Kaspersky® Web Traffic Security

Defesa estratégica para toda a sua rede

O servidor proxy é um gargalo natural para o tráfego da Web que passa entre a infraestrutura corporativa e o mundo externo. Esse posicionamento estratégico proporciona uma ótima oportunidade para conter ameaças precocemente e com esforço relativamente pequeno.

O aplicativo Kaspersky Web Traffic Security integra-se com os servidores proxy para proteger a rede corporativa de TI dos perigos da Web e aumentar a produtividade por meio do controle de uso da Internet. Ele processa o tráfego da Web que passa por ele e bloqueia qualquer item perigoso de acordo com as políticas corporativas de segurança. Embora o método em si seja um padrão de segurança do perímetro, a variedade de recursos e a qualidade inigualável da proteção contra ameaças diferenciam o Kaspersky Web Traffic Security das outras ofertas do mercado.

Destaques

- Proteção antimalware e antiphishing da próxima geração sob demanda e em tempo real
- Filtragem de conteúdo para bloquear tipos de arquivos perigosos e evitar o vazamento de dados
- Escalonável para suprir redes com grande volume de carga
- Disponível com licenças de assinatura mensal para usuários finais e MSPs
- Proteção contra ameaças de hora zero
- Suporte da inteligência global de ameaças da Kaspersky Security Network
- Compatível com o Microsoft Active Directory
- Acesso baseado em funções para administração e uso da Web
- Controle da Web para regulamentar o uso de recursos da Web
- Bloqueia ransomware antes que ele entre na rede
- Multilocação para MSPs e empresas diversificadas

Os benefícios

Reduz significativamente o risco de infecção, evitando a interrupção dos negócios.

Ao bloquear a maioria das ameaças que chegam no nível do gateway e impedir que elas atinjam seus endpoints, o Kaspersky Web Traffic Security reduz significativamente seu impacto potencial sobre os usuários finais e suas estações de trabalho.

Impulsiona a eficiência da proteção do gateway corporativo

Com uma das mais eficientes pilhas de tecnologias de proteção do setor, taxas de detecção superiores e um índice de falsos positivos próximo de zero, o aplicativo Kaspersky Web Traffic Security é um complemento ideal para as contramedidas existentes em seu gateway da Web, proporcionando um aumento notável da proteção. Isso é especialmente importante em empresas e instituições que operam dados sigilosos e/ou com baixa tolerância a incidentes de segurança.

Reduz a sobrecarga sobre as equipes de TI e de segurança de TI

Mesmo que a proteção de endpoints seja adequada, quando há menos alarmes em nível de endpoint, você tem menos usuários em pânico e menos tempo é gasto na investigação de incidentes.

Melhora a produtividade

Com o controle do uso de recursos da Internet, o Kaspersky Web Traffic Security reduz o risco de ataques cibernéticos e, ao mesmo tempo, também evita distrações, com menos chances de uso da TI paralela, especialmente quando há endpoints não Windows.

Adapta-se ao tamanho da sua empresa

A solução pode ser escalonada de acordo com a carga específica do sistema, permitindo o gerenciamento de vários nós e sua implementação hierárquica.

Requisitos de hardware dos servidores usados para instalar o Kaspersky Web Traffic Security

Servidor de trabalho:

- CPU: Intel Xeon E5606 (4 núcleos) de 1,86 GHz ou mais;
- 8 GB de RAM;
- Partição de troca de pelo menos 4 GB;
- 100 GB de espaço no disco rígido, incluindo:
- 25 GB para armazenamento de arquivos temporários;
- 25 GB para armazenamento de arquivos de log.

Servidor mestre:

- CPU: Intel Xeon E5606 (4 núcleos) de 1,86 GHz ou mais;
- 8 GB de RAM;
- Partição de troca de pelo menos 4 GB;
- 100 GB de espaço no disco rígido.

Se você instalar o servidor mestre e um servidor secundário no mesmo servidor físico:

- CPU: 2 Intel Xeon E5606 (8 núcleos) de 1,86 GHz ou mais;
- 16 GB de RAM;
- Partição de troca de pelo menos 4 GB;
- 200 GB de espaço no disco rígido, incluindo:
- 25 GB para armazenamento de arquivos temporários;
- 25 GB para armazenamento de arquivos de log.

Requisitos de software dos servidores usados para instalar o Kaspersky Web Traffic Security

- Red Hat Enterprise Linux versão 7.5 x64.
- Ubuntu 18.04.1 LTS.
- Debian 9.5.
- SUSE Linux Enterprise Server 12 SP3.
- CentOS versão 7.5 x64.

Requisitos adicionais

- Ngnix versões 1.10.3, 1.12.2 e 1.14.0.
- Balanceamento de carga HAProxy versão 1.5.
- Squid 3.5.20, se você instalar o serviço Squid no servidor secundário.

