAS
Uma solução de segurança única e eficaz para redes de servidores heterogêneos, com suporte às plataformas e aos servidores mais recentes, incluindo servidores de terminal, de cluster e virtuais, sem problemas de compatibilidade.

GERENCIAMENTO E RELATÓRIOS PODEROSOS
Ferramentas de gerenciamento eficientes e amigáveis, informações sobre o status de proteção dos servidores, configurações de tempo flexíveis para verificações e um extenso sistema de relatórios fornecem controle eficiente da segurança de servidores, ajudando a reduzir o custo total de propriedade.

RECURSOS

- **Proteção antimalware em tempo real** para servidores de arquivos que executam as versões mais recentes do Windows® (incluindo Windows Server® 2012/R2), Linux® e FreeBSD (ambos incluindo o Samba).
- **Proteção de servidores de terminal Citrix e Microsoft®.**
- **Totalmente compatível com servidores de cluster.**
- **Escalabilidade** — dando suporte e protegendo até mesmo as infraestruturas heterogêneas mais complexas com facilidade.
- **Confiabilidade, estabilidade e alta tolerância a falhas.**
- **Tecnologia de verificação otimizada inteligente** inclusive por demanda e com a verificação de áreas críticas do sistema.
- **As zonas confiáveis** ajudam a aumentar o desempenho da segurança e, ao mesmo tempo, a reduzir os níveis de recursos necessários para a verificação.
- **Quarentena e backup** de dados anteriores à desinfecção ou exclusão.
- **Isolamento** de estações de trabalho infectadas.
- **Instalação, gerenciamento e atualizações centralizados** com opções de configuração flexíveis.
- **Cenários flexíveis de resposta a incidentes.**
- **Relatórios abrangentes** sobre o status de proteção da rede.
- **Sistema de notificações sobre o status de aplicativos.**
- **Suporte a sistemas de Gerenciamento de Armazenamento Hierárquico** (HSM).
- **Suporte comprovado ao Hyper-V e Xen Desktop.**
- **VMware Ready.**
- **Suporte a ReFS.**

O Kaspersky Security for File Server está incluído no Kaspersky Endpoint Security for Business — SELECT e ADVANCED, assim como o Kaspersky Total Security for Business. Também está disponível para compra separadamente como uma solução direcionada.

SOBRE A NOSSA TECNOLOGIA DE 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 ajudam 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 endpoints, sem comprometer a produtividade.

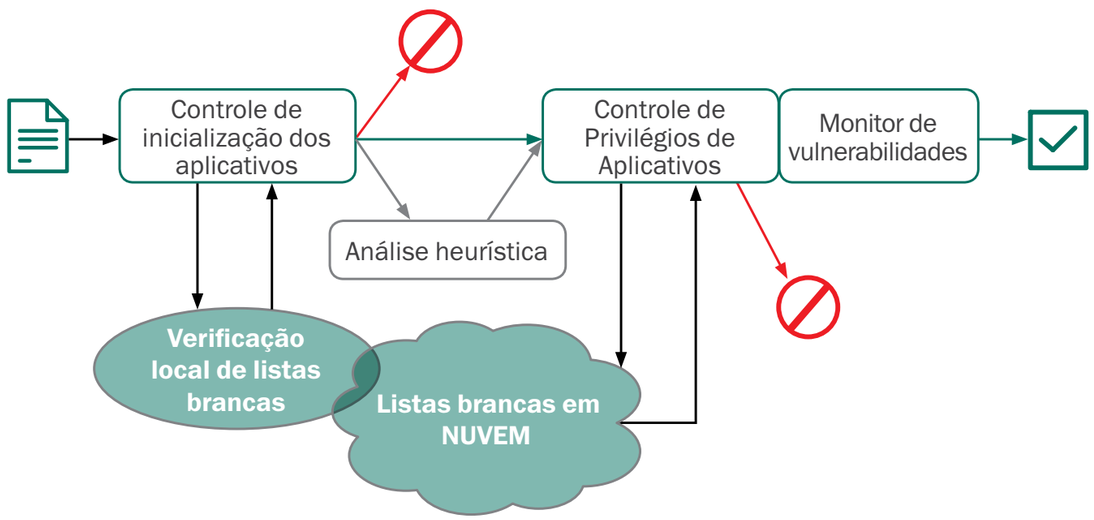
CONTROLE DE APLICATIVOS E LISTAS BRANCAS DINÂMICAS

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 endpoints 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**: Regula e controla 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" abrangentes, 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.

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 endpoints são gerenciados a partir do mesmo console, através de uma única interface.

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.

CONTROLES 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.

A tecnologia de Controles de endpoints está incluída no Kaspersky Endpoint Security for Business — SELECT e ADVANCED, e no Kaspersky Total Security for Business.

KASPERSKY SECURITY FOR MOBILE

Os dispositivos móveis estão cada vez mais atraentes para os criminosos virtuais. Enquanto isso, "Traga seu próprio dispositivo" (BYOD - Bring Your Own Device) está contribuindo para um mix cada vez mais complexo de dispositivos, criando um ambiente de gerenciamento e controle desafiador para administradores de TI.

O Kaspersky Security for Mobile garante a segurança de seu dispositivo, não importa onde ele esteja. Protege contra malware móvel em constante evolução. Ganhe visibilidade e controle sobre os smartphones e tablets em seu ambiente rapidamente e facilmente, a partir de uma localização central e com transtornos mínimos.

PRINCIPAIS RECURSOS DO PRODUTO

- **Antimalware avançado**
- **Antiphishing e antispam**
- **Proteção na Web**
- **Controle de aplicativos**
- **Detecção de Rooting / jailbreak**
- **Conteinerização**
- **Antirroubo**
- **Gerenciamento de dispositivos móveis**
- **Portal de autoatendimento**
- **Gerenciamento centralizado**
- **Console da Web**
- **Plataformas compatíveis:**
  - **Android™**
  - **iOS**
  - **Windows® Phone**

DESTAQUES

ANTIMALWARE AVANÇADO PARA DISPOSITIVOS MÓVEIS E SEGURANÇA DE DADOS

Só em 2014, a Kaspersky Lab lidou com quase 1,4 milhões de ataques móveis únicos de malware. O Kaspersky Security for Mobile combina antimalware com camadas profundas de tecnologias de proteção, protegendo os dados armazenados em dispositivos móveis contra ameaças conhecidas e desconhecidas.

GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM)

A integração com todas as plataformas líderes de gerenciamento de dispositivos móveis permite implementação e controle remotos OTA (Over the Air, por conexão sem fio) para facilitar a usabilidade e gerenciamento de dispositivos Android, iOS e Windows Phone.

GERENCIAMENTO DE APLICATIVOS MÓVEIS (MAM)

As funcionalidades de limpeza seletiva e conteinerização permitem a separação de dados pessoais e empresariais no mesmo dispositivo - compatíveis com iniciativas BYOD. Juntamente com a nossa funcionalidade de criptografia e antimalware, essas características fazem com que o Kaspersky Security for Mobile seja uma solução de proteção móvel proativa, ao invés de simplesmente tentar isolar um dispositivo e seus respectivos dados.

