KASPERSKY SECURITY FOR BUSINESS — CATÁLOGO DE PRODUTOS

Julho - Dezembro de 2014

KASPERSKY SECURITY FOR BUSINESS

Você foi designado a fazer a diferença e fazer os negócios avançarem, mas responder a emergências de TI e a constantes soluções de problemas consome seu tempo. Além disso, as ferramentas disponíveis não ajudam você a acompanhar os desafios que enfrenta.

Você precisa de algo mais, uma solução que permita acelerar o ritmo das coisas. A plataforma de segurança da Kaspersky faz exatamente isso, ajuda você a preparar sua empresa para o futuro, com uma pequena alteração no modo como você a protege hoje.

Proteger seus computadores, os usuários móveis e a infraestrutura virtual pode ser mais fácil e mais rápido do que você achava possível, tudo a partir de um console abrangente. A tecnologia inovadora e o conhecimento de ameaças incorporados à nossa plataforma integrada ajudam você a reduzir a sobrecarga do gerenciamento, a ganhar tempo para se concentrar em outras prioridades de TI, como responder às necessidades reais de sua empresa e a melhorar o futuro de sua organização.

Você fez uma escolha inteligente, considerando a Kaspersky Lab; nós podemos ajudá-lo a fornecer a segurança mais avançada sem problemas e riscos ou altos custos. Deixe-nos ajudá-lo a contar uma nova história de sucesso. Uma história na qual você consegue manter-se à frente de ameaças, e onde VOCÊ e sua empresa estão à frente do que acontecerá em seguida, e com segurança.

A equipe da Kaspersky Lab

Saiba mais em: www.kaspersky.com.
Para obter as informações mais recentes sobre antivírus, antispyware, antispam, outros problemas e tendências de segurança de TI, visite: www.securelist.com.

SOLUÇÕES DE SEGURANÇA CORPORATIVA

Desempenho perfeito por meio de uma única plataforma.

O Kaspersky Security for Business oferece um amplo conjunto de ferramentas e tecnologias que permitem ver, controlar e proteger todos os sistemas - físicos, virtuais ou móveis.

O Kaspersky Security for Business oferece a única plataforma de segurança completa que abrange antimalware, criptografia, mobilidade, avaliação de vulnerabilidade e correções, gerenciamento de sistemas, aplicação de políticas e ferramentas de controle - gerenciada a partir de um console central, fácil de implementar e utilizar, e tudo por um custo único, permitindo que você demonstre imediatamente seu valor para os negócios.

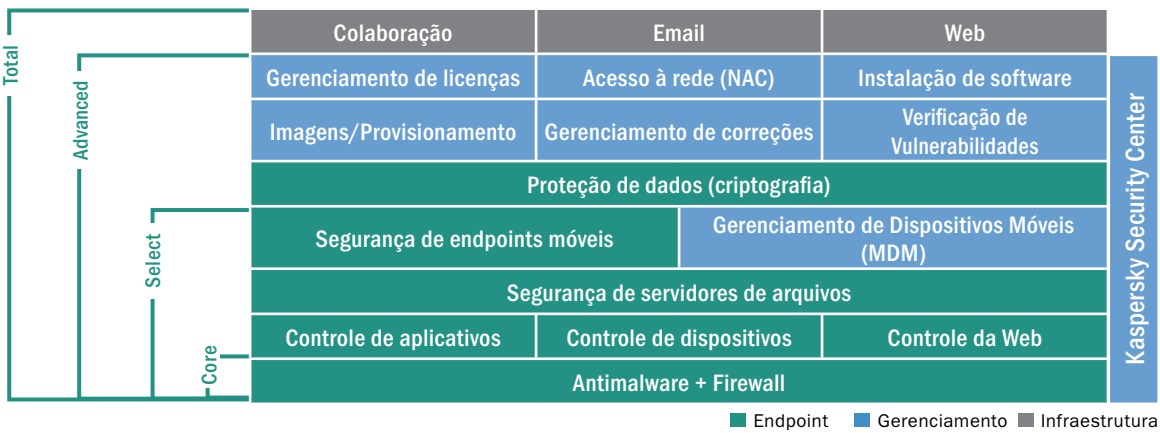
Kaspersky Endpoint Security for Business	Uma plataforma única de segurança integrada, começando com a melhor proteção antimalware do mundo, o Kaspersky Endpoint Security for Business cresce progressivamente com a incorporação de recursos, incluindo ferramentas robustas de controle de aplicativos, dispositivos e da Web, criptografia de dados, sistemas e segurança móvel e gerenciamento de correções. Tudo é gerenciado a partir um console central - o Kaspersky Security Center.	Páginas 6 a 8
Kaspersky Total Security for Business	Todos os avançados recursos de segurança e de proteção de endpoints do Kaspersky Endpoint Security acima, juntamente com segurança de email, da Web e do servidor de colaboração, protegendo seu perímetro e todo o ambiente de TI de sua empresa.	Páginas 9
Kaspersky Targeted Solutions	Soluções independentes para proteger áreas específicas de sua empresa. Algumas, como o Kaspersky Security for Mobile (páginas 12 e 13), também estão disponíveis como parte do Kaspersky Endpoint Security for Business. Outras, como o Kaspersky Security for Virtualization (páginas 20 e 21), estão disponíveis unicamente como soluções direcionadas. Todas foram desenvolvidas a partir da mesma plataforma integrada do Kaspersky Security for Business, e todas as soluções de segurança de endpoints físicos, móveis e virtuais são gerenciadas de maneira centralizada através do Kaspersky Security Center.	Páginas 11 a 21

