kaspersky BRING ON THE FUTURE

Kaspersky Security for Mail Server

Criar resiliência contra o principal vetor de ataque

O e-mail é o principal vetor de malware que ameaça a segurança de TI das empresas. Os atacantes possuem formas cada vez mais sofisticadas de infiltrar organizações através de ataques por e-mail, resultando em perdas financeiras, operacionais e de reputação. Para fazer frente a esta tendência, as empresas devem pensar na resiliência bem como na proteção. Ao otimizar a sua resiliência e minimizar a sua superfície de ataque, você pode tornar a sua empresa menos atraente e, até mesmo, um alvo inviável para criminosos – independente dela operar localmente, na nuvem ou em uma infraestrutura de email híbrida.

Principal vetor de violações de dados

- Segundo o Data Breach Investigation Report (DBIR) da Verizon, engenharia social é o padrão mais comum que resulta em violações de dados.
- O relatório também determina que "...phishing permanece uma das principais variedades de Ação em violações e tem sido assim nos últimos dois anos"

Fonte: Verizon Data Breach Investigation Report

Reforce a sua resiliência no principal ponto de entrada dos ataques

As aplicações do Kaspersky Security for Mail Server ajudam a criar resiliência aos ataques por e-mail ao:

Identificar e filtrar emails suspeitos e indesejados no nível do gateway

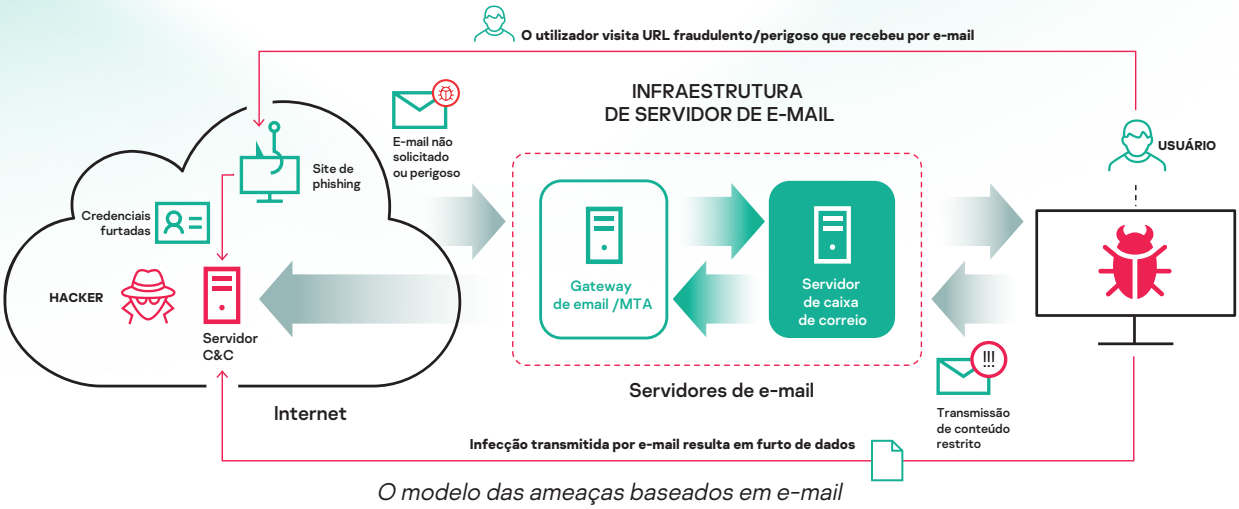
A maioria dos ataques por e-mail só são ativados ao nível do endpoint – o Kaspersky Security for Mail Server se propõe a interrompê-los muito antes de chegarem tão longe. A nossa proteção premiada reforça a sua resiliência ao detectar e interceptar ataques, logo no início da killchain, e antes que eles violem o seu perímetro e cheguem aos seus endpoints e usuários.

Processamento de emails legítimos com rapidez e precisão

A principal função que o e-mail desempenha nas comunicações de negócio significa que processamento da segurança deve ser rápido, ágil e conciso – sem impedir as comunicações legítimas. O Kaspersky Security for Mail Server oferece as tecnologias de proteção mais eficazes do setor contra tudo, desde emails de phishing e spam a ataques de Comprometimento de Emails Corporativos (BEC) e ransomware, com uma taxa de falsos positivos próxima a zero, permitindo que emails legítimos sejam transmitidos sem interrupções.