Para que o Kaspersky Web Traffic Security processe o tráfego da sua rede, você deve instalar e configurar um servidor proxy HTTP(S) que ofereça suporte aos serviços ICAP, Request Modification (REQMOD) e Response Modification (RESPMOD). Você pode usar um servidor proxy separado ou, por exemplo, instalar o serviço Squid em um servidor secundário do Kaspersky Web Traffic Security.

Requisitos de software para gerenciar o Kaspersky Web Traffic Security por meio de interface Web

Para executar a interface Web, é necessário ter um destes navegadores instalado no computador:

- Mozilla Firefox versão 39.
- Internet Explorer versão 11.
- Google Chrome versão 43.
- Microsoft Edge versão 40.

Reduz os riscos associados com a transmissão de determinados tipos de arquivos nas duas direções

O Kaspersky Web Traffic Security ajuda a reforçar a segurança restringindo a transmissão de determinados tipos de arquivos. Isso evita infecções que usam conteúdo malicioso incorporado em documentos e também reduz o risco de vazamento de dados. A eliminação do acesso a arquivos de mídia por usuários que não precisam disso para trabalhar também aumenta a produtividade.

Proporciona mais conveniência para provedores de serviços gerenciados (MSPs)

Conforme mais MSPs incluem a cibersegurança em sua proposta de valor, o Kaspersky Web Traffic Security proporciona funcionalidades de gerenciamento multilocatário e licenciamento flexível, e possibilita que o nível de controle adequado seja atribuído a cada administrador dos locatários.

Recursos

Proteção multicamadas contra ameaças alimentada pelo HuMachine™

A proteção contra malware da próxima geração da Kaspersky incorpora várias camadas de segurança proativa, que incluem algoritmos de Machine Learning e mecanismos eficientes baseados na nuvem. Ela elimina malware, ransomware e programas possivelmente indesejados do tráfego de entrada e de saída.

Inteligência global de ameaças: o Kaspersky Web Traffic Security usa dados obtidos globalmente para ter a visão mais atualizada do cenário de ameaças, mesmo durante sua evolução.

Machine Learning: o Big Data de inteligência de ameaças global é processado pela capacidade combinada dos algoritmos de Machine Learning e do conhecimento humano, proporcionando altos níveis de detecção comprovados com o mínimo de falsos positivos.

Sandbox de simulação

Para proporcionar proteção contra os malwares mais sofisticados, fortemente obscurecidos, os anexos são executados em um ambiente simulado seguro, onde são analisados para garantir que amostras perigosas não fiquem no sistema corporativo.

Detecção de scripts

Segundo os analistas de cibersegurança, os scripts estão cada vez mais sendo usados em ataques baseados na Web e para incorporar malware em arquivos do Office aparentemente inofensivos. O Kaspersky Web Traffic Security cuida desses dois casos, evitando ataques de execução e também a execução de malwares fatais mesmo antes que eles alcancem o endpoint solicitado.

Banco de dados de hosts relacionados com ataques cibernéticos

Para evitar até o menor risco de interação com recursos perigosos, o serviço baseado em nuvem verifica o recurso solicitado usando um amplo banco de dados de servidores de comando e controle de invasores cibernéticos ativos, objetos com exploits de “dia zero”, sites da Web perigosos e pontos de distribuição de malware identificados com propósitos de violação. Esse banco de dados é atualizado em tempo real com a inteligência da renomada GReAT Team da Kaspersky Lab, bloqueando até os recursos perigosos mais novos e emergentes antes que sua solicitação seja executada.

Filtragem baseada em reputação

O Kaspersky Web Traffic Security solicita reputações de arquivos e endereços dos bancos de dados em nuvem continuamente renovados da Kaspersky Security Network. Assim, recursos da Internet e arquivos suspeitos e indesejados podem ser bloqueados instantaneamente sem a necessidade de uma análise mais aprofundada.

A metodologia Kaspersky HuMachine™

Alimentado pela inteligência de ameaças de Big Data, funcionalidades de Machine Learning robótico e o conhecimento humano de especialistas, o Kaspersky HuMachine™ oferece diversos benefícios e proporciona uma proteção mais eficiente. Por meio da combinação de cada elemento, os componentes individuais são aprimorados em um todo ainda mais eficiente e eficaz.

Antiphishing avançado

O avançado sistema antiphishing da Kaspersky é baseado em análise de redes neurais, produzindo modelos de detecção eficientes. Com a utilização de mais de 1000 critérios, que incluem imagens, verificações de linguagem, scripts específicos, essa abordagem assistida em nuvem conta com o suporte de dados obtidos globalmente sobre URLs maliciosos e de phishing para oferecer proteção contra URLs de phishing conhecidos e desconhecidos/de hora zero contidos em arquivos baixados.

Filtragem de conteúdo

É possível proibir a transmissão de alguns tipos de arquivos; a filtragem é baseada em vários parâmetros, como nome, extensão/tipo (o reconhecedor de formatos é usado para arquivos com extensões falsas), tamanho, tipo MIME e hash. Isso tem vários objetivos, inclusive reduzir o risco de um ataque cibernético, evitar vazamentos de dados, diminuir o tráfego e melhorar a produtividade.