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.

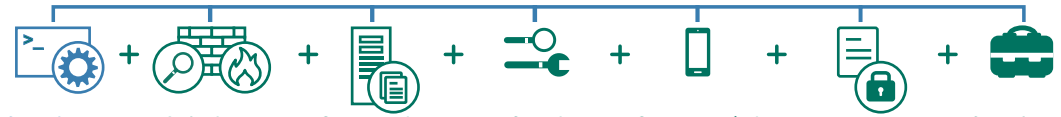


A Kaspersky apresenta uma lista completa de tecnologias - todas trabalhando em conjunto na mesma base de códigos e assistida pela Kaspersky Security Network com base na nuvem - para oferecer aos nossos clientes o nível de proteção de classe internacional de que necessitam.

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 SECURITY CENTER

Um console de gerenciamento abrangente



No centro desta abordagem unificada fica o Kaspersky Security Center, um console de gerenciamento intuitivo e totalmente escalonável que minimiza o custo total de propriedade de qualquer solução de segurança da Kaspersky Lab.

Administração de segurança simples e integrada para endpoinsts de desktop, portáteis, móveis e virtuais em uma única exibição, que inclui:

- **Implementação combinada de políticas**
- **Console da Web separado**
- **Relatórios programados e por demanda**

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – CORE

Um modelo de segurança em camadas começa com o melhor antimalware

O Kaspersky Security for Business — Core incorpora:

AVANÇADA VERIFICAÇÃO ANTIMALWARE DE ENDPOINTS

Operando em vários níveis do sistema operacional, elimina totalmente o malware usando uma combinação de tecnologias com base em assinaturas, heurísticas e assistidas na nuvem.

KASPERSKY SECURITY NETWORK: PROTEÇÃO ASSISTIDA NA NUVEM

As informações em tempo real de todo o mundo provenientes da Kaspersky Security Network fazem com que ameaças novas e desconhecidas possam ser identificadas e eliminadas à medida que surgem.

SISTEMA DE PREVENÇÃO DE INVASÕES COM BASE EM HOST (HIPS) COM FIREWALL PESSOAL

Regras predefinidas para centenas dos aplicativos mais comuns, reduzindo o tempo gasto em configuração de firewall.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT

Incluindo proteção de servidores de arquivos, controles de endpoints e segurança móvel/MDM

O gerenciamento de dispositivos móveis e as ferramentas granulares de controle de endpoints são combinados com a proteção antimalware para oferecer segurança em vários níveis, até mesmo para os dispositivos móveis dos funcionários. 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 'Negação Padrão'. O Controle de Privilégios de Aplicativos monitora e restringe os aplicativos que são executados de forma suspeita.

Controle da Web - políticas de navegação podem ser criadas com base em bancos de dados predefinidos ou personalizados de sites inapropriados, acompanhando o usuário na rede corporativa e em trânsito.

Controle de Dispositivos - permite que os administradores definam, programem e apliquem políticas de dados que controlam a conexão de dispositivos de armazenamento removível e outros periféricos a qualquer tipo de barramento.