GERENCIAMENTO CENTRALIZADO

Gerencia várias plataformas e dispositivos a partir do mesmo console como outros endpoints - aumenta a visibilidade e controle sem esforço ou tecnologia adicional para gerenciar.

RECURSOS DE SEGURANÇA E GERENCIAMENTO MÓVEIS

ANTIMALWARE AVANÇADO

Proteção com base em assinaturas, proativa e assistida em nuvem (via Kaspersky Security Network - KSN) contra ameaças de malware móveis conhecidas e desconhecidas. Verificações por demanda e programadas combinadas com atualizações automáticas para aumentar a proteção.

ANTIPHISHING E ANTISPAM

Poderosas tecnologias antiphishing e antispam protegem o dispositivo e seus dados de ataques de phishing e ajudam a filtrar chamadas e textos indesejados.

CONTROLE DA WEB/NAVEGAÇÃO SEGURA

Compatível com a Kaspersky Security Network (KSN), essas tecnologias trabalham em tempo real para bloquear o acesso a sites da Web maliciosos e não autorizados. Um navegador seguro entrega análise de reputação constantemente atualizada, garantindo navegação móvel segura.

CONTROLE DE APLICATIVOS

Integrados com a KSN, os Controles de aplicativos restringem o uso do aplicativo para apenas softwares aprovados, proibindo o uso de software desconhecido ou não autorizado. Torna a funcionalidade do dispositivo dependente da instalação de aplicativos necessários. O controle de inatividade do aplicativo permite que administradores exijam que o usuário reconecte-se se um aplicativo estiver ocioso por um período de tempo definido. Essa característica protege os dados mesmo se um aplicativo estiver aberto quando o dispositivo for perdido ou roubado.

DETECÇÃO DE ROOTING / JAILBREAK

Detecção e relatórios automáticos de rooting ou jailbreaking podem ser acompanhados com bloqueio automático de acesso aos contêineres, limpeza seletiva ou limpeza total do dispositivo.

CONTEINERIZAÇÃO

Dados pessoais e empresariais independentes através do "empacotamento" de aplicativos em contêineres. Políticas adicionais, como a criptografia, podem ser aplicadas para proteger dados sigilosos. A limpeza seletiva permite a exclusão de dados conteinerizados em um dispositivo quando um funcionário deixa a empresa, sem causar impacto nos dados pessoais.

ANTIRROUBO

Recursos remotos Antirroubo, incluindo limpeza, bloqueio do dispositivo, localização, verificação do chip, detecção de dispositivo por "retrato" e "alarme", podem ser ativados em caso de perda ou roubo do dispositivo. Dependendo do caso, os comandos antirroubo podem ser aplicados de uma forma muito flexível. Por exemplo, a integração com o Google Cloud Messaging (GCM) permite entregar os comandos quase imediatamente, aumentando os tempos de reação e melhorando a segurança, enquanto que enviar comandos através do Portal de autoatendimento não exige ações do administrador.

GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM)

Compatível com Microsoft® Exchange ActiveSync, Apple MDM e Samsung KNOX 2.0 – permite uma ampla gama de políticas, através de uma interface unificada, independentemente da plataforma. Por exemplo, aplica criptografia e senhas ou controla o uso da câmera aplicando políticas a usuários individuais ou grupos, gerenciando configurações APN/VPN, etc

PORTAL DE AUTOATENDIMENTO

Delega o gerenciamento de segurança de rotina aos funcionários, permite o auto registro dos dispositivos aprovados. Durante o processo de habilitação de novo dispositivo, todos os certificados exigidos podem ser entregues automaticamente através do portal, sem necessidade de envolvimento do administrador. Em caso de perda do dispositivo, o funcionário pode realizar todas as ações Antirroubo disponíveis através do Portal.

GERENCIAMENTO CENTRALIZADO

Gerencia todos os dispositivos móveis de forma central, a partir de um único console, que também permite o gerenciamento da segurança de TI para todos os outros endpoints. O Console da Web permite aos administradores controlar e gerenciar dispositivos remotamente, de qualquer computador.

O Kaspersky Security for Mobile está incluído no Kaspersky Endpoint Security for Business — SELECT e ADVANCED, assim como o Kaspersky Total Security for Business. Também está disponível para compra separadamente como uma solução direcionada.

SOBRE A NOSSA TECNOLOGIA DE CRIPTOGRAFIA

Impede o acesso não autorizado a dados causado pela perda ou roubo do dispositivo, ou malware para roubo de dados.

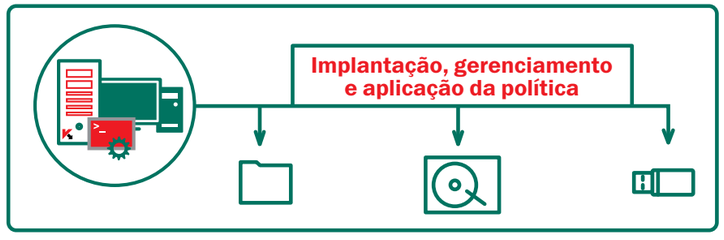
Proteção de dados e conformidade proativos são um imperativo global. A tecnologia de criptografia da Kaspersky Lab protege os dados valiosos contra perda acidental, roubo do dispositivo e ataques de malware direcionados. Ao combinar a poderosa tecnologia de criptografia com as tecnologias líderes do setor de proteção de endpoints da Kaspersky Lab, a nossa plataforma integrada protege os dados em repouso e em movimento.

Por ser da Kaspersky Lab, é fácil de implementar e administrar a partir de um console de gerenciamento centralizado, utilizando uma única política.

Impede a perda de dados e o acesso não autorizado às informações com a Tecnologia de criptografia da Kaspersky Lab:

- **Criptografia do disco completo (FDE)**
- **Arquivo/Nível de pasta (FLE)**
- **Dispositivos removíveis e internos**

ADMINISTRADO ATRAVÉS DE UM ÚNICO CONSOLE DE GERENCIAMENTO

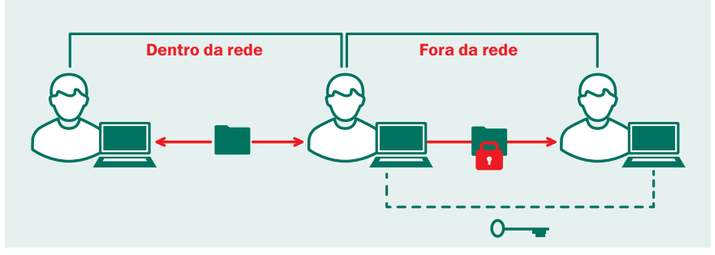


CRIPTOGRAFIA SEGURA PADRÃO DO SETOR
A Kaspersky Lab utiliza criptografia AES (Advanced Encryption Standard) de tamanho de chave de 256 bits com gerenciamento e garantia principais simplificados. É compatível com tecnologia Intel® AES-NI, plataformas UEFI e GPT.

FLEXIBILIDADE COMPLETA
A Kaspersky Lab oferece criptografia em nível de arquivo e pasta (FLE) e criptografia do disco completo (FDE), que abrange todos os possíveis cenários de uso. Os dados podem ser protegidos tanto nos discos rígidos como nos dispositivos removíveis. O "Modo portátil" permite o uso e transferência de dados em mídias removíveis criptografadas, mesmo em computadores sem o programa de criptografia — facilitando troca segura de dados "fora do perímetro".

