

# Kaspersky Anti Targeted Attack Platform

Os cibercriminosos de hoje se especializam na criação de métodos únicos e inovadores de invasão e comprometimento de sistemas. Conforme as ameaças continuam a evoluir e se tornar mais sofisticadas e devastadoras, a rápida detecção e a resposta mais ágil e adequada se tornaram essenciais.

É essencial que as empresas continuem repensando suas defesas de segurança de TI

para se manter um passo à frente das taxas cada vez maiores de ameaças virtuais e limitar as possíveis perdas financeiras geradas.

### Kaspersky Anti Targeted Attack Platform:

- **REDUZ** o tempo necessário para identificar e responder a ameaças
- **SIMPLIFICA** a análise de ameaças e resposta a incidentes
- **AJUDA** a eliminar falhas de segurança e a reduzir o "tempo de espera de ataques
- **AUTOMATIZA** tarefas manuais durante a detecção e resposta a ameaças
- **LIBERA** profissionais de segurança de TI para outras tarefas cruciais
- **SUPORTE** para compliance normativo total

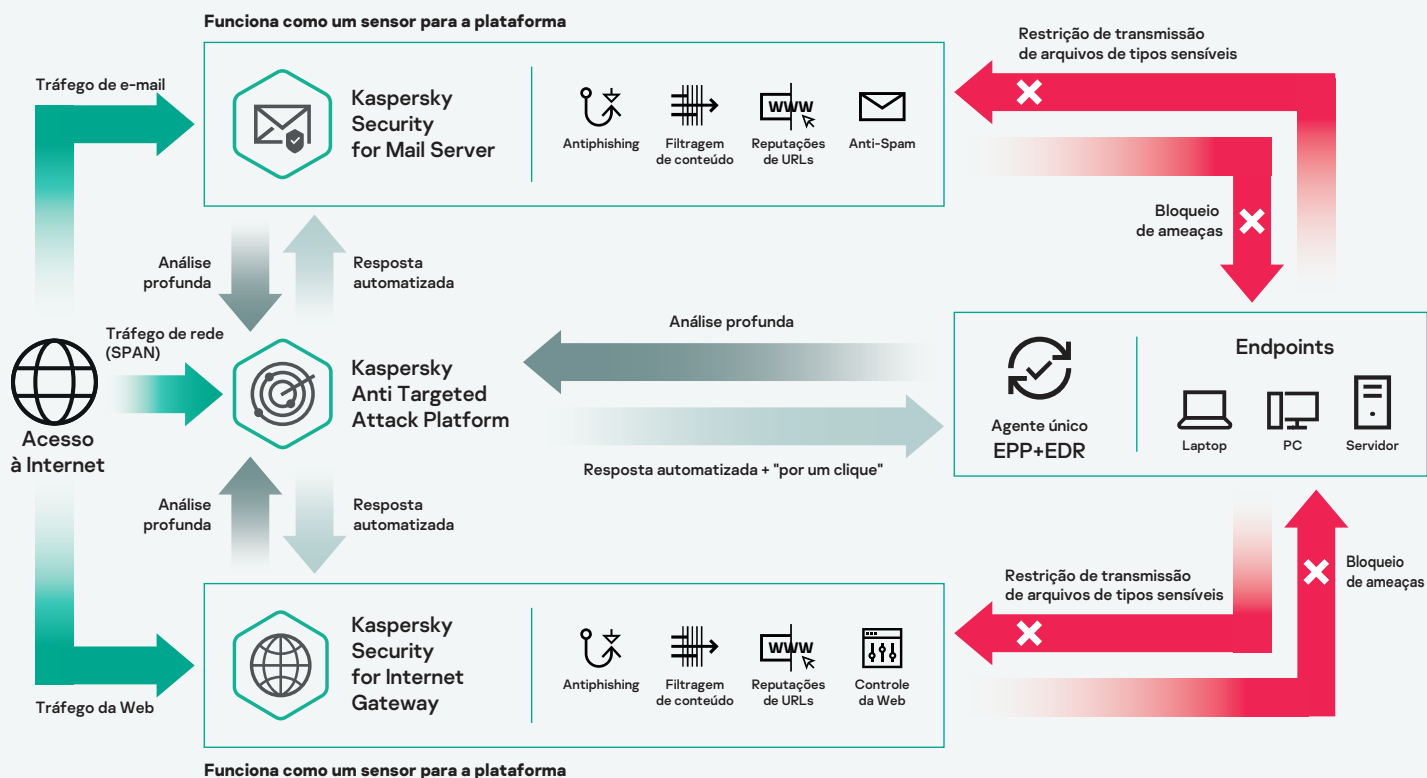
## Cibersegurança inigualável em uma solução unificada