SEGURANÇA MÓVEL

Antimalware para dispositivos móveis - tecnologias combinadas com base em assinaturas, proativas e assistidas na nuvem oferecem proteção avançada em tempo real para dispositivos móveis. O navegador seguro e o antispam melhoram ainda mais a segurança. O navegador seguro e o antispam melhoram ainda mais a segurança.

Gerenciamento de Dispositivos Móveis (MDM) - o Kaspersky Security for Mobile é compatível com os recursos fornecidos pelo Microsoft Exchange Active Sync, Apple MDM e Samsung SAFE.

Antirroubo remoto - a Verificação do Chip, o Bloqueio Remoto, a Limpeza Total ou Seletiva e a Localização impedem o acesso não autorizado a dados corporativos caso um dispositivo móvel seja perdido ou roubado.

Controles móveis - os administradores podem gerenciar e restringir o uso de aplicativos, enquanto proíbem a utilização de software indesejado ou desconhecido. Além de bloquear sites maliciosos, eles podem controlar o acesso a sites que não estiverem em conformidade com as políticas corporativas.

Conteinerização de aplicativos para BYOD - os dados e aplicativos corporativos podem ser isolados de arquivos pessoais no dispositivo do funcionário por meio da inserção de aplicativos corporativos em contêineres especiais, que podem ser criptografados e limpos separadamente dos dados pessoais do usuário.

SEGURANÇA DE SERVIDORES DE ARQUIVOS

Gerenciada em conjunto com a segurança de endpoints por meio do Kaspersky Security Center, a proteção de servidores de arquivos garante que malwares não possam se espalhar para endpoints seguros através de dados infectados armazenados.

O Kaspersky Endpoint Security - Select também inclui todos os componentes do nível Core.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED

Incluindo Criptografia e Gerenciamento de Sistemas

O Kaspersky Endpoint Security for Business — Advanced promove a eficiência e a conformidade administrativas da TI. A combinação de priorização de correções, gerenciamento de imagens do SO e resolução de problemas remota simplifica a administração diária, enquanto a infraestrutura, os usuários convidados e os inventários encontram-se sob o controle da TI. A criptografia abrangente e transparente adiciona mais uma camada de segurança, e todos os componentes são gerenciados por meio de um único console organizado - o Kaspersky Security Center.

GERENCIAMENTO DE SISTEMAS

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

Implementação do sistema operacional - fácil criação, armazenamento e implementação de imagens do SO a partir de um local centralizado, além da migração do SO.

Distribuição e resolução de problemas de software remoto - a implementação e atualização remotas a partir de um único console, automatizadas para mais de 100 aplicativos, podem ser executadas por demanda ou programadas para períodos com menos atividade. A resolução de problemas remota com economia de tempo é totalmente suportada, e um único 'agente' nas filiais pode aceitar atualizações para distribuição local usando a tecnologia Multicast.

Controle de Acesso à Rede (NAC) - reconhece e verifica automaticamente novos dispositivos na rede com relação a inventários e a políticas de segurança de TI, nega acesso a dispositivos comprometidos e redireciona dispositivos convidados a um portal cativo.

Inventários de hardware e software - total visibilidade e controle (incluindo bloqueio) de todos os softwares implementados na rede, juntamente com a identificação, o registro e o rastreamento automáticos de todos os itens de hardware, incluindo dispositivos removíveis.

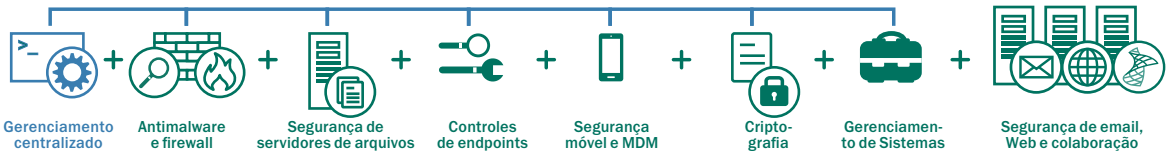
CRIPTOGRAFIA

Pasta/arquivo abrangente e disco completo - escolha proteção de disco completo ou de arquivo que seja transparente para o usuário e suportada pela criptografia AES (Advanced Encryption Standard) de 256 bits para proteger informações corporativas importantes em caso de roubo ou perda acidental de dispositivos. Inclui suporte de criptografia para dispositivos removíveis.