LOGIN ÚNICO, TRANSPARÊNCIA DE USUÁRIO FINAL
Da configuração ao uso diário, a tecnologia de criptografia da Kaspersky Lab funciona de forma transparente em todos os aplicativos, sem impedir a produtividade do usuário final. O login único garante criptografia integrada — o usuário final não percebe que a tecnologia está sendo executada.

A criptografia da Kaspersky Lab permite a transferência de arquivos transparente e integrada entre os usuários dentro e fora da rede.



RECURSOS DE CRIPTOGRAFIA

INTEGRAÇÃO PERFEITA COM AS TECNOLOGIAS DE SEGURANÇA DA KASPERSKY LAB
Integração completa com antimalware da Kaspersky Lab, controles de endpoints e tecnologias de gerenciamento para uma verdadeira segurança multicamadas construídas sobre uma base de código comum. Por exemplo, uma única política poderia aplicar a criptografia em dispositivos removíveis específicos. Aplica configurações de criptografia sob a mesma política como antimalware, controle de dispositivos e outros elementos de segurança de endpoints. Não há necessidade de implementar e gerenciar soluções distintas. A compatibilidade de hardware de rede é automaticamente verificada antes da implementação da criptografia; suporte padrão para as plataformas UEFI e GPT.

CONTROLE DE ACESSO COM BASE EM FUNÇÃO
Em organizações maiores, opte por delegar o gerenciamento de criptografia usando a funcionalidade de controle de acesso com base em função. Isso permite o gerenciamento de criptografia menos complexo.

AUTENTICAÇÃO PRÉ-INICIALIZAÇÃO (PBA)
As credenciais do usuário são necessárias antes que o sistema operacional inicialize, proporcionando uma camada adicional de segurança, com login único opcional. A tecnologia de criptografia PBA da Kaspersky Lab também está disponível para layouts de teclado diferentes do QWERTY.

AUTENTICAÇÃO POR CARTÃO INTELIGENTE E TOKEN
Compatível com autenticação de dois fatores através de marcas populares de cartões inteligentes e tokens, eliminando a necessidade de nomes de usuários e senhas adicionais e melhorando a experiência do usuário final.

RECUPERAÇÃO DE EMERGÊNCIA
Os administradores podem descriptografar os dados em caso de falha de hardware ou software. A recuperação de senha do usuário para PBA ou o acesso aos dados criptografados são implementados através de um mecanismo simples de desafio/resposta.

IMPLEMENTAÇÃO OTIMIZADA, CONFIGURAÇÕES PERSONALIZÁVEIS
Para facilitar a implementação, a funcionalidade de criptografia da Kaspersky Lab está habilitada somente dentro dos níveis "Advanced" e "Total" do Kaspersky Endpoint Security for Business, sem necessidade de instalação separada. As configurações de criptografia são pré-definidas, mas podem ser personalizadas para pastas comuns, como Meus Documentos, Área de Trabalho, novas pastas, extensões de arquivos e grupos, tais como documentos do Microsoft® Office ou arquivos comprimidos de mensagens.

A tecnologia de criptografia está incluída no Kaspersky Endpoint Security for Business — ADVANCED, e no Kaspersky Total Security for Business.

KASPERSKY SYSTEMS MANAGEMENT

Aprimora a segurança, reduz a complexidade com ferramentas de gerenciamento centralizado de TI.

Vulnerabilidades não corrigidas em aplicativos populares são uma das maiores ameaças à segurança de TI empresarial. Este risco é agravado pelo aumento da complexidade de TI - se você não sabe o que tem, como pode protegê-lo?

Ao centralizar e automatizar tarefas essenciais de segurança, configuração e gerenciamento, tais como avaliação de vulnerabilidades, distribuição de correções e atualizações, gerenciamento de inventários e distribuição de aplicativos, administradores de TI economizam tempo e otimizam segurança.

O Kaspersky Systems Management ajuda a minimizar os riscos de segurança de TI e a suavizar a complexidade de TI, oferecendo aos gerentes controle e visibilidade completa, em tempo real, sobre vários dispositivos, aplicativos e usuários, a partir de uma única tela.

PRINCIPAIS RECURSOS DO PRODUTO

- **Verificação de vulnerabilidades e gerenciamento de correções**
- **Inventários de hardware e software**
- **Instalação de software e solução de problemas remotos, incluindo a cobertura de escritórios remotos**
- **Implementação de sistemas operacionais**
- **Integração SIEM**
- **CONTROLE DE ACESSO COM BASE EM FUNÇÃO**
- **Gerenciamento centralizado**

SEGURANÇA APRIMORADA
Aumenta a segurança de TI e reduz as cargas de tarefas rotineiras oportunamente e as correções e atualizações automatizadas. A descoberta e priorização de vulnerabilidades automatizadas suporta uma maior eficiência e reduz a sobrecarga de recursos. Testes independentes[1] mostram que a Kaspersky Lab oferece a mais abrangente e automatizada cobertura de correções e atualizações, no tempo mais rápido.

CONTROLE COM VISIBILIDADE TOTAL
Visibilidade total da rede a partir de um único console elimina a adivinhação do administrador e fornece o conhecimento de todos os aplicativos e dispositivos (incluindo dispositivos convidados) que entram na rede. Isso direciona o controle centralizado de usuários e o acesso de dispositivos aos dados da organização e aplicativos de acordo com as políticas da TI.

GERENCIAMENTO CENTRALIZADO
O Gerenciamento de sistemas da Kaspersky Lab é um componente gerenciado do Kaspersky Security Center. Cada recurso é acessado e gerenciado através deste console central, usando comandos e interfaces intuitivas e consistentes para automatizar tarefas rotineiras de TI.

RECURSOS

VERIFICAÇÃO DE VULNERABILIDADES E GERENCIAMENTO DE CORREÇÕES
A verificação automatizada de software permite rápida detecção, priorização e neutralização de vulnerabilidades. Correções e atualizações podem ser entregues automaticamente, em prazos mais curtos[2], para software Microsoft® e outros. O administrador é notificado sobre o status da instalação das correções. Correções com menor importância podem ser adiadas para depois do expediente, mesmo se os computadores estiverem desligados, usando Wake-on-LAN. Transmissão Multicast permite distribuição local de correções e atualizações a escritórios remotos, reduzindo os requisitos de largura de banda.

INVENTÁRIOS DE HARDWARE E SOFTWARE
A descoberta automática, o inventário e a notificação e acompanhamento de hardware e software, incluindo dispositivos removíveis, fornecem aos administradores informações detalhadas sobre os dispositivos e ativos utilizados na rede corporativa. Dispositivos convidados podem ser detectados e receber acesso à Internet. O controle de licença fornece visibilidade em número de nós e prazo de validade.

PROVISIONAMENTO FLEXÍVEL DE SISTEMAS OPERACIONAIS E APLICATIVOS
Imagens do sistema otimamente protegidas são centralizadas, de fácil criação, armazenamento, clonagem e implementação. Implementação depois do expediente via Wake-on-LAN com edição pós-instalação para obter maior flexibilidade. Suporte a UEFI.

