



Kaspersky Next  
EDR Optimum

# Desvendando Kaspersky Next EDR Optimum



## O que é o Kaspersky Next EDR Optimum?

O Kaspersky Next EDR Optimum oferece uma proteção forte para endpoints, controles aprimorados, treinamento, gerenciamento de atualizações e muito mais — tudo aprimorado pela funcionalidade essencial de EDR.

A visibilidade, investigação e resposta a ameaças são simples, rápidas e guiadas, ajudando equipes de TI e de segurança de TI a repelir ataques rapidamente e gastando poucos recursos.



## Por que o Kaspersky Next EDR Optimum — e por que agora?

### O cenário em evolução de ameaças está tornando EDR um requisito, não uma escolha

Por anos, pequenas e médias empresas, assim como empreendimentos de baixo custo, têm conseguido contar com plataformas de proteção de endpoint (EPP) para se proteger de diversas ameaças “commodities” de produção em massa e de pouco esforço de disseminação. Mas os invasores de hoje em dia têm visado organizações de todos os tamanhos, todas as indústrias e todos os níveis de preparo — e estão armando ataques mais perigosos.

Essa evolução significa que, ao longo do tempo, ameaças cada vez mais sofisticadas, que antes afetavam apenas grandes organizações, estão se propagando para impactar pequenas e médias empresas e empreendimentos menores sem recursos internos para lidar com elas de forma eficaz.

Em particular, ocorreu o surgimento de ameaças evasivas, que utilizam ferramentas legítimas em ataques, incluem cenários prontos para contornar a EPP, têm baixo custo e estão disponíveis na dark web. Elas aumentaram os riscos à cibersegurança para organizações que utilizam soluções tradicionais de EPP.

Se o costume é ter apenas uma EPP, aprimorar suas defesas com detecção e resposta de endpoint (EDR) pode parecer um passo grande em termos de ferramentas e de habilidades. Mas, felizmente, não precisa ser assim.

Adicionar capacidades apropriadas de EDR à EPP moderna pode fornecer uma defesa eficaz contra ameaças evasivas mais avançadas

Seu negócio está sob ataque cibernético, como você reagirá?

É seu primeiro dia em um novo cargo de segurança de TI e você está ainda se inteirando das coisas quando a empresa sofre um ataque.

O que você faria? Como você reagiria?

Saiba mais

[www.kaspersky.com/response-game](http://www.kaspersky.com/response-game)

## Fazer o upgrade para EDR não precisa ser um desafio

Muitas organizações têm tempo e recursos limitados (ou um departamento de segurança de TI pequeno e sem planos de expansão), mas precisam entender o que está acontecendo em sua infraestrutura e ser capazes de responder a ameaças evasivas antes que ocorram danos.

Adicionar capacidades apropriadas de EDR à EPP moderna pode fornecer uma defesa eficaz contra ameaças evasivas mais avançadas. Portanto, se está começando em EDR, você deve procurar uma solução que permita respostas automatizadas, rápidas e precisas com um único clique, como quarentena de arquivos, isolamento de host, interrupção de processos, exclusão de objetos etc.

À medida que você ou a equipe de TI/EDR ficam mais experientes, sua solução também deve fornecer informações, insights e ferramentas para investigações eficazes, como análise de causa raiz, criação de indicadores de comprometimento (IoCs) personalizados, importação de IoCs e verificação dos mesmos em todos os endpoints.

Com disso, os resultados que você pode esperar do EDR incluem:

- Proteção robusta contra ameaças evasivas mais frequentes e disruptivas.
- Economia de tempo e de recursos com uma ferramenta automatizada simples.
- Avaliação do alcance de um ataque verificando IoCs em todos os endpoints.
- Compreensão da causa básica de cada ameaça e de que como ela realmente ocorreu.
- Prevenção de outros danos com a resposta automatizada rápida.

Portanto, se sua EPP está falhando em parar o aumento de novas ameaças desconhecidas e evasivas; se você tem visibilidade limitada do que está acontecendo em seus endpoints; se está preocupado com multas; ou se tem reputação da empresa sob ameaça por conta de um grande incidente de segurança, uma solução EDR moderna como o Kaspersky Next EDR Optimum oferece a maneira ideal de começar ou progredir em sua jornada EDR.