Controle da Web com as categorias da Kaspersky Lab

Nem todos os recursos da Web são necessários para as atividades de trabalho de todos os funcionários, e muitos podem representar um perigo considerável à segurança e à reputação corporativa, caso hospedem malware ou ofereçam produtos pirateados. O Controle da Web restringe determinadas categorias de recursos da Web para reduzir os riscos envolvidos e garante o trabalho ininterrupto sem distrações indesejadas. Se necessário, é possível implementar um cenário de Negação Padrão, limitando o uso de qualquer recurso da Web além dos que são absolutamente necessários para o trabalho do usuário ou daquele grupo específico.

Monitoramento seguro do tráfego SSL criptografado

A arquitetura da solução permite a fácil implementação do monitoramento do tráfego corporativo (também chamado de 'SSL bumping'). Conforme o tráfego da Web com criptografia SSL se torna de fato o padrão de comunicação da Internet, esse recurso torna-se obrigatório.

Segurança para sistemas compatíveis com ICAP

Além dos servidores proxy, a solução da Kaspersky Lab protege o tráfego em todos os outros dispositivos compatíveis com o protocolo ICAP. Eles podem incluir, por exemplo, armazenamentos conectados à rede (NAS, Network Attached Storage) ou outros sistemas que não podem ser protegidos por uma solução de segurança interna.

Integração com SIEMs

Se a sua empresa utiliza um sistema de gerenciamento de informações e eventos de segurança (SIEM, Security Information and Event Management) para controlar as atividades em toda a rede corporativa, o Kaspersky Web Traffic Security reforçará seu contexto de segurança por meio da exportação de informações em formato CEF (Common Event Format), além do syslog, amplamente usado.

Gerenciamento conveniente

O Kaspersky Web Traffic Security oferece um sistema de gerenciamento flexível e fácil de usar.

Console centralizado: controle a segurança de todos os seus sistemas compatíveis com ICAP, incluindo proxies e armazenamentos, em uma interface Web única que oferece excelente visibilidade e capacidade de gerenciamento para os administradores de segurança.

Painel conveniente: todos os elementos necessários para avaliar o estado atual da segurança corporativa em nível de gateway são reunidos em um único painel. Assim, você tem uma visão geral imediata e completa da situação, incluindo eventos urgentes.

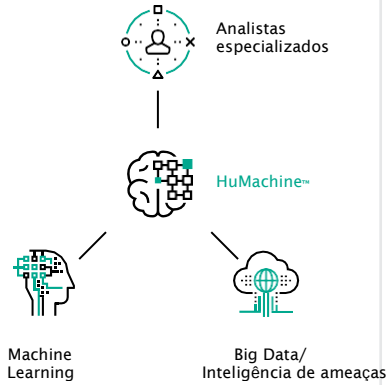
Gerenciamento de eventos: os resultados da análise de ameaças são apresentados usando uma abordagem centrada nos eventos e mostram atividades em tempo real. O comportamento dos usuários na Internet também pode ser analisado.

Sistema de configuração com regras flexíveis: além da eficácia das camadas de segurança da solução, as políticas de segurança ajustadas com precisão são um dos pilares da eficácia da solução, configuradas para serem consistentes com os processos de negócios existentes. O Kaspersky Web Traffic Security fornece um sistema de configuração de regras flexível e fácil de usar, que permite o gerenciamento granular da segurança do gateway e, ao mesmo tempo, garante que os administradores não precisem de muito tempo para aprender a usá-lo.

Sistema de acesso baseado em funções: os administradores podem definir uma função para restringir os direitos de administração de diferentes categorias de administradores. Isso é útil para a atribuição de tarefas internas ou para proporcionar o nível necessário de controle para os clientes atendidos, no caso de um MSP.

Integração com o Active Directory: o Kaspersky Web Traffic Security é capaz de obter informações de entidades do domínio corporativo (usuários, grupos de usuários, computadores, etc.) para configurar as políticas de segurança e as regras de acesso baseadas em funções em relação a objetos conhecidos que operam na rede de TI da empresa. Os dados que descrevem os objetos são sincronizados continuamente entre o Active Directory e o aplicativo para garantir a consistência com as alterações mais recentes na infraestrutura corporativa.

Multilocação: um modo especial para MSPs e empresa diversificadas permite atribuir áreas dedicadas (‘espaços de trabalho’) para as diversas unidades ou empresas gerenciadas, sendo possível gerenciá-las separadamente, associando políticas ‘globais’ e ‘locais’ conforme apropriado.



Como comprar
O aplicativo Kaspersky Web Traffic Security pode ser ativado por meio de vários produtos da Kaspersky Lab, dependendo da licença que você adquiriu.
- Kaspersky Security for Internet Gateway
- Kaspersky Security for Storage
- Kaspersky Security for xSP
- Kaspersky Total Security for Business

www.kaspersky.com