

# Kaspersky Endpoint Detection e Response Optimum

---

Coloque suas defesas de endpoint em um novo patamar e enfrente as ameaças evasivas de frente, e sem inconvenientes.



# Kaspersky Endpoint Detection and Response Optimum

Está na hora de subir um nível. Você não só está pronto para proteger a sua organização com as principais tecnologias anti-malware, como também para identificar, analisar e neutralizar com eficácia essas ameaças projetadas deliberadamente para escapar da proteção tradicional e se enterrar profundamente em seus sistemas, prontas para fazer o pior.

## Os desafios



### Detecção de ameaças evadindo

Malware, ransomware, spyware e outras ameaças evasivas estão se tornando mais inteligentes em evitar os mecanismos tradicionais de detecção – ao usar ferramentas de sistema legítimas e outras técnicas avançadas para o ataque.

**64%** das organizações já foram vítimas de ataques de ransomware. Destas, **79%** pagaram o resgate para seus atacantes.

**Kaspersky, Maio de 2021**



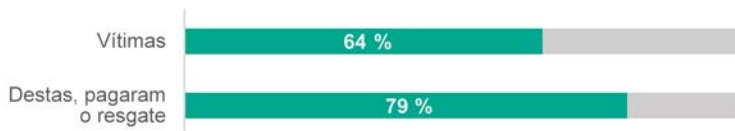
### Ransomware como um serviço

Os hackers compram ferramentas desenvolvidas prontas baratas e atacam qualquer pessoas- roubando dados, danificando sua infraestrutura e demandando valores crescentes de resgate.



### Recursos limitados

As infraestruturas estão se tornando ainda mais complexas e espelhadas, enquanto os recursos – tempo, dinheiro e spams de atenção – estão faltando. Não há lugar para shelfware.



"Nós valorizamos as soluções compreensivas, confiabilidade serviços e suporte disponíveis da Kaspersky. Elas estão garantindo a disponibilidade de nosso ambiente de TI".

**Marcelo Mendes CISO, NEO estudo de caso**

## Como podemos ajudar

O Kaspersky Endpoint Detection and Response (EDR) Optimum ajuda a identificar, analisar e neutralizar ameaças evasivas, fornecendo detecção avançada, investigação simplificada e resposta automatizada fáceis de usar.



### Proteção avançada

Nossos mecanismos de detecção avançada inclui tecnologias tal como aprendizado de máquina, análise de comportamento e sandbox na nuvem.

Ferramentas de análise visual simples significa que você pode entender por completo a ameaça e seu escopo – e ações de resposta rápida param os ataques em sua ocorrência, antes que o dano seja feito.



### Uma solução

A segurança de endpoint de próxima geração é trazida junto com um EDR simples de usar para a proteção aprimorada ee3 notebooks, estações de trabalho, servidores, cargas de trabalho na nuvem e ambientes virtuais.

Toda essa implementação e gerenciamento acontece em ul local, através de um console único na nuvem ou no local.



### Simple e eficiente

Nós desenvolvemos o EDR Optimum tendo em vista equipes menores de cibersegurança – para os que pensam em atualizar suas capacidades e resposta à incidente e desenvolver a especialização, mas que não têm muito tempo disponível.

Nós automatizamos e otimizamos a maioria das tarefas para que você tenha mais tempo para despendar nas coisas realmente mais importantes.



## Principais benefícios

- **Previna múltiplos tipos** de ameaças
- **Proteja seus sistemas e dados** contra ameaças evasivas
- **Identifique as ameaças atuais** antes que elas ajam
- **Reconheça as ameaças evasivas** entre os endpoints
- **Entenda a ameaça** e a analise rapidamente
- **Previna o dano** com uma resposta automatizada rápida
- **Economize tempo e recursos** com uma ferramenta simplificada
- **Defenda todos os endpoints:** notebooks, servidores, cargas de trabalho na nuvem



## Recursos principais

- Segurança inerente de **proxima geração**
- **Deteccção avançada** com base no aprendizado de máquina
- **Indicador de comprometimento (IoC)**
- **Ferramentas de investigação e análise** visual
- Todos os dados necessários em um **único cartão de alerta**
- **Resposta** guia e automação incorporados
- **Console único na nuvem ou no local** e automação
- Suporta **estações de trabalho, servidores virtuais e físicos, implementações VDI e cargas de trabalho públicas na nuvem**

## Principais casos de uso



### Estou sob ataque?

- **Deteccção avançada** - com base no aprendizado de máquina, incluindo o sandbox na nuvem - automaticamente detecta ameaças.
- **Baixe e verifique IoCs** de securelist, com ou outras fontes para encontrar ameaças avançadas.



### Posso neutralizála?

- **Utilize opções de múltiplas respostas** - isole o host, previna a execução do arquivo ou remova-o.
- **Verifique outros hosts** quanto a sinais da ameaça analisada.
- **Aplique uma resposta automática** entre os hosts ao descobrir uma ameaça (IoC).



### Como obtenho treinamento em habilidades?

- **Verifique o guia de resposta** no cartão de alerta.
- **Acesse o Portal de Inteligência da Ameaça** e a TI mais recente.
- **Desenvolva sua especialização** quando você analisa e responde às ameaças.



### Como isso aconteceu?

- Analise a ameaça em um **processo visual em árvore**.
- Rastreie suas ações em um **gráfico expansível**.
- **Entenda sua causa raiz e ponto de entrada** na infraestrutura.



### Como posso parar de isso nunca acontecer mais?

- **Coloque a informação aprendida em prática** - sabendo quais IPs e sites bloquear, políticas para modificar e funcionários a treinar.
- **Crie regras para prevenir** tais ameaças no futuro, exemplo, prevenir a execução de arquivo.



