

Cibersegurança
para pequenas
e médias empresas

O que faz sua pequena e sólida empresa ficar ainda mais forte

43%* dos ataques têm como alvo PMEs

1 semana a 6 meses

Possível tempo de inatividade



cerca de 70 mil USD*

É o custo médio de um incidente (perda de dados, phishing, ransomware, fraude, danos à reputação)

O que está acontecendo e por que isso é importante para o seu negócio

Plataformas em nuvem, trabalho remoto, dispositivos móveis, ferramentas e serviços on-line e automação baseada em IA facilitam muitos aspectos das operações diárias, mas também aumentam a complexidade e dificultam a manutenção da segurança dos sistemas.



Mais ferramentas, mais pontos de entrada

Cada novo serviço adiciona mais uma possível porta de entrada para o seu negócio



Tempo e equipe limitados

Equipes de TI pequenas não conseguem monitorar tudo o tempo todo



Trabalho fora do controle da empresa

Usar contas e dispositivos pessoais para o trabalho coloca os dados fora do escopo de proteção e expõe a empresa a possíveis multas



Mais ataques impulsionados por IA

A IA permite ataques de phishing e de senhas automatizados, de baixo custo e em grande escala

Todos esses fatores ameaçam a continuidade e o crescimento dos negócios, podendo levar a:

- possíveis prejuízos financeiros,
- violações de dados
- e danos à reputação.

O que coloca seu negócio em risco, tanto interna quanto externamente

A maioria dos incidentes cibernéticos não começa com algo significativo. Eles começam com situações do dia a dia e desafios atuais.

Riscos externos e internos



Ransomware



Operações interrompidas



Malwares e ataques sem arquivo (fileless)



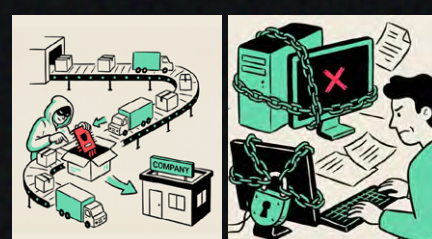
Roubo de dados, sistemas instáveis



Engenharia social



Credenciais roubadas, interrupção dos negócios



Ataques a cadeias de suprimentos



Interrupções para os clientes e consequente perda de confiança

Desafios



Crescimento rápido da TI



Segurança não consegue acompanhar



TI sobrecarregada



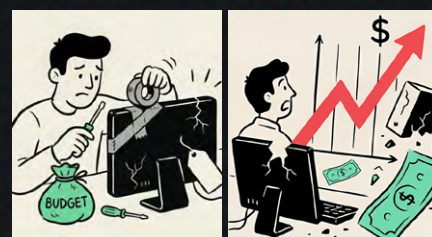
Ameaças não detectadas e resposta tardia



Escassez de competências no tratamento de incidentes



Decisões erradas pioram as situações

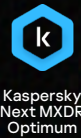
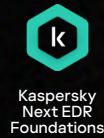


Orçamento limitado



Custos de recuperação mais elevados no futuro

Como a Kaspersky lida com ameaças e desafios



	Malware + <i>Ameaças comuns</i>	●	●	●	●
	Ransomware	●	●	●	●
	Ataques sem arquivo	●	●	●	●
	Phishing	●	●	●	●
	Malware desconhecido <i>Novos e direcionados</i>		●	●	●
	Erros humanos		●	●	●
	Terceiros não controlados		●	●	●
	Engenharia social			●	●
	Movimentação lateral			●	●
	Falta de recursos				●
	Continuidade dos negócios				●

Serviço gerenciado por especialistas da Kaspersky

O que significa segurança confiável para você

Proteção automática de ameaças

Proteção integrada contra ameaças em massa, reduzindo a necessidade de resposta manual

Redução da carga da TI

Menos tarefas manuais, menos erros, mais tempo para o que importa, com implementação simplificada na nuvem

Detecção precoce de ameaças

Interrompa ameaças evasivas antes que elas se tornem incidentes

Rápida recuperação em caso de incidentes

Menos tempo de inatividade, mais estabilidade para os negócios e menos perda de receita

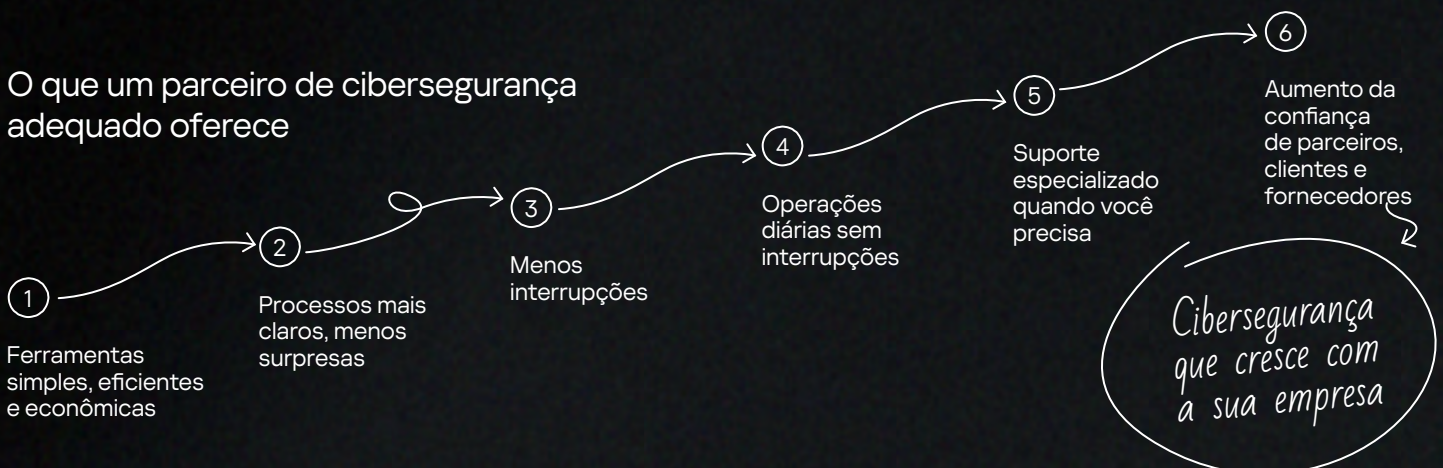
Proteção contra engenharia social

Treinamento em cibersegurança que ajuda os funcionários a identificar golpes, phishing e manipulação

Segurança especializada sem precisar montar uma equipe

Proteção robusta sem o custo e a complexidade de contratar especialistas

O que um parceiro de cibersegurança adequado oferece



Sua empresa está pronta para ter segurança nativa da nuvem feita sob medida?

Obtenha proteção eficaz desde o primeiro dia

www.kaspersky.com.br

Fale conosco

© 2026 AO Kaspersky Lab.
As marcas comerciais registradas e as marcas de serviço pertencem aos seus respectivos proprietários.