DISTRIBUIÇÃO DE SOFTWARE
Implementação/atualização remota, a partir de um único console. Mais de 100 aplicativos populares, identificados através da Kaspersky Security Network podem ser instalados automaticamente depois do expediente, se necessário. Suporte completo para solução remota de problemas, com segurança aprimorada, através de permissões de usuário e registros/auditorias de sessão. Economiza no tráfego para escritórios remotos com tecnologia Multicast para distribuição local de software.

INTEGRAÇÃO SIEM
Reporta diretamente e efetua transferências de eventos para os principais sistemas de SIEM — IBM® QRadar e HP ArcSight. Coleta registros e outros dados relacionados com a segurança para análise, minimizando a carga de trabalho e ferramentas do administrador, além de simplificar relatórios de nível empresarial.

CONTROLE DE ACESSO COM BASE EM FUNÇÃO
Distingue funções e responsabilidades administrativas em redes complexas. Personaliza a exibição do console de acordo com a função e os direitos.

GERENCIAMENTO CENTRALIZADO
Como um console de administração integrado, o Kaspersky Security Center dá suporte à administração de segurança de sistemas para desktops, dispositivos móveis e endpoints virtuais em toda a rede, através de uma única interface.

1, 2 Teste de soluções de gerenciamento de correções encomendado pela Kaspersky Lab e executado pela AV-TEST GmbH (Julho de 2013)

O Gerenciamento de Sistemas Kaspersky está incluído no Kaspersky Endpoint Security for Business — ADVANCED, e no Kaspersky Total Security for Business, e também está disponível para compra separadamente como uma solução direcionada.

KASPERSKY SECURITY FOR MAIL SERVER

O Kaspersky Security for Mail Server proporciona excelente proteção para o tráfego em execução em servidores de e-mail contra spam, phishing, malware e ameaças de malware genéricas e avançadas, mesmo nas infraestruturas heterogêneas mais complexas.

Proteção contra perda de dados confidenciais através de e-mails e anexos também é fornecida para Microsoft® Exchange Server Environments.

DESTAQUES

PROTEÇÃO CONTRA AMEAÇAS DE MALWARE
Avançada proteção contra malware é fornecida pelo mecanismo antimalware premiado da Kaspersky, com suporte em tempo real pela Kaspersky Security Network assistida em nuvem, e com proteção proativa contra exploits e filtragem de URLs maliciosos.

PROTEÇÃO ANTISPAM
Para servidores de e-mail do Microsoft Exchange e com base em Linux®, o mecanismo antispam assistido em nuvem da Kaspersky tem ajudado a reduzir até 99,96% de spams que auxiliam na perda de recursos e de tempo, com o mínimo de falsos positivos.

PROTEÇÃO E CONTROLE DE PERDA DE DADOS (SERVIDORES DO MICROSOFT EXCHANGE)*
AO IDENTIFICAR A INCLUSÃO DE DADOS EMPRESARIAIS, FINANCEIROS, PESSOAIS E OUTROS DADOS SIGILOSOS EM E-MAILS ENVIADOS E ANEXOS NOS SERVIDORES DO MICROSOFT EXCHANGE, E AO CONTROLAR O FLUXO DESTAS INFORMAÇÕES, O KASPERSKY SECURITY FOR MAIL SERVES PROTEGE SEUS DADOS CONFIDENCIAIS E OS DE SEUS FUNCIONÁRIOS, GARANTINDO A CONFORMIDADE COM A LEGISLAÇÃO DE PROTEÇÃO DE DADOS. TÉCNICAS ANALÍTICAS SOFISTICADAS, INCLUINDO PESQUISAS DE DADOS ESTRUTURADAS E GLOSSÁRIOS ESPECÍFICOS DE NEGÓCIOS AJUDAM A IDENTIFICAR E-MAILS SUSPEITOS QUE PODEM ENTÃO SER BLOQUEADOS. O SISTEMA PODE ATÉ ALERTAR GERENTE DE LINHA DO REMETENTE PARA A POTENCIAL FALHA DE SEGURANÇA DE DADOS.

ADMINISTRAÇÃO SIMPLES E FLEXÍVEL
Ferramentas de gerenciamento e criação de relatórios amigáveis e configurações de verificação flexíveis dão a você um controle eficiente da segurança de seu e-mail e documentos, ajudando a reduzir o custo total de propriedade.

RECURSOS

- Proteção antimalware em tempo real suportada pela Kaspersky Security Network assistida na nuvem.
- Proteção imediata contra exploits desconhecidos e até mesmo vulnerabilidades de dia zero.
- Proteção avançada contra spam - o mecanismo antispam da Kaspersky Lab bloqueia mais de 99% do tráfego de e-mails indesejados.
- Proteção contra vazamento de dados (Microsoft Exchange Servers)*. Detecção de informações confidenciais em e-mails e anexos, por meio de categorias (incluindo dados sobre detalhes pessoais e sobre cartões de pagamento), glossários e análise em nível profundo usando dados estruturados.
- Verificação antispam assistida em nuvem em tempo real de todas as mensagens dos servidores Microsoft® Exchange, incluindo pastas públicas, usando a Kaspersky Security Network.
- Verificação programada de e-mails e bancos de dados Lotus Domino.
- Verificação de mensagens, bancos de dados e outros objetos nos servidores IBM® Domino®.
- Filtragem de mensagens por formato, tamanho e nome de anexos reconhecidos.
- Processo de atualização fácil e prático do banco de dados de antispam e antimalware.
- Armazenamento de backup de dados anteriores à desinfecção ou exclusão.
- Escalabilidade e tolerância a falhas.
- Fácil instalação e administração integrada flexível.
- Sistema de notificações sofisticado.
- Relatórios abrangentes sobre o status de proteção da rede.

* Ao comprar este produto, a opção para evitar a perda ou vazamento de dados confidenciais é vendida separadamente.

KASPERSKY SECURITY FOR INTERNET GATEWAY

O Kaspersky Security for Internet Gateway é uma solução antimalware global que garante a segurança do acesso à Internet para toda sua equipe de trabalho.

DESTAQUES

A PROTEÇÃO AVANÇADA REDUZ O TEMPO DE INATIVIDADE E POSSÍVEIS TRANSTORNOS
O mecanismo antimalware premiado da Kaspersky Labs impede que possíveis ameaças de malware mais recentes entrem na rede local por meio de programas maliciosos ou perigosos.

EFICIÊNCIA DO DESEMPENHO ATRAVÉS DA OTIMIZAÇÃO
A tecnologia de verificação e o balanceamento de carga otimizada e inteligente reduzem a carga dos recursos, ajudando a poupar largura de banda, sem comprometer o desempenho da segurança.

SUPORTE A VÁRIAS PLATAFORMAS
Suporte para as mais recentes plataformas e servidores, inclusive os servidores proxy, ideal para volumes intensos de tráfego de rede em ambientes heterogêneos. O suporte ao Microsoft® Forefront® TMG estende-se ao e-mail corporativo e à proteção de gateways da Web.