Compartilhamento seguro de dados - permite que os usuários criem facilmente pacotes criptografados e com extração automática para assegurar que os dados estejam protegidos quando compartilhados através de dispositivos removíveis, email, da rede ou da Web.

O Kaspersky Endpoint Security for Business - Advanced também inclui todos os componentes dos níveis Select e Core.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Incluindo segurança periférica para servidores e gateways

O Kaspersky Total Security for Business apresenta a mais completa plataforma de proteção e gerenciamento oferecida atualmente no setor. O 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 EMAIL

Impede de maneira eficaz ameaças de malware, ataques de phishing e spams com base em emails 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.

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, enquanto os recursos de filtragem de conteúdos e de arquivos ajudam a evitar o armazenamento de conteúdo inadequado.

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		●	●	●	●	●
Criptografia			●	●	●	
Gerenciamento de imagens do SO			●	●	●	●
Gerenciamento de licenças			●	●	●	●
Gerenciamento de vulnerabilidades			●	●	●	●
Gerenciamento de correções			●	●	●	●
Controle de acesso à rede			●	●	●	●
Segurança de servidores de colaboração				●		●
Segurança para servidores de email				●	●	●
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 dos sistemas.

DESTAQUES

PROTEÇÃO ANTIMALWARE AVANÇADA
O mecanismo antimalware premiado da Kaspersky proporciona proteção avançada 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.

GERENCIABILIDADE E SISTEMA DE RELATÓRIOS SOFISTICADOS
Ferramentas de gerenciamento eficientes e amigáveis, informações sobre o status de proteção dos servidores, configurações de tempo flexíveis para as verificações e um extenso sistema de relatórios fornecem controle eficiente da segurança de servidores de arquivos, 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 escolha dos métodos de instalação e gerenciamento.
- **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.**

KASPERSKY SECURITY FOR MOBILE

Gerenciamento, segurança e controle centralizados para endpoints móveis corporativos e BYOD

O Kaspersky Security for Mobile torna o gerenciamento seguro e centralizado de dispositivos móveis simples e direto, ao mesmo tempo que oferece proteção precisa contra ameaças atuais e futuras.

DESTAQUES

EXCELENTE PROTEÇÃO PARA DISPOSITIVOS MÓVEIS E OS DADOS QUE ELES ARMAZENAM
Os recursos avançados de segurança móvel incluem tecnologias antimalware e antiphishing. Os controles de aplicativos e navegação na Web fornecem níveis aprofundados de proteção abrangente para dados corporativos no seu próprio dispositivo móvel e nos de seus funcionários.

CONTROLE E PROTEJA SEUS DADOS
Para as iniciativas BYOD, os dados corporativos podem ser isolados em "contêineres" criptografados separados no dispositivo do funcionário e, se necessário, apagados remotamente e de forma independente, mantendo assim seus dados seguros e respeitando a privacidade do funcionário.

GERENCIAMENTO DE DISPOSITIVOS MÓVEIS SIMPLIFICADO
O gerenciamento unificado e centralizado com integração com iOS e Samsung MDM, além do suporte ao Microsoft ActiveSync, agilizam e simplificam o gerenciamento remoto e o controle por conexão sem fio (OTA) de dispositivos móveis em todas as principais plataformas móveis, mantendo o custo administrativo baixo.

GERENCIAMENTO CENTRALIZADO A PARTIR DE UMA ÚNICA TELA
O gerenciamento centralizado se estende além de dispositivos móveis de várias plataformas a todos os aspectos de sua infraestrutura. Com o Kaspersky Security Center, você pode gerenciar a segurança de todos os endpoints - dispositivos móveis corporativos e de funcionários, estações de trabalho, computadores portáteis e até mesmo a infraestrutura virtual - organicamente por meio de um único console.