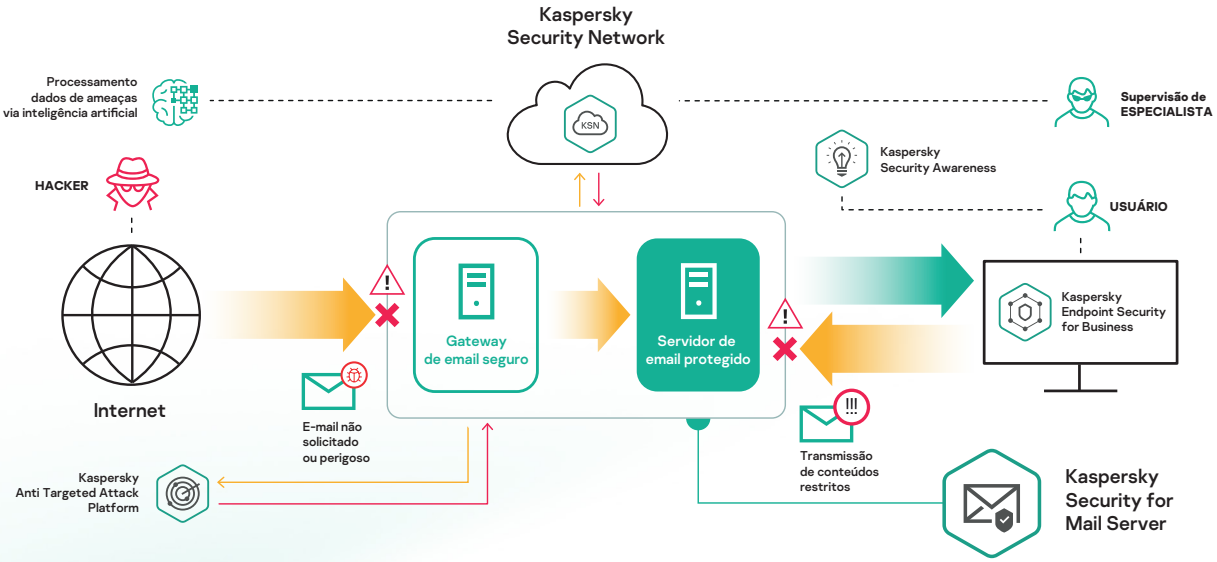
Protegendo emails além do gateway

O Kaspersky Security for Mail Server detecta conteúdo mal-intencionado ou indesejado não apenas no gateway, mas também no nível das caixas de correio individuais do Microsoft Exchange Server e/ou Microsoft Exchange Online. Ataques de phishing com atraso projetados para evadir contramedidas no nível do gateway, mensagens BEC geradas após apropriações de contas, e cenários de ameaças internos que nunca precisam passar pelo gateway – tudo isso pode ser identificado e erradicado, tornando a proteção de caixas de correio do servidor um item obrigatório.



O modelo das ameaças baseados em e-mail

Recursos principais



Como o Kaspersky Security for Mail Server combate as ciberameaças transmitidas por e-mail

Proteção de malware multicamadas

Várias camadas de segurança são capazes de parar a maioria dos malwares complexos transmitidos por email – incluindo spyware, wipers, mineradores e ransomware – todos são frequentemente liderados por phishing direcionado. Dados de reputação da nuvem, detecção precisa, modelos de machine learning local e na nuvem, inteligência de ameaças adquirida globalmente e dados de pesquisa exclusivos são combinados para garantir uma das melhores taxas de detecção de falsos positivos do setor.

Abrangência dos cenários: uma licença para todos

Uma única licença de produto cobre uma variedade única de cenários – incluindo aumento da proteção da infraestrutura de email pré-existente ou criação de uma nova e segura. Uma série de arquiteturas de email englobando tecnologias Linux ou Windows, locais, virtualizadas, na nuvem ou uma combinação delas, tudo em um único produto da Kaspersky

Antispam automatizado (com reputação de conteúdo e endereço de origem)

O sistema antispam da Kaspersky usa mecanismos inteligentes para minimizar a possibilidade de falsos positivos conforme eles se adaptam continuamente a mudanças nas técnicas de disseminadores de spam. Os dados de reputação coletados globalmente são processados na nuvem e usados para alimentar aspectos de inteligência artificial, fornecendo uma base sólida para detecção eficiente de spams.

Combatendo o Comprometimento de Emails Corporativo (BEC)

Um sistema dedicado de detecção baseada em aprendizagem automática, com modelos algorítmicos atualizados regularmente com novos cenários, processa uma série de indicadores indiretos, permitindo que o sistema possa bloquear mesmo os e-mails falsos mais convincentes.
O suporte a mecanismos de autenticação do remetente, tais como SPF/DKIM/DMARC, ajuda a proteger contra spoofing de origem – o que é especialmente útil para ajudar em cenários de Comprometimento de Emails Corporativos (BEC).