GERENCIAMENTO E GERAÇÃO SIMPLIFICADOS DE RELATÓRIOS
Ferramentas de gerenciamento simples e amigáveis, configurações de verificação flexíveis e sistemas de relatórios de status de proteção.

RECURSOS

- **Proteção proativa contra** ameaças de malware conhecidas e emergentes.
- **Excelentes taxas de detecção de malware** combinadas com o mínimo de falsos positivos.
- **Tecnologia de verificação otimizada e inteligente.**
- **Verificação em tempo real** do tráfego HTTP, HTTPS e FTP de servidores publicados.
- **Proteção para Squid**, um dos servidores proxy Linux mais populares.
- **Ferramentas práticas** para instalação, gerenciamento e atualizações.
- **Ferramentas de verificação flexíveis e cenários de resposta a incidentes**.
- **Balanceamento de carga** de processadores de servidores.
- **Escalabilidade e tolerância a falhas.**
- **Relatórios abrangentes** sobre o status de proteção de rede.

RECURSOS ESPECÍFICOS PARA SERVIDORES MICROSOFT® FOREFRONT® TMG E ISA:

- Monitoramento do status de proteção de aplicativos em tempo real.
- Verificação de conexões VPN.
- Verificação em tempo real do tráfego HTTPS (apenas TMG).
- Proteção de tráfego de e-mail (via protocolos POP3 e SMTP).
- Armazenamento de backup (apenas TMG).

O Kaspersky Security for Mail Server e o Kaspersky Security for Internet Gateway estão incluídos no Kaspersky Total Security for Business, e também estão disponíveis para compra separadamente como soluções direcionadas.

KASPERSKY SECURITY FOR COLLABORATION

Proteção de dados e controle de plataformas de colaboração, incluindo farms do SharePoint.

DESTAQUES

PROTEGE TOTALMENTE SUA PLATAFORMA SHAREPOINT
A poderosa proteção contra ameaças conhecidas, desconhecidas e avançadas é fornecida através da Kaspersky Security Network com base em nuvem, enquanto que a tecnologia antiphishing protege os dados colaborativos contra ameaças com base na Web.

IMPEDE O VAZAMENTO DE DADOS CONFIDENCIAIS*
Usando dicionários pré-instalados ou personalizados e categorias de dados, o Kaspersky Security for Collaboration verifica cada documento colocado em servidores SharePoint para obter informações sigilosas, palavra por palavra e frase por frase.

APLICA POLÍTICAS DE COMUNICAÇÃO
Os recursos de filtragem e conteúdo ajudam a reforçar suas políticas de comunicação e seus padrões, identificando e bloqueando conteúdos inadequados, ao mesmo tempo em que impedem o armazenamento desnecessário de arquivos e formatos de arquivo inadequados.

RECURSOS

PROTEÇÃO ANTI malware
- **Verificação ao acessar** — arquivos são verificados em tempo real, durante o upload ou download.
- **Verificação em segundo plano** — arquivos armazenados no servidor são verificados regularmente usando as assinaturas de malwares mais recentes.
- **Integração com a Kaspersky Security Network** — fornecendo proteção em tempo real assistida em nuvem até mesmo contra ameaças de "dia zero".

SUPORTE PARA AS POLÍTICAS DE COMUNICAÇÃO DA SUA EMPRESA
- **A filtragem de arquivo** — ajuda a aplicar as políticas de armazenamento de documentos e a reduzir demandas nos dispositivos de armazenamento. Analisando formatos de arquivo reais, independentemente do nome da extensão, o aplicativo assegura que usuários não usem um tipo de arquivo banido, pois estarão violando a política de segurança.
- **Proteção de wikis/blogs** — protege todos os repositórios de SharePoint, incluindo wikis e blogs.
- **A filtragem de conteúdo** — evita o armazenamento de arquivos que incluem conteúdo inadequado. O conteúdo de cada arquivo é analisado, com base nas palavras-chave. Os clientes também podem criar seus próprios dicionários personalizados para filtragem de conteúdo.

PREVENÇÃO DE PERDA DE DADOS CONFIDENCIAIS*
- **Verificação de documentos para obter informações confidenciais.** A solução integra módulos que identificam tipos específicos de dados, o que confirma que cumpre as normas legais pertinentes - por exemplo, dados pessoais (definido por conformidades regulatórias, como HIPAA ou diretrizes da UE 95/46EC) ou dados padrão do PCI DSS (Payment Card Industry Data Security Standard). Os dados são verificados contra dicionários integrados e temáticos, atualizados regularmente e contra dicionários personalizados.
- **Pesquisa de dados estruturados** — se informações apresentadas em estruturas específicas são encontradas em uma mensagem, elas serão tratadas como potencialmente confidenciais, o que garante o controle sobre dados sigilosos, como bancos de dados de clientes, realizado em matrizes complexas.

GERENCIAMENTO FLEXÍVEL
- **Facilidade de gerenciamento** — um farm de servidores inteiro pode ser gerenciado centralmente a partir de um único console. Uma interface intuitiva inclui todos os cenários administrativos mais frequentemente utilizados.
- **Painel único** — um painel claramente projetado permite acesso em tempo real ao status atual do produto, ao status da versão e da licença do banco de dados de todos os servidores protegidos.
- **Backup de arquivos modificados** — no caso de um incidente, se necessário, os arquivos originais podem ser restaurados, e as informações detalhadas de backup sobre arquivos modificados podem ser utilizadas para apoiar as investigações.
- **Integração com Active Directory®** — ativa autenticação de usuários do Active Directory.

O Kaspersky Security for Collaboration está incluído no Kaspersky Total Security for Business e também está disponível para compra separadamente como uma solução direcionada.

* Ao comprar este produto, a opção para evitar a perda ou vazamento de dados confidenciais é vendida separadamente.

KASPERSKY SECURITY FOR STORAGE

Proteção de alto desempenho para Armazenamentos EMC, NetApp, Hitachi e IBM®.

DESTAQUES

AVANÇADA PROTEÇÃO ANTIMALWARE EM TEMPO REAL
Proteção proativa para soluções NAS (Network Attached Storage). O avançado mecanismo antimalware da Kaspersky verifica todos os arquivos executados ou modificados em relação a todas as formas de malware, incluindo vírus, worms e cavalos de Troia. A análise heurística avançada identifica ameaças novas e desconhecidas.

DESEMPENHO OTIMIZADO
A verificação de alto desempenho, com tecnologia de verificação otimizada e configurações de exclusão flexíveis, oferece máxima proteção e minimiza o impacto sobre o desempenho do sistema.

CONFIÁVEL
Uma tolerância a falhas excepcional é obtida através de uma arquitetura simples, utilizando componentes unificados criados e construídos para trabalharem em conjunto com perfeição. O resultado é uma solução estável e resistente que, quando desativada, será reiniciada automaticamente para uma proteção confiável e contínua.

FÁCIL ADMINISTRAÇÃO
Os servidores "prontos para usar" são instalados e protegidos remotamente, sem reinicializações, e administrados em conjunto através de um console central simples e intuitivo - o Kaspersky Security Center - junto com as outras soluções de segurança da Kaspersky.

