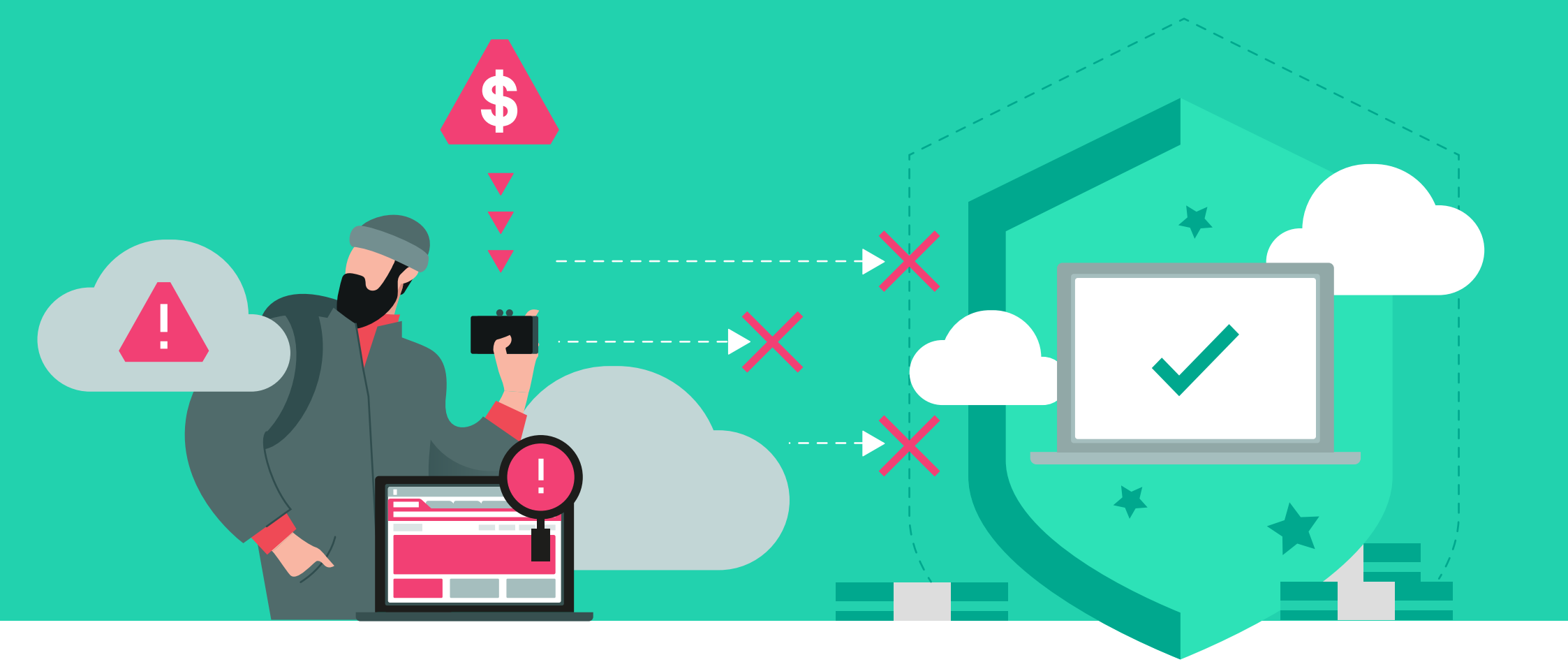


Porque escolher a proteção da Kaspersky contra Ransomware?

kaspersky

O Problema

O ransomware é uma ameaça persistente que, em 2020, continua evoluindo. Esses ataques envolvem um risco cada vez maior, são muito mais direcionados a segmentos e setores específicos, e conquistam resgates mais valiosos. Os custos dos contratempos devido a paralisações cresceram drasticamente, e o número de novas famílias de ransomware de agentes não definidos aumenta continuamente, tornando o ransomware um dos maiores problemas de segurança de TI para as PMEs.

A Solução

A excelente proteção de endpoints da Kaspersky foi desenvolvida com o objetivo de vencer os desafios de 2020 e além, incorporando ferramentas anti-ransomware de detecção de comportamento na nuvem para verificar e bloquear ransomware e criptomalware, protegendo as cargas de trabalho na nuvem, endpoints físicos e virtuais e redes compartilhadas e revertendo os arquivos afetados ao estado pré-criptografia.