Sandboxing

Para proteger até mesmo contra o malware mais furtivo e sofisticado, os anexos são executados em um ambiente emulado seguro, onde são analisados para garantir que amostras perigosas não penetrem no sistema corporativo. Para os usuários da Kaspersky Anti Targeted Attack, a integração agrega "detonação" a um ambiente de sandbox avançado, realista e externo – proporcionando níveis muito mais detalhados de avaliação e análise dinâmica.

Antiphishing avançado

O sistema antiphishing avançado da Kaspersky usa análise baseada em rede neural para criar modelos de detecção eficazes. Com mais de 1.000 critérios usados – incluindo imagens, verificações de linguagem e scripts específicos – esta abordagem assistida por nuvem é apoiada por dados adquiridos globalmente sobre URLs e endereços IP mal-intencionados e de phishing e emails de phishing desconhecidos/de hora zero.

Bloqueando transferências de conteúdos inseguros

O sistema de filtragem de anexos configurável da Kaspersky pode detectar disfarces de arquivos comumente usados por criminosos cibernéticos, identificando anexos possivelmente perigosos. A funcionalidade semelhante a DLP permite que o administrador configure regras complexas para evitar vazamento de dados, armado com o poder de expressões regulares e se beneficiando de uma infinidade de práticas recomendadas acumuladas pela comunidade.

Para além do gateway – resiliência ao nível da caixa de correio

As tecnologias no nível de caixas de correio incluem:

Novas verificações de emails – abordando cenários como ativação de URLs de phishing com atraso.

Quarentena de sombra antispam – ideal para ambientes de baixa tolerância. Os e-mails eventualmente suspeitos podem ser colocados em quarentena temporária até o Kaspersky Security Network ter juntado provas suficientes para avaliar se a entrega é realmente segura.

Visibilidade

Uma interface baseada na Web clara e amigável permite que o administrador monitore os níveis de proteção do email corporativo, com ferramentas como:

- Painel configurável.
- Visualizador de eventos conveniente com uma poderosa pesquisa de eventos booleana.
- Exportação de eventos para o sistema SIEM próprio.
- Relatórios no console ou por email.
- Monitor de integridade do sistema.

Dimensionamento e resiliência

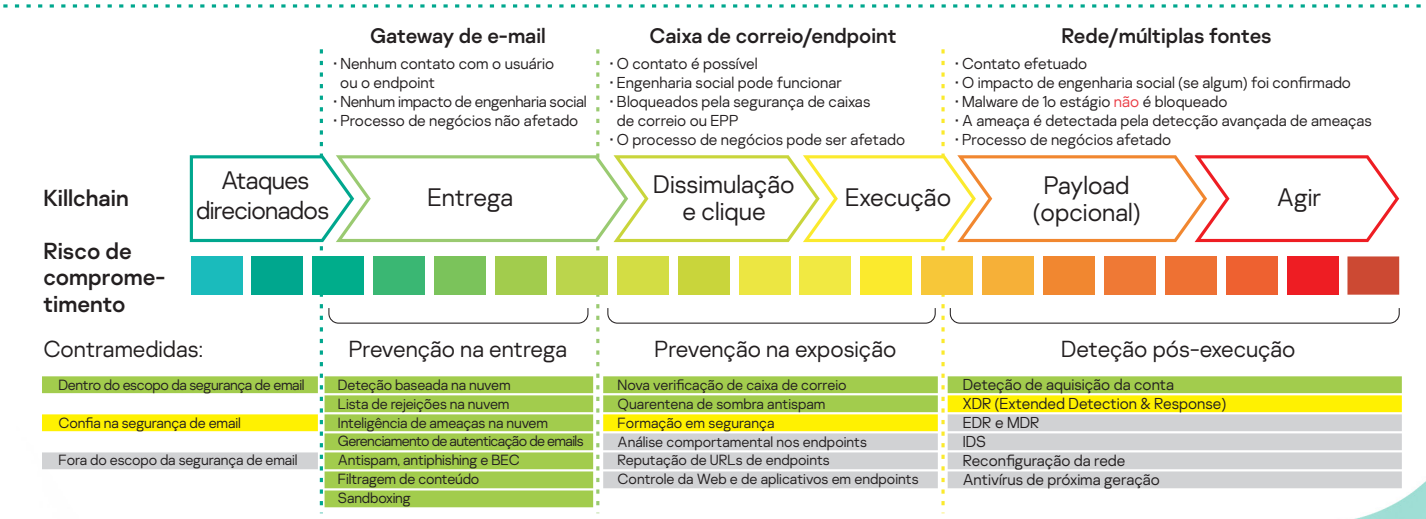
A solução é compatível com arquiteturas em cluster para lidar com cargas de tráfego crescentes e garantir resiliência de todo o sistema de segurança de email em caso de um desastre. Para garantir que nenhum dado crítico seja perdido devido à desinfecção, exclusão ou acidente técnico, um backup das mensagens originais pode ser feito de acordo com critérios especificados pelo administrador, permitindo um acesso sem riscos.