RECURSOS DE SEGURANÇA

- **Antimalware para dispositivos móveis.** O mecanismo antimalware da Kaspersky Lab apresenta uma combinação de tecnologias de detecção com base em assinaturas e heurísticas, juntamente com a proteção contra ameaças novas e desconhecidas, por meio de contínuas atualizações da Kaspersky Security Network (KSN), o banco de dados global e em tempo real assistido na nuvem da Kaspersky Lab. Um navegador seguro e a avançada tecnologia antiphishing também ajudam a garantir que o dispositivo e os dados que ele contém não sejam comprometidos por softwares nocivos.
- **Antirroubo.** Se um dispositivo for perdido ou roubado, o Bloqueio Remoto poderá ser acionado. Os administradores podem executar remotamente uma Limpeza Total ou Seletiva do dispositivo, identificar a localização de um dispositivo ausente usando a função de "Localização" por GPS, receber uma notificação automática se o chip for removido ou trocado.
- **Controle de aplicativos.** Os aplicativos instalados em cada dispositivo móvel podem ser monitorados e controlados remotamente segundo as políticas de grupo predefinidas. Os usuários podem ser limitados para instalar somente aplicativos aprovados ou podem ser proibidos de instalar aqueles considerados possivelmente perigosos ou inadequados. Também é possível ativar a exigência de um novo login após determinado período de inatividade.
- **Controles da Web.** O Controle da Web e a Navegação Segura na Web são suportados pela Kaspersky Security Network, trabalhando em tempo real para identificar sites infectados por malware ou que contenham malware. Além de bloquear sites suspeitos, os administradores podem controlar o acesso a determinados tipos de sites que não estejam em conformidade com as políticas corporativas - por exemplo, redes sociais, sites de jogos, com conteúdo para adultos, servidores proxy ou lojas virtuais.
- **Detecção de jailbreak/rooting.** Se um jailbreak é detectado, o administrador é notificado automaticamente, o acesso a aplicativos corporativos é bloqueado e o dispositivo pode ser apagado de forma seletiva ou total.
- **Integridade de dados corporativos e pessoais: contêineres.** Para apoiar um cenário em que o dispositivo pertence ao funcionário, os dados corporativos podem ser colocados em “contêineres” isolados. Isso proporciona segurança máxima para os dados corporativos e excelente integridade para o conteúdo pessoal.
- **Proteção de dados corporativos no contêiner.** Funcionalidades adicionais de segurança, como a criptografia de dados ou um nível superior de autorização, podem ser aplicadas a esses contêineres. Quando um funcionário sai da organização, os contêineres podem ser apagados remotamente, deixando os arquivos pessoais inalterados.

RECURSOS DE GERENCIAMENTO

- **Gerenciamento de dispositivos móveis.** O Kaspersky Security for Mobile é compatível com a funcionalidade fornecida pelo Microsoft Exchange Active Sync, pelo Apple MDM e o Samsung SAFE. Os administradores podem aplicar as definições de PIN, definir a complexidade das senhas, controlar recursos de criptografia, impedir o uso da câmara e gerenciar remotamente os recursos relacionados a uma grande variedade de smartphones e tablets em um único painel.
- **Provisionamento por conexão sem fio (OTA)** Smartphones e tablets podem ser habilitados na rede corporativa por conexão sem fio (OTA), usando um link ou código QR enviado ao funcionário via email ou SMS. A solução pode ser instalada automaticamente pelo usuário, evitando qualquer falha na segurança de TI.
- **Gerenciamento de várias plataformas em um único console.** Não são necessários consoles individuais para cada componente do MDM, pois o gerenciamento de dispositivos móveis em todas as plataformas é feito em um console único, o Kaspersky Security Center. Além dos dispositivos móveis, a segurança de endpoints físicos e de sistemas virtuais, incluindo a criptografia e a aplicação de políticas, também pode ser gerenciada em conjunto e de forma remota no mesmo console único.

GERENCIAMENTO DE SISTEMAS KASPERSKY

Eficiência e segurança de TI aprimoradas

Introdução ao Gerenciamento de Sistemas Kaspersky. Esta solução oferece um amplo conjunto de avançadas ferramentas de produtividade de TI para ambientes Windows, programadas no mesmo código e gerenciadas a partir de um único console. A plataforma resultante oferece a simplicidade e a automação que você deseja - e a segurança e o controle de que você precisa.

DESTAQUES

SEGURANÇA APRIMORADA
A descoberta automática e oportuna, a priorização de vulnerabilidades em sistemas operacionais e no software e a distribuição rápida e automatizada de correções e atualizações necessárias são combinadas para melhorar sua conduta de segurança e ao mesmo tempo reduzir a sobrecarga administrativa.