RECURSOS

SEGURANÇA PROATIVA
O Kaspersky, líder do setor de mecanismos de verificação antimalware, desenvolvido por especialistas em inteligência de ameaças de todo o mundo, fornece proteção proativa contra ameaças emergentes e potenciais utilizando tecnologias inteligentes para uma detecção aprimorada.

ATUALIZAÇÕES AUTOMÁTICAS
Os bancos de dados antimalware são atualizados automaticamente, sem interromper a verificação, garantindo a proteção contínua e minimizando a carga de trabalho do administrador.

PROCESSOS DE EXCLUSÃO E ZONAS CONFIÁVEIS
O desempenho da verificação pode ser ajustado com o uso de "zonas confiáveis" que, juntamente com formatos de arquivo e processos, como backups de dados, podem ser excluídos da verificação.

VERIFICAÇÃO DE OBJETOS COM EXECUÇÃO AUTOMÁTICA
Para maior proteção do servidor, é possível realizar verificações do sistema operacional e dos arquivos com execução automática para evitar que malwares sejam inicializados durante a reinicialização do sistema.

VERIFICAÇÃO FLEXÍVEL PARA UM DESEMPENHO OTIMIZADO
Reduz o tempo de verificação e configuração e promove o balanceamento de carga, ajudando a otimizar o desempenho do servidor. O administrador pode especificar e controlar a profundidade, amplitude e duração da atividade de verificação, definindo quais são os tipos de arquivos e as áreas que devem ser verificados. A verificação por demanda pode ser programada para períodos de baixa atividade do servidor.

PROTEGE SOLUÇÕES HSM E DAS
Dá suporte aos modos de verificação off-line para proteção eficiente dos sistemas de Gerenciamento de Armazenamento Hierárquico (HSM). A proteção DAS (Direct Attached Storage) também ajuda a promover a utilização de soluções de armazenamento de baixo custo.

SUPORTE PARA TODOS OS PRINCIPAIS PROTOCOLOS
O Kaspersky Security for Storage suporta os principais protocolos usados por diferentes sistemas de armazenamento: agente CAVA RPC e ICAP.

PROTEÇÃO DE SISTEMAS VIRTUAIS E SERVIDORES DE TERMINAL
A segurança flexível inclui proteção para sistemas operacionais virtuais (convidados) em ambientes virtuais Hyper-V e VMware e para infraestruturas de terminal da Microsoft® e Citrix.

ADMINISTRAÇÃO

INSTALAÇÃO E GERENCIAMENTO CENTRALIZADOS
A instalação, a configuração e o gerenciamento remotos, incluindo notificações, atualizações e relatórios flexíveis, são administrados através do intuitivo Kaspersky Security Center. O gerenciamento por linha de comando também está disponível, se preferido.

CONTROLE SOBRE PRIVILÉGIOS DE ADMINISTRADOR
Níveis de privilégios diferentes podem ser atribuídos a cada administrador do servidor, ajudando a manter a conformidade com as políticas corporativas específicas da segurança de TI.

RELATÓRIOS FLEXÍVEIS
São fornecidos por meio de relatórios gráficos ou revisões dos logs de eventos do Microsoft Windows® ou do Kaspersky Security Center. Ferramentas de pesquisa e de filtragem proporcionam acesso rápido a dados em logs de grande volume.

KASPERSKY SECURITY FOR VIRTUALIZATION

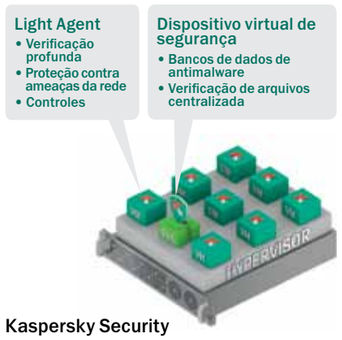
O Kaspersky Security for Virtualization é uma solução flexível que oferece proteção e desempenho para seu ambiente.

AGENTE LEVE PARA PROTEÇÃO AVANÇADA

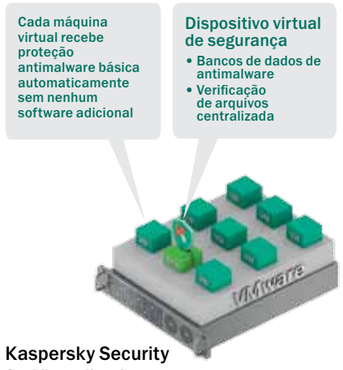
O Kaspersky Security for Virtualization inclui um agente poderoso, mas leve, que é implementado em cada máquina virtual. Isso permite a ativação de recursos avançados de segurança de endpoints. Como monitoramento de vulnerabilidades, controles de aplicativos, de dispositivos e da Web, proteção antivírus para mensagens instantâneas, e-mails e Web, além de heurística avançada. O resultado é uma segurança sólida e em vários níveis combinada com um desempenho eficiente.

CONFIGURAÇÃO OPCIONAL SEM AGENTES PARA AMBIENTES VMWARE

A forte integração com as tecnologias VMware significa que o Kaspersky Security for Virtualization também pode ser facilmente implementado e gerenciado nessa plataforma em uma configuração de segurança sem agentes. Todas as atividades de segurança estão concentradas no dispositivo virtual de segurança, que faz interface com o vShield para a proteção automática e instantânea das máquinas virtuais, e com o vCloud para a proteção da rede.



Kaspersky Security for Virtualization
Configuração light agent



Kaspersky Security for Virtualization
Configuração sem agentes*

PRINCIPAIS RECURSOS DO PRODUTO

- **Gerenciamento centralizado através do Kaspersky Security Center**
- **Proteção centralizada de VMs com base em SVA**
- **Antimalware avançado**
- **Prevenção contra intrusão com base em host (HIPS) e firewall**
- **Controles de endpoint para aplicativos, acesso à Web e periféricos**
- **Segurança assistida na nuvem através da Kaspersky Security Network**
- **Bloqueio de ataques de rede**
- **Antiphishing**
- **Antivírus para mensagens instantâneas, e-mail e tráfego da Internet**
- **Nenhuma instalação adicional ou reinicialização para novas VMs****

LICENCIAMENTO FLEXÍVEL

Dependendo de suas necessidades, o Kaspersky Security for Virtualization está disponível com as seguintes opções de licença:

- Licenciamento com base em máquina:
  - Por desktop
  - Por servidor
- Licenciamento com base em recursos:
  - Por núcleo.

DIVERSAS PLATAFORMAS: CUSTO ÚNICO

Uma única licença do Kaspersky Security for Virtualization inclui suporte para ambientes virtuais com base em Citrix, Microsoft® e VMware.

DISPOSITIVO VIRTUAL DE SEGURANÇA (SVA)

A Kaspersky Lab oferece duas soluções interessantes dessa categoria, com base em um dispositivo virtual de segurança.

O dispositivo virtual de segurança (SVA) da Kaspersky Lab verifica de forma centralizada todas as VMs no ambiente do host. Essa arquitetura promove a proteção eficiente das VMs sem sacrificar os recursos dos endpoints com a eliminação das verificações antivírus, das 'tempestades' de atualizações e dos períodos de latência, gerando assim taxas de consolidação melhores.