### E sobre as ameaças às commodities?

- **A segurança de endpoint de próxima geração** está integrada para parar imediatamente a maioria das ameaças.
- **Aumentar suas correções** com o Gerenciamento de Vulnerabilidades e Correções.
- **Automatizar sua redução da superfície de ataque** e o ajuste da política com controles de endpoint.

## Como funciona?



Para uma demonstração rápida, assista a [este vídeo](#).

## De onde você está vindo?



Tem anti-malware, mas não é suficiente?

### Aumente sua proteção de endpoint

Se você estiver usando a proteção de endpoint da Kaspersky ou de terceiros, este pode ser o momento certo de pensar sobre implementar EDR.

Não é apenas sobre as capacidades aprimoradas de detecção e prevenção, mas também estar preparado contra ameaças evasivas – identificando, analisando e neutralizando as mesmas.

Saiba como se proteger contra ameaças evasivas com o [Guia de Comprador para a Segurança de Nível ótimo](#).



Já está usando a Kaspersky?

### Otimize sua segurança

Nós estamos continuamente aprimorando nossos produtos, portanto assegure-se de que esteja nos usando por completo com uma atualização – ou mova para a nuvem e esqueça completamente sobre as tarefas de rotina irritantes.

Na versão mais recente do Kaspersky EDR Optimum:

- Resposta guiada no cartão de alerta!
- Verificação dos objetos críticos do sistema antes de aplicar a resposta!
- Reputação do arquivo de inteligência de ameaça no cartão de alerta!
- Profundidade ilimitada do processo de análise em árvore!

Saiba mais sobre os novos recursos [aqui](#).



Ainda não conhece a Kaspersky?

### Otimize sua segurança

Milhares de empresas ao redor do mundo usam o Kaspersky EDR Optimum porque ele fornece:

- EPP poderoso e EDR básico em um único produto
- Capacidades EDR simples de usar projetadas para pequenas equipes de cibersegurança
- Uma solução leve e flexível com implementação na nuvem ou no local

Examine o [Kaspersky Optimum Security](#) – uma solução composta contra ameaças evasivas com base na tecnologia EDR e MDR

## Siga adiante com uma abordagem de estágio por estágio

As ferramentas que você usa deveriam ser uma adequação perfeita para sua cibersegurança e necessidades da empresa, e para sua equipe e recursos. Portanto, nós o fizemos simples para escolher o nível de cibersegurança que seja seu foco principal neste momento, com três opções diferentes dependendo do perfil de sua organização.



### Kaspersky Security Foundations

Bloqueie automaticamente a grande maioria das ameaças.

- Prevenção automatizada multivetorial de incidentes causados por ameaças a commodities, que representam a grande maioria dos ataques cibernéticos.
- O estágio base para organizações de qualquer tamanho e complexidade no desenvolvimento de uma estratégia de defesa integrada.
- Proteção de endpoints confiável para quem tem equipes de TI pequenas e pouca experiência em segurança.

» [Saiba mais](#)



### Kaspersky Optimum Security

Desenvolvimento de defesas contra ameaças evasivas para aqueles que:

- Têm uma equipe de segurança de TI pequena com conhecimento básico em cibersegurança.
- Um ambiente de TI que está crescendo em tamanho e complexidade, o que aumenta a superfície de ataque.
- Falta de recursos de cibersegurança, em contraste com a necessidade de mais proteção.
- Necessidade crescente de desenvolver a capacidade de resposta a incidentes.

» [Saiba mais](#)



### Kaspersky Expert Security

Disposição imediata para ataques complexos e semelhantes a APT:

- Com ambientes de TI complexos e distribuídos.
- Uma equipe de segurança de TI madura ou um Centro de operações de segurança (SOC) estabelecido.
- Baixo apetite por risco devido a custos mais elevados de incidentes de segurança e violações de dados.
- Quem está operando em uma área de conformidade regulatória é uma preocupação.

» [Saiba mais](#)

## Quem somos

Nós somos uma empresa privada cibersegurança global com centenas de clientes e parceiro ao redor do mundo, comprometidos com a **transparência e independência**. Por 25 anos nós estamos desenvolvendo ferramentas e fornecendo serviços para mantê-lo seguro com nossas **tecnologias mais testadas e mais premiadas**.

### IDC

IDC MarketScape Worldwide Modern Endpoint Security for Enterprise e SMB 2021 Vendor Assessments

#### Principal atuante



### AV-Test

Proteção Avançada de Endpoint: Teste de Proteção Conta Ransomware

#### 100% de proteção



### Radicati Group

Quadrante de mercado de ameaças persistentes avançadas (APT)

#### Principal atuante



## Se você precisar de mais ainda

Examine o **Kaspersky EDR Expert**, uma poderosa ferramenta EDR para equipar seus especialistas com capacidades de busca profunda, personalização estendida e mecanismos superiores de detecção.

## Examine mais de perto

Para saber mais sobre como o Kaspersky Endpoint EDR Optimum enfrenta ameaças cibernéticas e facilita a vida da sua equipe de segurança e dos seus recursos, visite <https://www.kaspersky.com/enterprise-security/edr-security-software-solution>

Notícias sobre ciberameaças: [securelist.it](https://www.securelist.it)  
Notícias sobre segurança de TI: [business.kaspersky.com](https://business.kaspersky.com)  
Segurança de TI para PMEs: [kaspersky.com.br/business](https://kaspersky.com.br/business)  
Segurança de TI para Grandes Empresas: [kaspersky.com.br/enterprise](https://kaspersky.com.br/enterprise)

**kaspersky.com.br**

© 2022 AO Kaspersky Lab.  
As marcas registradas e de serviço pertencem aos seus respectivos proprietários.