TRABALHO COM EFICIÊNCIA
Os administradores podem distribuir e instalar atualizações, correções e aplicativos remotamente. A resolução remota de problemas permite que o administrador não perca tempo indo de mesa em mesa ou ao telefone. A implementação centralizada e automatizada do sistema operacional também ajuda a reduzir a carga de trabalho, eliminando a duplicação do trabalho necessário para configurar usuários individuais.

CONTROLE COM TOTAL VISIBILIDADE
Com total visibilidade da rede em um único console, os administradores têm ciência de todos os dispositivos e aplicativos que entram na rede, incluindo os dispositivos convidados. Essa visibilidade possibilita o suporte ao controle centralizado de usuários e do acesso de dispositivos a dados corporativos e aplicativos de software de acordo com as políticas da TI.

GERENCIAMENTO CENTRALIZADO
Esses e outros recursos fazem parte do Gerenciamento de Sistemas Kaspersky e são todos acessados em conjunto pelo console de administração do Kaspersky Security Center. Como cada ferramenta não requer seu próprio console independente, os comandos são consistentes e intuitivos e não é necessário treinamento adicional.

COMPONENTES

PROVISIONAMENTO DE SISTEMAS OPERACIONAIS E APLICATIVOS

Fácil criação, armazenamento, clonagem e implementação de imagens do sistema em um local centralizado. Garante que os sistemas sejam entregues ao usuário sem problemas e com as melhores configurações de segurança, inclusive em implementações após o expediente, via Wake-On-LAN. Essa ferramenta é adequada para a migração de sistemas operacionais.

VERIFICAÇÃO DE VULNERABILIDADES E GERENCIAMENTO DE CORREÇÕES

A verificação de hardware e software com um clique compara os resultados com vários bancos de dados de vulnerabilidades, priorizando automaticamente as vulnerabilidades e definindo quais precisam de atenção imediata e quais podem ser adiadas para depois do expediente. As correções e atualizações podem, então, ser implementadas automaticamente, seja por demanda ou no modo programado.

CONTROLE E PROVISIONAMENTO DE LICENÇAS

A visibilidade do número de usuários de um aplicativo em um determinado momento ajuda a identificar onde os custos de licenciamento podem ser aprimorados e onde os usuários estão fora de conformidade.

DISTRIBUIÇÃO DE SOFTWARE

O software pode ser implementado e atualizado remotamente a partir de um único console. Mais de 100 aplicativos mais populares, conforme identificados pela Kaspersky Security Network, podem ser instalados e atualizados automaticamente, depois do expediente, se necessário, simplificando ainda mais o processo de distribuição. Há suporte total à resolução remota de problemas no mesmo console para qualquer sistema cliente e, usando a tecnologia Multicast, as estações de trabalho da filial podem ser atribuídas como "agentes" centrais para a distribuição local de atualizações. Como resultado, as distribuições de software são mais rápidas e utilizam menos largura de banda.

INVENTÁRIOS DE HARDWARE E SOFTWARE

Os computadores, discos rígidos e até mesmo dispositivos removíveis são detectados e incluídos no inventário automaticamente. A introdução de um novo dispositivo gera uma notificação que é enviada ao administrador, que pode acompanhar o status e o uso do hardware na rede. Da mesma forma, o inventário de software rastreia exatamente quais softwares estão em uso a qualquer momento e pode ser implementado em conjunto com as ferramentas de controle de endpoints da Kaspersky Lab para bloquear ou limitar o uso de aplicativos de software específicos.

CONTROLE DE ACESSO À REDE (NAC)

O NAC torna o controle de acesso de convidado mais fácil e simples. Os novos dispositivos na rede são reconhecidos e verificados automaticamente pelo inventário de hardware e das políticas de segurança de TI. O acesso à rede pode ser negado aos dispositivos comprometidos, enquanto que os dispositivos convidados podem ser redirecionados para um portal cativo e obter acesso à Internet.

GERENCIAMENTO CENTRALIZADO

As ferramentas de Gerenciamento de Sistemas Kaspersky fazem parte de uma única plataforma de segurança integrada, oferecendo recursos abrangentes de gerenciamento e segurança de TI através de um console de administração central, o Kaspersky Security Center. O Kaspersky Security Center oferece suporte à administração de endpoints de desktop, móveis e virtuais em toda a rede corporativa em uma exibição única, eliminando a complexidade e reforçando sua conduta de segurança.