Os números de 2020

US$ 40 bilhões

CUSTO GLOBAL ESTIMADO
das exigências e da paralisação devido a ransomware em 2020.[1]

23x

MAIS CUSTOS DEVIDO A PARALISAÇÕES
incorridos em relação aos pedidos médios de resgate, mostra a pesquisa.[2]

US$ 141,000

CUSTO MÉDIO DO TEMPO DE INATIVIDADE CAUSADO POR RANSOMWARE
em 2019 (200% de aumento em relação a 2018).[3]

[1] Ransomware Demands: $170B Worldwide Forecase in 2020, Report

[2] Datto's Global State of the Channel Ransomware Report 2019

[3] Help Net Security: 1 in 5 SMBs have fallen victim to a ransomware attack

62.4%

DAS EMPRESAS FORAM VÍTIMAS DE RANSOMWARE
segundo uma pesquisa internacional de 2019 com tomadores de decisões de TI.

30%

DOS ALVOS DE RANSOMWARE NO ÚLTIMO ANO
são usuários corporativos.[5]

20%

DAS PMES FORAM VÍTIMAS
de ataques de ransomware em 2019, segundo a pesquisa[9]

[4] Statista: Percentage of organizations victimized by ransomware attacks worldwide from 2017 to 2019

[5] Um terço dos ataques de ransomware visa usuários corporativos: Kaspersky e INTERPOL recomendam backups e proteção no Dia Anti-Ransomware

[6] Um terço dos ataques de ransomware visa usuários corporativos: Kaspersky e INTERPOL recomendam backups e proteção no Dia Anti-Ransomware

21%

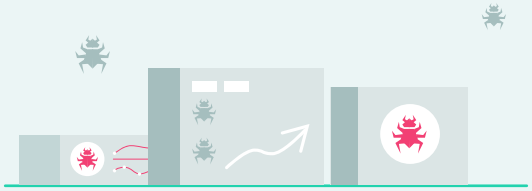
PARCELA DO WANNACRY
dentre todos os ataques de ransomware detectados no ano passado.[6]

22

NOVAS FAMÍLIAS DE RANSOMWARE
surgiram + 46.156 modificações de agentes de criptografia.[7]

49%

DOS ATAQUES DE RANSOMWARE DETECTADOS NO PRIMEIRO TRIMESTRE DE 2020
são de ransomware de criptografia.[8]



[7] Boletim de Segurança de 2019 da Kaspersky. Estatísticas

[8] Relatório da KSN: Ransomware 2018-2020

[9] Datto's Global State of the Channel Ransomware Report 2019

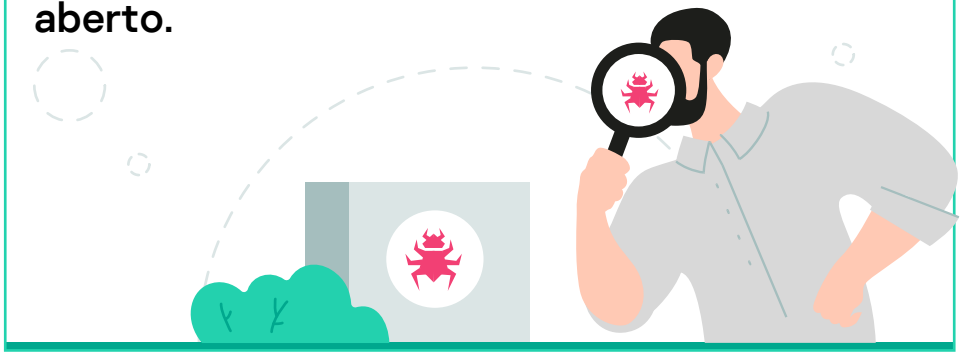
As soluções de cibersegurança da Kaspersky oferecem proteção comprovada contra ransomware nos estágios de entrega e execução do malware usando tecnologias sofisticadas de proteção em várias camadas.

EDR automatizado

O Kaspersky Endpoint Detection and Response proporciona visibilidade abrangente da rede e defesa sofisticada, automatizando tarefas para descobrir, priorizar, investigar e neutralizar ransomware e outras ameaças complexas. O EDR implementa métodos “pesados” de detecção (Sandbox, modelos de deep learning, correlação de eventos), além das ferramentas especializadas de investigação de incidentes, busca proativa de ameaças e resposta a ataques.