INTEGRAÇÃO COM A ARQUITETURA DAS PLATAFORMAS

O Kaspersky Security for Virtualization é compatível com as plataformas VMware, Microsoft® Hyper-V® e Citrix Xen e com suas principais tecnologias.

VMware	Microsoft Hyper-V	Citrix Xen
Alta disponibilidade	Memória dinâmica	Controle de memória dinâmica
Integração do vCenter	Volumes compartilhados em cluster	Proteção e recuperação de VM (VMPR)
vMotion – host DRS	Backup em tempo real	XenMotion (migração em tempo real)
Horizon view (clones completos e clones vinculados)	Migração em tempo real	ICA multistream
		Receptor Citrix
		vDisk pessoal

* Recursos de segurança avançados, como quarentena de arquivos, HIPS, verificação de vulnerabilidades e controles de endpoints, não estão disponíveis nesta configuração.
** Para VMs não permanentes, há proteção instantânea disponível depois de incluir o agente leve na imagem da VM. Para VMs permanentes, o administrador deve implementar o agente leve manualmente durante a instalação.

SERVIÇOS DE INTELIGÊNCIA DE SEGURANÇA KASPERSKY

Como um profissional de segurança CISO/de nível sênior, é sua responsabilidade proteger sua organização contra as ameaças atuais e antecipar os perigos que vêm pela frente nos próximos anos. Isso exige um nível de inteligência de segurança estratégica que poucas empresas têm os recursos para desenvolver internamente.

A Kaspersky Lab é um parceiro de negócios valioso, sempre disponível para compartilhar inteligência atualizada através de diferentes canais, ajudando sua equipe de segurança de SOC/TI a permanecer totalmente equipada para proteger a organização de qualquer ameaça on-line.

EDUCAÇÃO SOBRE SEGURANÇA VIRTUAL
O programa de educação sobre segurança virtual da Kaspersky Lab foi desenvolvido especificamente para qualquer organização que procura promover o papel da segurança virtual, a fim de melhor proteger sua infraestrutura e propriedade intelectual.

O programa abrange tudo, desde os fundamentos em segurança a perícia digital avançada e análise de malware, ajudando os clientes a melhorar o seu conhecimento de segurança virtual em três áreas principais:

- Conhecimentos fundamentais do tópico
- Perícia digital e resposta a incidentes
- Análise de malware & engenharia reversa

FEEDS DE DADOS DE AMEAÇAS
Os feeds de dados de ameaças da Kaspersky Lab são projetados para integrar inteligência de segurança atualizada em sistemas existentes de Informações de Segurança e Gerenciamento de Eventos (SIEM), fornecendo uma camada adicional de proteção.

ANÁLISE DE MALWARE; PERÍCIA DIGITAL; RESPOSTA A INCIDENTES
Os serviços de investigação da Kaspersky Lab podem ajudar as organizações a formular suas estratégias de defesa fornecendo análise de ameaças em profundidade e aconselhando sobre as medidas necessárias para a solução do incidente.

Três níveis de investigação são oferecidos:

- Análise de malware - ajuda você a entender o comportamento e os objetivos de arquivos de malware específicos que estão visando sua organização.
- Perícia digital - fornece uma visão geral do incidente e de que forma sua organização é afetada.
- Resposta a incidentes - um ciclo completo de investigação de incidentes que inclui uma visita in loco dos especialistas da Kaspersky Lab.

RASTREAMENTO DE AMEAÇAS DE BOTNET
A solução especializada da Kaspersky Lab rastreia a atividade de botnets e fornece uma rápida notificação de ameaças (em 20 minutos) associadas a usuários de sistemas de pagamentos on-line individuais e de serviços bancários. Você pode usar essas informações para orientar e informar os seus clientes, prestadores de serviços de segurança e os órgãos que aplicam as leis sobre as ameaças atuais.

RELATÓRIOS DE INTELIGÊNCIA
Os relatórios de inteligência da Kaspersky Lab dão acesso a informações relevantes atualizadas com base em mais de 80 milhões de estatísticas de usuário coletadas de 200 países, aumentando a sua consciência e conhecimento das ameaças que a sua organização enfrenta.

O conhecimento, experiência e inteligência profunda da Kaspersky Lab a tornou a parceira confiável das agências do governo e de aplicação da lei do mundo todo. Você pode aproveitar essa inteligência em sua organização hoje.

SOLUÇÕES EMPRESARIAIS KASPERSKY

PROTEÇÃO DDOS - DEFESA E MITIGAÇÃO TOTAL

Cuida de todas as etapas necessárias para defender a sua empresa de ataques de Negação de Serviço Distribuído (DDoS).

O Kaspersky DDoS Protection fornece tudo que sua empresa precisa para se defender contra - e atenuar os efeitos de - todos os tipos de ataques DDoS. Isso inclui a análise contínua de todo o tráfego on-line, alertando-o para a possível presença de um ataque e então redireciona e limpa seu tráfego, retornando a você um tráfego "limpo".

KASPERSKY FRAUD PREVENTION - PARA BANCOS E INSTITUIÇÕES FINANCEIRAS

Uma plataforma de tecnologia abrangente, bastante personalizada e fácil de usar que trata dos riscos de fraude para transações financeiras on-line e móveis.

O Kaspersky Fraud Prevention protege os clientes de instituições financeiras, independentemente do tipo de dispositivo que eles usam para acessar estes serviços: PC, laptop, smartphone ou tablet. A plataforma também inclui um componente de software do tipo bank-side que detecta malware e automaticamente identifica padrões de comportamento anormal em transações de clientes individuais. Mesmo se o Karspersky Fraud Prevention for Endpoints não foi instalado, o Clientless Engine pode impedir transações fraudulentas.

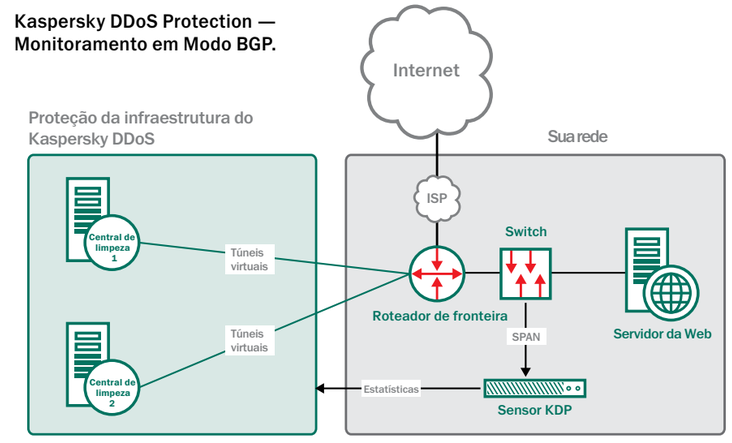
PROTEÇÃO DA INFRAESTRUTURA CRÍTICA

Protege sistemas de controle industrial e redes

O Kaspersky Endpoint Security for Business oferece proteção eficaz de "modo industrial", protegendo endpoints ICS/SCADA das ameaças e vulnerabilidades que formam o backdoor de escolha para muitos criminosos que visam os sistemas críticos.