KASPERSKY SECURITY FOR MAIL SERVER

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

DESTAQUES

PROTEÇÃO CONTRA AMEAÇAS DE MALWARE

A avançada proteção contra malware é fornecida pelo mecanismo antimalware premiado da Kaspersky Lab, com suporte em tempo real pela Kaspersky Security Network assistida na nuvem, e com proteção proativa contra exploits e filtragem de URLs maliciosos.

PROTEÇÃO ANTISPAM

Para servidores de email Microsoft Exchange e com base em Linux, o mecanismo antispam assistido na nuvem da Kaspersky Lab ajuda a eliminar até 99,92% dos spams que consomem tempo e recursos, com uma taxa de 0% a 0,05% de falsos positivos.

OTIMIZAÇÃO DE RECURSOS DO SISTEMA

O balanceamento de carga, a tecnologia de verificação otimizada e as exclusões confiáveis ajudam a reduzir os recursos necessários para executar verificações de malware, ao mesmo tempo em que a filtragem de spam inteligente reduz de forma significativa carga de tráfego.

ADMINISTRAÇÃO SIMPLES E FLEXÍVEL

As ferramentas amigáveis de gerenciamento e geração de relatórios, as informações sobre o status de proteção de emails e as configurações de verificação flexíveis proporcionam um controle eficiente da segurança de emails e de documentos, ajudando a reduzir o custo total de propriedade.

RECURSOS

- **Proteção antimalware em tempo real** suportada pela Kaspersky Security Network assistida na nuvem.
- **Proteção avançada** contra a exploração de vulnerabilidades desconhecidas e até mesmo de hora zero com o ZETA Shield.
- **Proteção eficaz contra spam.**
- **Verificação assistida na nuvem** de todas as mensagens de spam do servidor Microsoft® Exchange, incluindo pastas públicas, utilizando a Kaspersky Security Network.
- **Verificação programada de emails e bancos de dados** 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 de rede.

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 Lab 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 otimizados e inteligentes reduzem a carga dos recursos, ajudando a preservar a valiosa 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 email 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 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 email (via protocolos POP3 e SMTP).
- Armazenamento de backup (apenas TMG).

KASPERSKY SECURITY FOR COLLABORATION

O Kaspersky Security for Collaboration oferece uma plataforma de proteção premium em tempo real, ao mesmo tempo em que ajuda a reforçar a comunicação interna e suas políticas de armazenamento, para que seus usuários possam colaborar com confiança.

DESTAQUES

PROTEÇÃO ANTIMALWARE PREMIUM

Equipado com o premiado e mais recente mecanismo antimalware da Kaspersky Lab, o Kaspersky Security for Collaboration detecta e elimina ameaças de malware. A avançada proteção em tempo real contra malwares novos e desconhecidos é fornecida através da Kaspersky Security Network com base na nuvem, enquanto que a tecnologia antiphishing protege os dados colaborativos contra ameaças com base na Web.

PLATAFORMA DE SEGURANÇA COMPLETA

Se você utiliza o Microsoft SharePoint Server, deve saber que as soluções de proteção de endpoints são incompatíveis, pois todo o conteúdo é armazenado em um banco de dados SQL. O Kaspersky Security for Collaboration foi criado com isto em mente, a fim de proteger todo o farm do SharePoint e todos os seus usuários.

CONTROLE DE CONTEÚDO E ARMAZENAMENTO

Os recursos de filtragem de conteúdo e de arquivos 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.

ADMINISTRAÇÃO SIMPLES

A segurança de todo o farm de servidores pode ser administrada centralmente a partir de um único painel integrado. A administração é rápida e simples, sem a necessidade de treinamento específico.

RECURSOS

- **Avançada proteção antimalware**. A verificação de segurança em segundo plano e por acesso incorpora informações em tempo real sobre ameaças novas e emergentes.
- **Antiphishing.** O conteúdo da Web é verificado em busca de links de phishing para proteger os dados do usuário contra roubos.
- **Filtragem de arquivos.** Analisa os formatos de arquivo reais, independentemente do nome da extensão, impedindo que os usuários armazenem tipos de arquivos específicos (por exemplo, arquivos de música, de vídeo e arquivos executáveis).
- **Filtragem de conteúdo.** Análises com base em palavras-chave (predefinidas ou personalizadas) impedem o armazenamento de arquivos que incluem conteúdos inadequados.
- **Backup e armazenamento** de dados anteriores à desinfecção ou exclusão.
- **Integração com o Active Directory.** Configuração e autenticação simplificadas de usuários.
- **Gerenciamento centralizado.** É possível definir configurações globais de gerenciamento para todos os servidores protegidos em um único painel.
- **Administração simples.** Um painel de fácil compreensão apresenta os cenários mais utilizados.