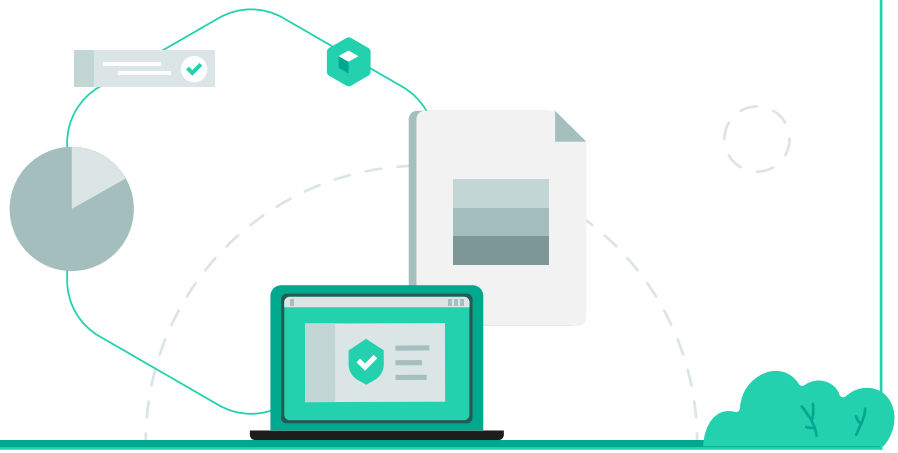
Prevenção de exploits

A prevenção de exploits da Kaspersky impede a infiltração de malware (inclusive ransomware) por meio de vulnerabilidades de software. Acionado por ações suspeitas, o componente realiza a análise de comportamento em relação a padrões maliciosos. São adicionadas assinaturas especiais para malware que utiliza exploits, possibilitando a detecção de arquivos maliciosos antes que sejam abertos. A proteção proativa permite a detecção e o bloqueio do malware assim que o arquivo é aberto.



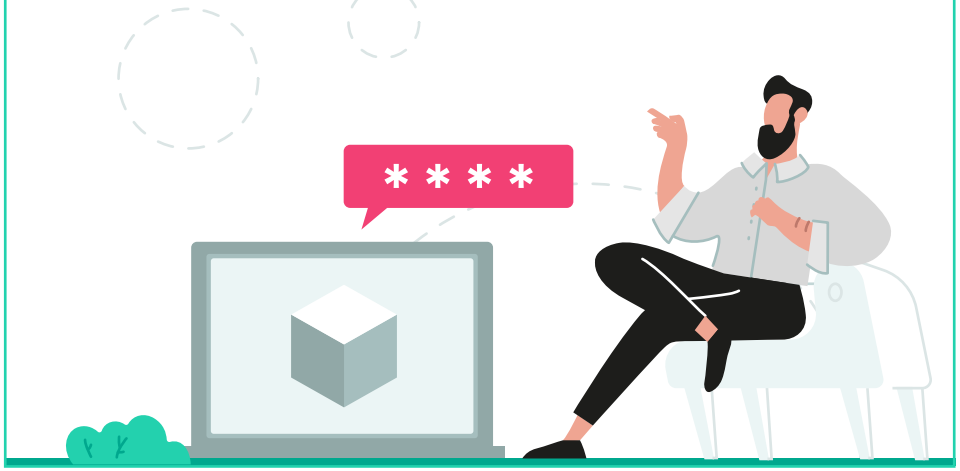
Detecção de comportamento acionada por Machine Learning (com reversão automática)

As tecnologias da Kaspersky baseadas em Machine Learning detectam ameaças de malware desconhecidas (inclusive ransomware) por meio do 'aprendizado' a partir da inteligência de ameaças de Big Data relevante e da criação de modelos de detecção eficientes, no local e como um processo de análise de ameaças no laboratório, utilizando múltiplas camadas de segurança. A Kaspersky Anti-Ransomware Tool tenta reverter automaticamente a ação de aplicativos maliciosos (por exemplo, restaurando os arquivos modificados e o Registro do sistema).