Gerenciamento e controle de acesso

Regras flexíveis permitem ao administrador configurar políticas que combinam vários critérios e rastrear quaisquer tentativas de violação. Para um all-in-one appliance de email seguro, instrumentos especialistas para configurar aspectos do sistema não relacionados a segurança são oferecidos no mesmo console de gerenciamento. Controle de acesso baseado em funções significa que administradores separados podem ser alocados a diferentes áreas da empresa ou a diferentes clientes.

Extended Detection and & Response

A integração com a Kaspersky Anti Targeted Attack fornece a você acesso a uma pilha de tecnologias de detecção de nível especialista composta por sandbox avançada, analisador de ameaças móvel, feeds de dados especiais com dados de C&C e muito mais. Após uma detecção bem-sucedida, um ataque direcionado poderá ser interrompido bloqueando seus componentes ao descobri-los e isolá-los em diferentes camadas da infraestrutura, usando cenários XDR pelos produtos.



A função da segurança de email em diferentes estágios da killchain de ataques cibernéticos

Embarque no Kaspersky Security for Mail Server

O Kaspersky Security for Mail Server é apenas um da série de produtos e soluções da Kaspersky, desenvolvido internamente, aproveitando mais de 20 anos de conhecimento focado, criado de uma única base de código e projetado para se integrar facilmente, fornecendo uma plataforma de segurança abrangente e incontestável.

Se você já usa o Kaspersky Endpoint Security for Business, instalar o Kaspersky Security for Mail Server significa que você poderá ter certeza de que a sua proteção de gateway de email fornecerá os mesmos padrões de alto desempenho que o resto da sua segurança.

Se ainda não o usar, é um bom momento para reforçar o seu perímetro e aumentar a sua resiliência ao instalar o Kaspersky Security for Mail Server ao mesmo tempo ou em vez da sua proteção de e-mail atual.

Talvez você também queira considerar...

Kaspersky Security for Internet Gateway — complemente a proteção do seu perímetro de email com uma segurança de gateway para Web igualmente poderosa — também incluída no Kaspersky Total Security for Business.

Kaspersky Endpoint Security for Business — a nossa principal solução de segurança para endpoints, oferece a proteção de endpoints mais testada e premiada do mercado.

Kaspersky EDR Optimum — o novo carro-chefe das soluções de segurança de endpoints da Kaspersky, oferecendo visibilidade aprimorada e informações detalhadas sobre detecções de malware suplementadas por opções de análise de causa raiz e respostas automatizadas.

Como comprar

O Kaspersky Security for Mail Server é vendido como solução direcionada autônoma ou como add-on disponível apenas para os clientes do Kaspersky Endpoint Security for Business.

Aplicações incluídas

- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Security for Cloud Mail

Licenciamento

O Kaspersky Security for Internet Gateway está disponível com:

- Licenciamento anual
- Subscrição mensal

Experimente antes de comprar

Explore o Kaspersky Security for Mail Server agora com a nossa avaliação grátis de 30 dias.

Solicite uma chamada

Ainda precisa de mais informações? Solicite uma ligação nossa!

Compre através de um parceiro de confiança

Já se sente pronto para comprar? Encontre um revendedor local para ajudá-lo com a sua compra.

Notícias sobre ameaças cibernéticas: www.securelist.lat
Notícias sobre segurança de TI: business.kaspersky.com
Tecnologias da Kaspersky: kaspersky.com/technowiki
Segurança de TI para pequenas e médias empresas: kaspersky.com.br/business
Segurança de TI para grandes empresas: kaspersky.com.br/enterprise

www.kaspersky.com.br

Somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de construir um mundo mais seguro, onde a tecnologia melhore nossas vidas. Por isso, nós a protegemos. Para que todos tenham acesso às infinitas oportunidades que ela proporciona. Garanta a cibersegurança para um futuro mais seguro.

Saiba mais em kaspersky.com.br/transparency

Proven. Transparent. Independent.