KASPERSKY SECURITY FOR STORAGE

O Kaspersky Security for Storage proporciona proteção escalonável, robusta e de alto desempenho para dados corporativos sigilosos e valiosos armazenados em sistemas de armazenamento EMC™ VNX™ e NetApp.

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 até mesmo 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 excepcional a falhas 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 do Kaspersky Security Center, junto com as outras soluções de segurança da Kaspersky.

RECURSOS

- **Segurança proativa.** Para sistemas de armazenamento EMC e NetApp contra ameaças novas e potenciais.
- **Atualizações automáticas**. Verificação sem interrupções.
- **Processos e zonas confiáveis isentos.** "Zonas confiáveis", formatos de arquivos definidos e processos especificados podem ser excluídos da verificação.
- **Verificação de objetos com execução automática.** Para evitar que malwares sejam inicializados durante a reinicialização do sistema.
- **Verificação flexível para um desempenho otimizado.** O administrador pode especificar e controlar a profundidade, a amplitude e a duração da atividade de verificação, definindo quais são os tipos de arquivos e as áreas que devem ser verificados. Inclui iSwift e iChecker.
- **Protege soluções HSM e DAS**. Oferece suporte aos modos de verificação offline para tecnologias HSM (Gerenciamento de Armazenamento Hierárquico) e DAS (Direct Attached Storage).
- **Proteção de sistemas virtuais e servidores de terminal.** Protege sistemas operacionais virtuais (convidados) em ambientes Hyper-V e VMware, e infraestruturas de terminais Microsoft e Citrix.
- **Instalação e gerenciamento centralizados.** Gerenciado através do intuitivo Kaspersky Security Center. O gerenciamento por linha de comando também está disponível, se preferido.
- **Controle sobre privilégios de administrador.** Diferentes níveis de privilégios podem ser atribuídos a cada administrador do servidor.
- **Relatórios flexíveis.** São fornecidos por meio de relatórios gráficos ou revisão 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.

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 VMs (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

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, emails e Web, além de heurística avançada. O resultado é uma segurança sólida e em vários níveis combinada com um desempenho eficiente.

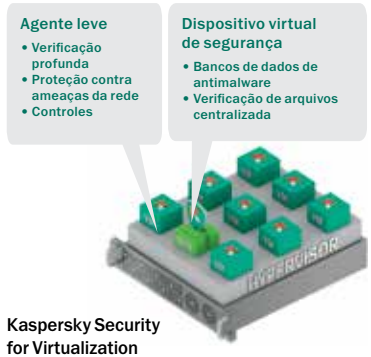
CONFIGURAÇÃO OPCIONAL SEM AGENTES PARA AMBIENTES VMWARE

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.

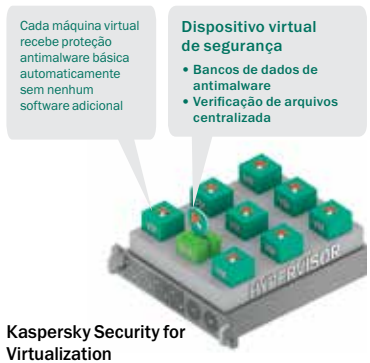
LICENCIAMENTO FLEXÍVEL

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.



Kaspersky Security for Virtualization
Configuração com agentes leves



Kaspersky Security for Virtualization
Configuração sem agentes**

VÁRIAS PLATAFORMAS: UM ÚNICO CUSTO

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

PRINCIPAIS RECURSOS DO PRODUTO

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

* 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 deveimplementar o agente leve manualmente durante a instalação.

LOCALIZAÇÕES DA KASPERSKY LAB

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


Cazaquistão
Federação Russa
Ucrânia
China
Hong Kong
Índia
Japão
Malásia
Coreia do Sul
Israel
Turquia
EAU
África do Sul
Austrália

Kaspersky Lab ZAO, Moscou, Rússia
www.kaspersky.com

Tudo sobre segurança na Internet:
www.securelist.com

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

KASPERSKY lab