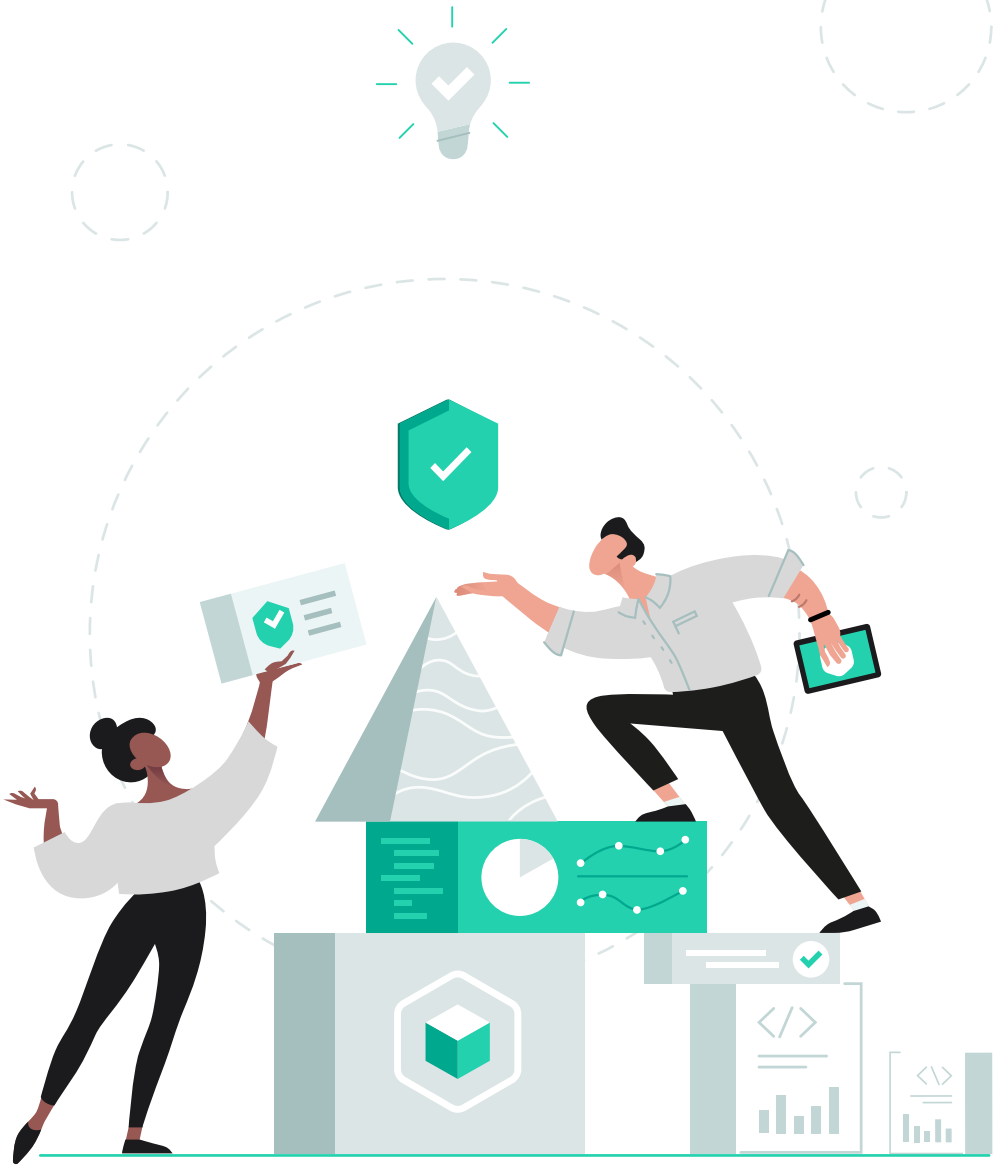
Gerenciamento da criptografia

O ransomware é um malware que criptografa os arquivos da vítima. O gerenciamento da criptografia da Kaspersky configura a criptografia dos dispositivos gerenciados com Windows e macOS, impedindo que usuários não autorizados tenham acesso não permitido aos dados armazenados. A Criptografia do Disco Completo evita o vazamento de dados quando um dispositivo é perdido. A criptografia em nível de arquivos protege os arquivos transferidos em canais não confiáveis, e o Crypto Disk armazena os dados do usuário criptografados em um arquivo separado.



Avaliação de vulnerabilidades e gerenciamento de patches

A avaliação de vulnerabilidades e gerenciamento de patches da Kaspersky evita que malware, inclusive ransomware, explore vulnerabilidades recém-descobertas e não corrigidas em sistemas operacionais e aplicativos comuns. Ela possibilita a fácil detecção de softwares vulneráveis em qualquer endpoint com a automação da avaliação de vulnerabilidades, da distribuição de patches e atualizações e do lançamento de aplicativos em um único console de gerenciamento integrado.



