



Kaspersky Endpoint Security for Business

A tecnologia é a força de transformação para as empresas - mantenha o ritmo ou fique estagnado. Mas a tecnologia também abre portas para os criminosos, com o endpoint sendo um alvo principal. Portanto, você precisa ser mais inteligente do que os cibercriminosos que têm você nos sites deles, implementando soluções rigorosas e confiáveis para proteger o que sua empresa mais valoriza.

Desafios



Aumento de pressão dos ataques

Agora que as ferramentas dos cibercriminosos são tão baratas, estamos observando um crescimento significativo de eventos e riscos na segurança. Ransomware, spyware financeiro, phishing e outras ameaças podem atingir sua organização com severas perdas, particularmente se você estiver no auge da transformação digital.



Uma infraestrutura heterogênea para proteger

A proliferação de trabalho remoto, serviços na nuvem, e processos ágeis que toda estratégia de segurança precisa para cobrir a gama completa de seus dispositivos endpoint, incluindo notebooks, estações de trabalho, servidores e dispositivos móveis, incluindo os dispositivos pessoais usados para o trabalho. Você também precisa pensar sobre os diversos sistemas operacionais aos quais estiver dando suporte.



Altos níveis de complexidade para competir

Uma infraestrutura complexa de TI e a especialização necessária para dar suporte e proteger isso, tudo tem um custo. Você tem que investir com eficácia nas soluções corretas para atender suas mudanças de requisitos de segurança corporativa - em termos de tempo, orçamento, equipe e habilidades específicas.

Solução



Segurança adaptativa ágil

Você precisa ser capaz de:

- Proteger por completo seus dados, funcionários e a infraestrutura sem impactar o desempenho.
- Confie na inteligência de ameaça mais recente e mais confiável para identificar e enfrentar as ameaças emergentes indo ao seu encontro.
- Reconheça os padrões de comportamento da ameaça para que até as ameaças desconhecidas possam ser neutralizadas.
- Reduza sua superfície de ataque ao controlar quais aplicativos, sites e dispositivos possam interagir com seus endpoints e usuários.



Solução única para qualquer plataforma

Estaremos procurando por:

- A melhor segurança possível para cada estação de trabalho, servidor e dispositivo móvel que armazenam seus dados - seja onde esteja ou se você tem ou não a propriedade deles. Pense também sobre os pontos de entrada de ameaça e como proteger a Web e gateways de e-mail sem criar mais trabalho para sua equipe.
- A garantia de que você possa cobrir cada SO em seu ambiente misto - incluindo Windows, Mac, Linux, iOS e Android - com uma solução única, funcionando em um único console.



Gerenciamento flexível e automação de tarefas

E você irá querer maximizar seus recursos com:

- Altos níveis de automação - particularmente para tarefas essenciais mas de rotina, tal como a aplicação de correções e implementação de SO. O tempo e especialização de sua equipe é muito valioso para ser desperdiçado.
- Capacidades de gerenciamento remoto - seja configurar estações de trabalho em home offices ou tornando os dados seguros com opções de criptografia.
- Centralização Sem esquivar-se entre consoles - você precisa de gerenciamento direto e integrado em uma única tela em seu perímetro ou na nuvem.

Custo de violações de dados

105 mil dólares
par PMEs

927 mil dólares
para corporações

101 mil dólares
2020

▲ 105 mil dólares
2021

US\$ 1,09 milhão
2020

▼ 927 mil dólares
2021

Fonte: Kaspersky IT security economics report 2021

Três pacotes de recursos progressivos

As ferramentas e tecnologias no Kaspersky Endpoint Security for Business são equilibradas de forma inteligente em níveis progressivos para atender à sua segurança envolvente e as necessidades de TI na medida em que sua empresa cresce.

<ul style="list-style-type: none">Proteção de ameaças contra arquivo, Web e e-mailProteção para estações de trabalho, servidores e dispositivos móveisDeteção de ComportamentoPrevenção e remediação de ransomware e exploitAcesso à Kaspersky Security Network (KSN)Console de gerenciamento na nuvem ou no localControle de aplicativos para estações de trabalhoControle de Dispositivos e da WebLimpeza de dados remotosAvaliação de vulnerabilidadesGerenciamento de dispositivos móveisExportação de eventos através do SyslogIntegração EDR e sandbox na nuvem	Selected Endpoint Security for Business
<ul style="list-style-type: none">Controle de acesso baseado em funçõesControle de aplicativos para servidoresGerenciamento de CorreçõesControle adaptativo de anomaliasGerenciamento de criptografia (a nível de arquivo, disco e dispositivo)Inventário de HW e SWInstalação de software de terceiros e sistemas operacionaisExportação automática para SIEM (suporte CEF e LEFF)	Advanced Endpoint Security for Business
<ul style="list-style-type: none">Proteção do tráfego de e-mail e da Web no nível do gatewayAntiphishing avançadoFiltragem de reputação e deteção de endereço maliciosoFiltragem de conteúdo e antispamDeteção de Comprometimento de E-mails Corporativos (BEC)Proteção para os serviços do Microsoft Office 365	Total Security for Business

Ameças de ransomware

Estes ataques foram executados em indivíduos ou corporações, com alguns dos ataques mais notáveis nos últimos anos atingindo as principais marcas.