Trabalhando com os principais fornecedores de automação industrial, tais como Emerson, Rockwell Automation e Siemens, a Kaspersky Lab criou muitos procedimentos especializados para garantir a aprovação e compatibilidade com a tecnologia operacional do cliente. Isso nos permite garantir uma proteção eficaz para infraestruturas críticas sem impactar na continuidade e consistência operacional.

Kaspersky DDoS Protection — Monitoramento em Modo BGP.



SERVIÇOS PROFISSIONAIS DA KASPERSKY LAB

Para clientes com instalações de TI complexas, os serviços do Kaspersky Professional Deployment and Upgrade, Training and Health Check são projetados para garantir que as soluções do Kaspersky Security for Business estão configuradas, implementadas e gerenciadas corretamente para oferecer um ótimo desempenho.

KASPERSKY SMALL OFFICE SECURITY

Proteção de classe mundial facilitada para as empresas pequenas.

ra seus desafios únicos: uma solução única. Poderosa proteção de classe mundial que é mais rápida e mais fácil do que nunca usar.

- Especialmente projetada para empresas com 25 usuários ou menos.
- Fácil de instalar e executar - nenhum treinamento necessário.
- Console da Web para administração com base na Internet a partir de qualquer lugar.

NÃO É NECESSÁRIO TER EXPERIÊNCIA
O Kaspersky Small Office Security é projetado até para a pessoa com menos conhecimentos técnicos ser capaz de instalar e executar com facilidade. É repleto de "assistentes" simples para guiá-lo automaticamente através de itens como:

- Configurações, incluindo a remoção de qualquer antimalware existente
- Definir os controles e escolher as políticas que funcionam melhor para você e sua empresa
- Baixar automaticamente essas alterações para vários computadores ao mesmo tempo

Tudo é administrado através de um painel com base na Web para que você, ou qualquer outra pessoa que você escolha, possa gerenciar a sua segurança de TI remotamente através da internet.

O Kaspersky Small Office Security oferece segurança excelente, mas é executado de forma tão harmoniosa e eficiente em segundo plano que você quase esquece que ele está lá.

DIVERSAS CAMADAS DE PROTEÇÃO
O Kaspersky Small Office Security aplica camada sobre camada de proteção em seus PCs e Macs, servidores, tablets e smartphones. Todas as ferramentas de segurança que sua empresa em expansão necessita, e muito mais, estão incluídas. Você pode confiar no Kaspersky Small Office Security para lidar com sua segurança de TI, deixando-o livre para gerir seus negócios.

- Proteção em tempo real assistida em nuvem contra ameaças virtuais novas e emergentes.
- Protege computadores Windows® e Mac, servidores Windows e dispositivos móveis Android ™.
- O premiado "Safe Money" protege transações financeiras on-line de hackers e ladrões de identidade on-line.
- Controles que permitem que você gerencie a navegação na Web e as redes sociais dos funcionários.
- Criptografia para proteger os dados confidenciais da empresa e dos clientes.
- Tecnologias antiphishing para proteger contra sites falsos e maliciosos.
- Poderosa filtragem de spam.
- Gerenciamento seguro de senhas.*
- Backup automático de seus dados via Dropbox para impedir a perda de dados.

AJUDA A ECONOMIZAR O SEU DINHEIRO
Além de proteger contra ataques de hackers que visam roubar seu dinheiro, o Kaspersky Small Office Security ajuda a manter seus funcionários mais produtivos, regulando o acesso à Web e configurando controles para quando eles podem navegar ou enviar mensagem. Recursos avançados de segurança, como criptografia, garantem a seus clientes que os dados deles estão seguros em suas mãos, aumentando seu potencial de vendas e a satisfação de seu cliente.

* Válido apenas para aplicativos de 32 bits. Inclui dispositivos Android e iOS.

CONTRATOS DE SUPORTE E MANUTENÇÃO DA KASPERSKY

O suporte de alta qualidade para incidentes, problemas de configuração, incompatibilidades e outras dores de cabeça de segurança de TI é fundamental para as organizações que buscam paz de espírito, bem como tempo de operação ideal.

Os Contratos de Suporte e Manutenção da Kaspersky Lab (MSAs) oferecem garantias de tempo de operação e cuidado contínuo da qualidade das redes de segurança de TI de sua organização. Esses contratos fornecem suporte superior em caso de incidentes inesperados, desde configuração imprópria a surtos de malware, contribuindo para a estabilidade e eficiência de toda a organização.

Os Contratos de suporte e manutenção da Kaspersky incluem cobertura para os seguintes problemas:

- Surtos globais de vírus inesperados
- Tempo de inatividade severo devido à infraestrutura complexa
- Otimização de implementação & correções personalizadas
- Problemas de incompatibilidade de rede
- Processo de atualização de produto da Kaspersky Lab
- Investigação de incidentes de malware
- Suporte a instalação e configuração de produto*
- Implementação de correções e outras atualizações*

Sempre que sua equipe necessitar de ajuda, especialistas da Kaspersky Lab estarão disponíveis através de linhas prioritárias exclusivas, em idiomas locais e em janelas de respostas adaptadas para atender às necessidades de sua organização. A matriz abaixo descreve as opções de suporte disponíveis.

	Suporte padrão		Suporte estendido	
	MSA Starter	MSA Plus	MSA Business	MSA Enterprise
Linha de telefone prioritária	Sim	Sim	Sim	Sim
Gerente de conta técnica	Não	Não	Sim	Sim, exclusiva
Suporte ao idioma local	8x5	8x5	8x5	24x7x365
Suporte gravidade 1	8x5	8x5	24x7x365	24x7x365
Tempo de resposta gravidade 1	8 Horas de trabalho	6 Horas de trabalho	4 Horas	30 Minutos
Suporte gravidade 2	8x5	8x5	8x5	24x7x365
Serviço profissional Consulta	Não	Não	Custos adicionais	Verificação de saúde & relatórios personalizados
Limitação de incidentes	6	12	36	Ilimitado

* Opções pagas para MSA Business. Não disponível para MSA Starter e MSA Plus.

LABORATÓRIOS KASPERSKY NO MUNDO TODO

A Kaspersky oferece suporte a empresas locais e internacionais com seus escritórios no mundo todo. Para saber mais sobre como comprar soluções Kaspersky Security for Business, entre em contato com seu revendedor local.

www.kaspersky.com

APAC

1. Austrália
2. China
3. Hong Kong
4. Índia
5. Coreia
6. Malásia

Europa

7. Áustria
8. França
9. Alemanha
10. Itália
11. Holanda
12. Portugal
13. Espanha
14. Noruega
15. Suíça
16. Reino Unido

Mercados emergentes

17. Letônia
18. Polônia
19. Romênia
20. Eslovênia
21. África do Sul
22. Turquia
23. Ucrânia
24. Emirados Árabes Unidos

Japão

25. Japão (Tóquio)

América do Norte

26. Canadá
27. Estados Unidos da América (Boston)
28. Estados Unidos da América (Miami)

Rússia e CEI

29. Rússia
30. Cazaquistão


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscou, Rússia
www.kaspersky.com

Tudo sobre segurança na Internet:
www.securelist.com

Encontre um parceiro perto de você:
www.kaspersky.com/buyoffline

Catalog_SP1/Fev15/Global