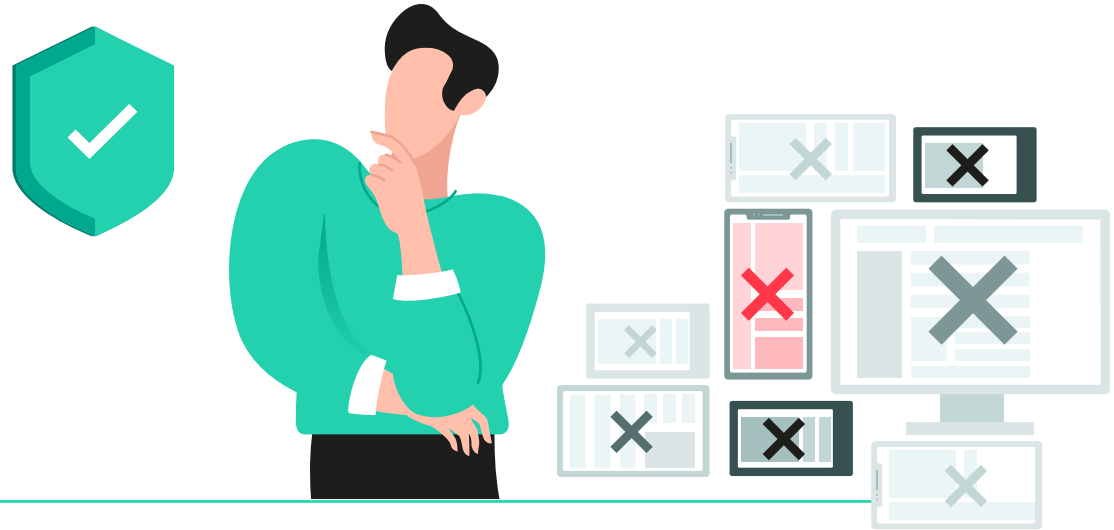
Embora o número absoluto de ataques de ransomware tenha diminuído nos últimos 12 meses, o impacto negativo de um ataque bem-sucedido sobre as organizações aumentou drasticamente, associando o custoso tempo de inatividade, efeitos sobre a reputação e pagamentos de resgates. O ransomware continua sendo uma das ameaças cibernéticas mais temidas pelas organizações de todos os tamanhos e setores.

Como proteger os dispositivos de ransomware

- [x] Faça backup de seus dados regularmente em um local de fácil acesso em caso de emergência.
- [x] Use ferramentas capazes de detectar vulnerabilidades automaticamente, além de baixar e instalar todos os patches.
- [x] Sempre mantenha o software e os sistemas operacionais atualizados em todos os dispositivos.
- [x] Esteja sempre atento a ataques de phishing, mensagens e links falsos, e arquivos possivelmente maliciosos.
- [x] Instrua seus funcionários. Cursos de treinamento, como o Kaspersky Automated Security Awareness Platform, podem ajudar.
- [x] Instale uma cibersegurança em várias camadas bem avaliada, como o Kaspersky Endpoint Security for Business, ou, em dispositivos pessoais, o Kaspersky Security Cloud, para ter proteção contra malware de criptografia de arquivos e reverter as alterações feitas por aplicativos maliciosos.

O que fazer se os seus dados forem infectados por ransomware

- ✓ Interrompa a conexão com a Internet.
- ✓ Como regra, não faça nenhum pagamento. Um terço das vítimas não recupera o acesso aos dados, mesmo depois de pagar.
- ✓ Obtenha ajuda técnica imediatamente para recuperar seus dados.
- ✓ Entre em contato com a iniciativaNo More Ransom para obter recursos, inclusive mais de 100 ferramentas gratuitas de descriptografia.



Não deixe seus dispositivos vulneráveis à exploração por ransomware

Instale a Kaspersky Anti-Ransomware Tool GRÁTIS e utilize recursos de ponta, como a detecção de comportamento na nuvem, para verificar e bloquear ransomware e criptomalware imediatamente! Nossa ferramenta é compatível com o GDPR e funciona em paralelo com a maioria dos softwares de segurança.

A Kaspersky Anti-Ransomware Tool não é o único produto da Kaspersky com uma história de sucesso. As soluções de cibersegurança da Kaspersky são comprovadamente consistentes em testes independentes:

A PROTEÇÃO MAIS TESTADA E MAIS PREMIADA DO MUNDO

86	64	81%
TESTES/ANÁLISES REALIZADOS	PRIMEIROS LUGARES	3 PRIMEIROS LUGARES

Descubra os benefícios das avançadas tecnologias de proteção abrangente da Kaspersky com o Kaspersky Endpoint Security for Business. Proteja vários endpoints, dispositivos móveis e servidores de arquivos remotamente, de qualquer lugar, com o Kaspersky Endpoint Security Cloud.

kaspersky