88% dos executivos de empresas que tinham sido anteriormente atingidos por ransomware disseram que iriam pagar se fossem atacados novamente.

O ransomware é uma questão crescente para as empresas ao redor do mundo, com o número de ataques usando ransomware quase duplicando somente em 2021. Isso pode ser atribuído principalmente para a pandemia, que viu mais pessoas trabalhando de casa. Com um modelo de trabalho híbrido que parece que chegou para ficar, a probabilidade de uma ataque ransomware permanece presente.

O que nós entregamos para você

- Segurança verdadeira. Nós protegemos por completo todos os seus endpoints contra ameaças amplamente espalhadas e emergentes, graças ao inigualável desempenho das tecnologias da Kaspersky, tal como **proteção contra ataque sem arquivo**, análise de comportamento com **base em ML** e proteção específica contra exploits, ransomware e spyware financeiro.
- Proteção proativa Nós paramos os ataques antes que eles comecem. A proteção de pré-execução pelo **Controle de Anomalia Adotiva** combina a simplicidade de regras de bloqueio com a inteligência de ajuste automático com base na análise de comportamento.
- Um completo ecossistema para sua crescente maturidade de segurança de TI. Resposta automatizada e alavancagem de análise de **integrações** com soluções **EDR** e **SIEM**.
- Vantagem econômica. Nossa abordagem em camadas significa que você somente paga pelas capacidades de que precisa no momento.
- À prova do futuro. A atualização é racional - basta mover entre as camadas. Nossa solução totalmente dimensionável está pronta para dar suporte a **milhares de dispositivos gerenciados** na medida em que você cresce.
- **Adoção racionalizada da nuvem**. Com a proteção para os serviços do **Microsoft Office 365**
- Flexibilidade. **Escolha sua opção preferida de implementação**: na nuvem, no local, lacuna de ar e em implementações híbridas. A seguir, aloque diferentes níveis de acesso aos sistemas de segurança com diferentes membros da equipe com controle de acesso granular com base na função (**RBAC**).
- Tranquilidade. Todos os seus dados confidenciais estão totalmente protegidos com o **conjunto de recursos de proteção de dados**, incluindo o gerenciamento de criptografia nos níveis completos de arquivo e disco e em dispositivos externos. A limpeza de dados remotos erradica os dados se um dispositivo for perdido ou roubado.
- Defesas do perímetro. **Prevenir ataques com base na Web** atinjam os alvos principais: os seus usuários e seus endpoints

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

IDC | ANALYZE THE FUTURE



A segurança que conquista mais prêmios e tão valorizada por nossos clientes

Entre 2013 e 2021, os produtos da Kaspersky participaram de 741 testes e análises independentes. Nossos produtos ficaram 518 vezes em primeiro lugar. Veja mais detalhes em www.kaspersky.com.br/top3

Casos de uso



Defenda seu sistema automaticamente

A detecção baseada em comportamento faz parte da abordagem da próxima geração em vários níveis da Kaspersky. É uma das formas mais eficientes de proteção contra ameaças avançadas, tal como malware sem arquivos, ransomware e malware de dia zero.

O uso de dados do Kaspersky Security Network assegura respostas mais rápidas à novas ameaças, aprimora o desempenho dos componentes de proteção, e reduz a probabilidade de falsos positivos. No final do dia, taxas superiores de detecção e segurança adaptativa incorporada significa uma resposta rápida aos ataques com um mínimo de falsos positivos. A Kaspersky é o único fornecedor de cibersegurança a ter uma taxa de 100% em proteção contra ransomware em um estudo [AV-Test recente](#). [AV-Test Advanced Endpoint Protection: Ransomware Protection test](#), AV-Test, 30 de setembro de 2021



Reduza sua superfície de ataque

Alinhe os dispositivos remotos com sua segurança corporativa de TI. Os controles de aplicativo afetam a produtividade (ao restringir o acesso aos aplicativos ou redes sociais, por exemplo) e os funcionários de segurança podem se tornar vítimas de phishing e malware em aplicativos invadidos e sites duvidosos, ao apenas conectar um USB moderno, colocar uma impressora em rede pode resultar em vazamento de dados confidenciais. Todos esses vetores de ataque mais o risco de erro humano, podem ser significativamente reduzidos através dos controles granulares de aplicativo, Web e dispositivo.

O Controle de Anomalia Adaptativa significa que você pode fortalecer as políticas comuns e ver como o sistema irá aplicar as regras com base no comportamento do usuário.



Minimize o tempo, esforço e custos

Gerencie o Kaspersky Endpoint Security for Business a partir do console na nuvem.

A abordagem com base em SaaS não requer investimento em hardware e deixa você focar nas iniciativas de negócios ao invés de gastar tempo em atualizações, suporte e disponibilidade - ou de todo em infraestrutura na nuvem.