## Como o Kaspersky Next EDR Optimum pode ajudar



### O que ele faz

Oferece uma proteção forte para endpoints, controles superiores, treinamento, gerenciamento de patches e muito mais

Recursos essenciais de EDR incluem visibilidade clara das ameaças, investigação simples e resposta guiada e direta, repelindo rapidamente os ataques gastando poucos recursos



### Como funciona

Aprimora a visibilidade e visualização de ameaças

Simplifica a análise da causa principal

Entrega uma resposta rápida, centralizada e automatizada

Console na nuvem ou local



### Valor comercial

Protege seu negócio de ameaças evasivas perigosas e melhora sua postura de cibersegurança com uma única solução

Permite que equipes de TI ou de segurança de TI trabalhem de forma mais eficaz sem precisar equilibrar várias ferramentas e consoles

Automatiza uma vasta gama de processos para evitar a dependência de processos tradicionais de remediação que possam resultar em tempo de inatividade

Facilita a monitoração, detecção e investigação de ameaças, assim como a resposta e prevenção de ataques



### Para quem isso é melhor

Empresas com uma equipe interna de segurança de TI (ou apenas um a três especialistas em segurança) que necessitam de visibilidade granular de endpoints e resposta automatizada para reduzir tarefas de manipulação manual

## O que você recebe?



### Proteção de endpoints

Antivírus de arquivos, de web e de e-mail, proteção de rede, detecção de comportamento, remediação, prevenção de exploits, HIPS, AMSI, anti-cryptor, prevenção de ataque BadUSB



### Gerenciamento de segurança

Controle de firewall, da web, de dispositivo e de aplicativos, controle adaptativo de anomalias, monitoramento de integridade de arquivos, inspeção de registros, monitoramento de integridade do sistema



### Proteção e gerenciamento de dispositivos móveis

Proteção, controle e gerenciamento, iOS MDM



### Cenários de TI

Avaliação da vulnerabilidade, gerenciamento de patches, limpeza de dados, inventário de software/hardware, instalação de aplicativos de terceiros e sistema operacional, conexão remota



### Criptografia

Criptografia e gerenciamento de criptografia



### Proteção na nuvem

Descoberta na nuvem e bloqueio, descoberta de dados, segurança para MS O365



### Educação

Treinamento em cibersegurança para administradores de TI



### Recursos de EDR

Análise da causa raiz, verificação de IoC, clique único e resposta automatizada, orientação de resposta

**Kaspersky Next EDR Optimum** ajuda as organizações a aumentar sua segurança de acordo com seus ambientes de TI

## E se você já estiver usando a segurança da Kaspersky?

À medida que as empresas se desenvolvem e suas necessidades de TI aumentam em complexidade, suas necessidades de segurança também crescem e se diversificam. Kaspersky Next EDR Optimum ajuda as organizações a aumentar sua segurança em conjunto com seus ambientes de TI, começando a desenvolver processos e experiência de resposta a incidentes e a combater as ameaças avançadas que vêm com uma superfície de ataque expandida. Isso permite que os ataques sejam detectados, analisados e abordados de forma rápida e automática, reduzindo significativamente seu impacto.

### Sua solução da Kaspersky



**Kaspersky Endpoint Security Cloud Pro**



**Kaspersky Endpoint Security for Business Advanced**



**Kaspersky Total Security for Business**



**Kaspersky Endpoint Detection and Response Optimum**

### Migração recomendada



**Kaspersky Next EDR Optimum**



**Kaspersky Next EDR Optimum**



**Kaspersky Next EDR Optimum**

### Mais benefícios pra você

- Monitoramento de integridade de arquivos
- Inspeção de logs
- Monitoramento de integridade de sistemas
- Inventário de software/hardware
- Instalação de aplicativos terceiros
- Instalação de SO no local
- Capacidade de usar o console empresarial localmente ou na nuvem (visualização Expert)
- Opção de console simples na nuvem
- Funcionalidade EDR essencial, incluindo análise de causa raiz, verificação de IoC e resposta automatizada
- Treinamento em cibersegurança para administradores de TI
- Cloud Discovery e bloqueio
- Data Discovery
- Segurança para MS Office 365
- Opção de console simples na nuvem
- Treinamento em cibersegurança para administradores de TI
- Cloud Discovery e bloqueio
- Data Discovery
- Segurança para MS Office 365

### Saiba mais sobre o [Kaspersky Next EDR Optimum](#)



**Kaspersky Next EDR Optimum**



**Kaspersky Next EDR Foundations**

Saiba mais



**Kaspersky Next XDR Expert**

Saiba mais

Notícias sobre ciberameaças: [securelist.com](https://securelist.com)  
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**

© 2024 AO Kaspersky Lab. As marcas registradas e de serviço pertencem aos seus respectivos proprietários.

Saiba mais sobre o Kaspersky Next em:  
<https://go.kaspersky.com/next>

Escolha o nível que melhor se adequa a você e responda a uma breve pesquisa em nossa ferramenta interativa:  
[https://go.kaspersky.com/Kaspersky\\_Next\\_Tool](https://go.kaspersky.com/Kaspersky_Next_Tool)