Os criminosos virtuais profissionais de hoje preferem uma abordagem multivetorial. A Kaspersky Anti Targeted Attack Platform combina recursos de EDR e descoberta avançada de ameaças em nível de rede enquanto proporciona aos especialistas de segurança todas as ferramentas que precisam para cuidar de descoberta superior de ameaças multidimensionais, aplicar tecnologias de ponta, realizar investigações eficientes, buscar ameaças de forma proativa e oferecer uma resposta ágil e centralizada - tudo isso por meio de uma única solução.

## Os ataques mais sofisticados sob seu foco e controle

A plataforma atua como uma solução de resposta e detecção estendida, proporcionando proteção APT completa por nossa inteligência de ameaças e mapeada para a estrutura MITRE ATT&CK. Todos os possíveis pontos de entrada de ameaças (rede, Web, e-mail, computadores, notebooks, servidores e máquinas virtuais) estão sob seu controle.

A Kaspersky Anti Targeted Attack Platform é totalmente integrada com o Kaspersky Endpoint Security for Business, compartilhando um agente único com o Kaspersky EDR. Ela também se integra com o Kaspersky Security for Mail Server e o Kaspersky Security for Internet Gateway, atuando como um sensor para a plataforma e garantindo uma resposta automatizada para ameaças mais complexas oriundas da Web e de e-mails.



## Uma solução de segurança confiável que assegura total privacidade

Todas as análises de objetos são realizadas no local, sem fluxo de saída de dados, e o Kaspersky Private Security Network fornece atualizações de reputação recebidas em tempo real, preservando simultaneamente o total isolamento dos dados corporativos.

### Uma plataforma unificada para acelerar a inovação em transformação digital através de:

- **Continuidade de negócios integral** Pensamos na segurança e compliance de novos processos desde o início
- **Visibilidade completa** da sua infraestrutura de TI corporativa
- **Flexibilidade máxima** possibilitando a implantação em ambientes virtuais e físicos, sempre que visibilidade e controle forem necessários
- **Automação de tarefas de resposta e descoberta de ameaças**, otimizando o custo-benefício de suas equipes de segurança, resposta de incidentes e SOC
- **Integração descomplicada e avançada** com produtos de segurança atuais, aprimorando os níveis gerais de segurança e protegendo o investimento de segurança de legado

## Principais recursos:



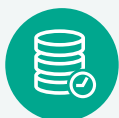
**Arquitetura de sensores em múltiplas camadas** – visibilidade completa através de uma combinação de rede, sensores da Web e e-mails e agentes de endpoint.



**Amplos mecanismos de detecção de ameaças** – trabalhando com dados de sensores de rede (análise de tráfego de rede) e agentes de endpoints (capacidades de EDR) para rápidos vereditos e menos falso-positivos.



**Área restrita avançada** – proporciona um ambiente seguro para análise profunda de atividade de ameaças, apoiando a randomização de componentes de SO, aceleração de tempo em máquinas virtuais, técnicas contra evasão, simulação de atividade de usuário e mapeamento de resultados para a base de conhecimento MITRE ATT&CK - tudo isso contribuindo para detecção altamente eficiente baseada em comportamentos.



**Análise retrospectiva** – mesmo em simulação onde endpoints afetados são inacessíveis ou dados foram criptografados – através de dados automatizados, coleta de objetos e veredito e armazenamento centralizado.



**Dois modos de interação de inteligência de ameaças** – comparação automatizada com dados de reputação globais do Kaspersky Security Network e as consultas de investigação e busca manual de ameaças do Kaspersky Threat Intelligence Portal.