Epense sobre o tempo que sua equipe gasta em fortalecer o endpoint, com o gerenciamento de dispositivo remoto, com a implementação do SO e com o gerenciamento de criptografia. O Kaspersky Endpoint Security racionaliza e automatiza todas essas tarefas e mais - fornecendo uma solução única em uma interface na Web para gerenciar tudo. Sem mais consoles separados ou diferentes produtos para cada tarefa ou tipo de dispositivo.



Desenvolva uma forte postura de proteção dos dados

Os ataques atuais usam ferramentas e aplicativos legítimos que permitem aos atores de ameaças encontrar novas vulnerabilidades e exploits de zero-dia em aplicativos comuns. O gerenciamento automatizado de correções reduz significativamente o risco aos seus dados destes ataques, enquanto a criptografia dos dados assegura que somente usuários legítimos possam acessar arquivos confidenciais ou dispositivos externos específicos. O criptografia completa do disco rígido também protege os dados se um dispositivo for perdido ou roubado.

A integração disponível no Kaspersky Total Security for Business também protege a colaboração e o compartilhamento de arquivos no Microsoft Office 365 e ajuda a prevenir o vazamento de PII (Informações de Identificação Pessoal).

EXPERIMENTE VOCÊ MESMO

Por que você mesmo não experimenta a proteção adaptativa? Visite [esta página](#) para obter uma avaliação gratuita de 30 dias do Kaspersky Endpoint Security for Business.



Abordagem em fases

Construir uma base de segurança para a sua organização escolhendo o produto ou serviço certo é apenas o primeiro passo. Desenvolver uma estratégia de segurança virtual corporativa com uma visão de futuro é a chave para o sucesso a longo prazo.

Nosso portfólio reflete as demandas de segurança das empresas de hoje, respondendo às necessidades de sua corporação, seja qual for o tamanho de sua organização ou seu nível de maturidade de segurança de TI, através de uma abordagem em fases.

Essa abordagem combina diferentes camadas de proteção contra todos os tipos de ameaças cibernéticas, ajuda prevenir automaticamente as ameaças - e depois as empodera sistematicamente e metodicamente, para você adicionar recursos novos e avançados para combater ameaças mais sofisticadas à medida que sua empresa evolui. Nós vemos o quadro completo para que você possa focar sem medo na inovação.



Kaspersky Security Foundations



Kaspersky Endpoint Security for Business



Kaspersky Hybrid Cloud Security



Kaspersky Embedded System Security



Kaspersky Security for Storage



Kaspersky Security for Mail Server



Kaspersky Security for Internet Gateway



Kaspersky Professional Services



Kaspersky Premium Support and Professional Services

- Proteção para usuários corporativos e dispositivos móveis
- Segurança de servidores em ambientes híbridos
- Proteção para desktops virtuais (VDI)
- Proteção para endpoints especializados e PCs herdados
- Proteção contra o vetor de ataque mais comum – e-mails
- Proteção de vanguarda contra ameaças baseadas na Web
- Assistência à implementação, configuração e manutenção

Desfrute ao máximo do ecossistema completo da Kaspersky



Kaspersky Security Foundations

Nossa prevenção de ameaças gerenciado na nuvem permite que todas as organizações interrompam automaticamente as ameaças cibernéticas às commodities em qualquer dispositivo, VDI e infraestrutura de servidor híbrido.

- Protege todos os dispositivos, incluindo endpoints herdados e especializados
- Entrega a visibilidade e controle sobre todos os ativos de TI
- Ajuda a prevenir ou mitigar os erros do usuário
- Fornece a automação de gerenciamento de sistemas de que você precisa, sem gastar muito



Kaspersky Optimum Security

Ajuda a proteger empresas contra ameaças novas, desconhecidas e evasivas. Solução de detecção e resposta de ameaças, fácil no monitoramento de recursos de segurança 24/7, caça automatizada às ameaças e as respostas guiadas e gerenciadas suportadas por especialistas da Kaspersky.

- Atualiza a proteção de endpoints contra ameaças evasivas
- Suporta a criação de processos essenciais de resposta a incidentes
- Otimiza o uso de recursos de cibersegurança



Kaspersky Expert Security

Desenvolvida para atender às necessidades diárias de qualquer empresa com segurança de TI madura para lidar com as ameaças atuais mais sofisticadas, incluindo APTs (Ameaças Persistentes Avançadas) e ataques direcionados.

- Otimiza as cargas de trabalho dos seus especialistas
- Melhora seus conhecimentos e habilidades
- Dá apoio aos seus especialistas

Notícias sobre ameaças cibernéticas:

securelist.lat

Notícias sobre segurança de TI:

www.kaspersky.com.br/blog/category/business/

Segurança de TI para PMEs:

www.kaspersky.com/business

Segurança em TI para empresas:

kaspersky.com.br/enterprise

kaspersky.com.br

© 2022 AO Kaspersky Lab. As marcas registradas e de serviço são propriedade dos respectivos titulares.



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



**Proven.
Transparent.
Independent.**

Saiba mais em kaspersky.com.br/transparency