**Busca de ameaças automática e em tempo real** – eventos são correlacionados com um conjunto único de indicadores de ataque (IoAs) gerados pelos caçadores de ameaças Kaspersky e mapeados para a matriz MITRE ATT&CK, proporcionando descrições de eventos claras, exemplos e recomendações de respostas.



**Busca proativa de ameaças com desenvolvedor flexível e poderoso de consultas** – analistas podem desenvolver consultas complexas para procurar comportamento atípico e atividades suspeitas, além de ameaças específicas para sua infraestrutura.

## Resumindo

Proteção de dados confiável, segurança da infraestrutura de TI, estabilidade para processos de negócios e conformidade atualmente são pré-requisitos para o desenvolvimento corporativo sustentável.

A Kaspersky Anti Targeted Attack Platform ajuda uma organização amadurecida em segurança de TI como a sua a criar defesas confiáveis que protegem a infraestrutura corporativa contra ameaças semelhantes a APT e ataques direcionados e suportam a conformidade regulamentar, sem exigir recursos adicionais de segurança de TI. Incidentes complexos são rapidamente identificados, investigados e respondidos, o que aumenta a eficiência da equipe de segurança de TI ou SOC, aliviando-os de tarefas manuais, graças a uma solução unificada que maximiza o uso da automação e a qualidade dos resultados.

# Consagrado como a solução mais eficaz da indústria



A SE Labs testou a Kaspersky Anti Targeted Attack Platform em um conjunto de ataques de hackeamento e nos concedeu a classificação AAA.



No teste independente "ICSA Labs: Defesa avançada de ameaças (3º trimestre de 2019)", a Kaspersky Anti Targeted Attack Platform atingiu **taxas de detecção de 100%, sem falso-positivos.**



THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

Radicati Group reconhece Kaspersky como **um dos principais nomes em seu teste de Proteção de Ameaças Avançadas e Persistentes (APT) – Market Quadrant 2020.**



## Escolha de Soluções de EDR 2020 da Gartner Peer Insights Customers coloca Kaspersky como principal fornecedora

Como uma das únicas 6 fornecedoras a ser reconhecida na Gartner Peer Insights Customers' Choice para soluções de EDR em 2020 – a honraria máxima para nossa solução ampliada de EDR – a Kaspersky Anti Targeted Attack Platform com o Kaspersky EDR em seu núcleo.

### Isenção de responsabilidade da Gartner

O Gartner Peer Insights Customer' Choice constitui opiniões subjetivas de análises, classificações e dados individuais do usuário final aplicados em relação a uma metodologia documentada; eles não representam as visões, nem constituem um endosso por parte, da Gartner ou de suas afiliadas.

## MITRE | ATT&CK®

### Qualidade de detecção confirmada pela avaliação MITRE ATT&CK

O elemento principal do Kaspersky Anti Targeted Attack Platform – o Kaspersky EDR – participou da MITRE Evaluation Round 2 (APT29) e demonstrou altos níveis de desempenho na detecção das principais técnicas de ATT&CK aplicadas em etapas cruciais dos ataques direcionados de hoje.

Saiba mais em [kaspersky.com/MITRE](https://kaspersky.com/MITRE)

Para conhecer melhor a Kaspersky Anti Targeted Attack Platform, acesse:

[kaspersky.com/enterprise-security/anti-targeted-attack-platform](https://kaspersky.com/enterprise-security/anti-targeted-attack-platform)

Notícias sobre ameaças virtuais: [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 empresas: [kaspersky.com.br/enterprise](https://kaspersky.com.br/enterprise)

[www.kaspersky.com](https://www.kaspersky.com)

© 2020 AO Kaspersky Lab.  
As marcas registradas e marcas de serviço pertencem aos seus respectivos proprietários.



Somos comprovados. Somos independentes. Somos transparentes. Estamos empenhados em construir um mundo mais seguro, onde a tecnologia melhora as nossas vidas. É por isso que criamos soluções de segurança. Para que todas as pessoas, em todos os lugares, possam aproveitar as infinitas oportunidades que a tecnologia oferece. Leve a segurança virtual para um amanhã mais seguro.

Saiba mais em [kaspersky.com.br/transparency](https://kaspersky.com.br/transparency)



**Proven.  
Transparent.  
Independent.**