Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

Criminosos virtuais estão se tornando cada vez mais sofisticados e capazes de burlar a proteção existente com sucesso. Todas as áreas dos seus negócios podem ser expostas a riscos, afetando processos críticos de negócios, afetando a produtividade e elevando os custos operacionais.

Com o Kaspersky EDR, sua organização pode:

- **MONITOR** ameaças com eficiência - muito além do malware
- **DETECTAR** ameaças com efetividade - graças às tecnologias avançadas
- **AGREGAR** dados brutos e vereditos de forma central
- **RESPONDER** rapidamente a ataques
- **EVITAR** ações maliciosas por ameaças descobertas

...tudo isso com uma interface da Web intuitiva que facilita investigar e reagir

Kaspersky EDR e as principais ligações do relatório Endpoint Security 2020 da IDC*

Uma solução de EPP fraca pode destruir o valor de uma ferramenta EDR

A Kaspersky oferece defesas de endpoint poderosas e completas (EPP+EDR) através de um único agente

Desta forma, as pessoas e o tempo se tornarão a nova base para medição de retorno em investimento para as ferramentas EDR

A Kaspersky aplica altos níveis de automação para problemas complexos, devolvendo tempo valioso aos seus especialistas em segurança

O EDR precisa aproveitar dados que estão fora de endpoints

A Kaspersky eleva a eficiência de EDR ao adicionar visibilidade e descoberta avançadas de ameaças baseada na Web e em e-mails através de uma só ferramenta

Turbine suas defesas de endpoint primeiro

Para criminosos virtuais, os endpoints corporativos, onde dados, usuários e sistemas corporativos se unem para gerar e implementar processos de negócio, continuam sendo o principal alvo. Para proteger seus endpoints corporativos e evitar que eles sejam usados como pontos de entrada para sua infraestrutura, sua equipe de segurança de TI deve buscar aprimorar a segurança já implementada. A implementação do ciclo completo de proteção de endpoints, desde o bloqueio automático de ameaças comuns até a rapidez e a proatividade na resposta a incidentes complexos, exige que as tecnologias preventivas sejam complementadas com recursos de defesa avançados.

O Kaspersky Endpoint Detection and Response (EDR) fornece segurança poderosa com visibilidade abrangente de todos os endpoints na rede corporativa juntamente com defesas superiores, possibilitando, assim, a automatização de tarefas rotineiras para descobrir, priorizar, investigar e neutralizar ameaças complexas e ataques como os de APT.

Destaques

- O Kaspersky EDR aprimora a nosso principal, mais testada e premiada plataforma de proteção de endpoint (EPP) – **o Kaspersky Endpoint Security for Business** – com recursos poderosos de EDR, elevando ainda mais seus níveis gerais de segurança. O uso de um único agente que forneça proteção automática contra ameaças comuns e defesas avançadas contra ataques complexos simplifica o tratamento de incidentes e minimiza os requisitos de manutenção. Não há sobrecarga adicional nos endpoints e sem novos custos, o que permanece é a informação de que seus servidores e estações de trabalho estarão totalmente protegidos contra as ameaças mais sofisticadas e direcionadas.
- O Kaspersky EDR reduz o tempo necessário para coleta inicial de evidências, oferece análise completa de telemetria e maximiza a automação de processos de EDR, diminuindo tempos gerais de resposta a incidentes sem a necessidade de atrair recursos adicionais de segurança de TI.
- O Kaspersky EDR pode ser absorvido para a **Kaspersky Anti Targeted Attack Platform**, combinando recursos de EDR e descoberta avançada de ameaças a nível de rede. Os especialistas de segurança de TI têm todas as ferramentas necessárias para tratar a descoberta de ameaças multidimensionais de alto nível, tanto no nível de rede quanto no de endpoint, aplicando tecnologia avançada, empregando investigações eficazes e proporcionando uma rápida resposta centralizada. Tudo isso em uma única solução.

* IDC PERSPECTIVE, Endpoint Security 2020:
O Ressurgimento do EPP e o Destino Manifesto do EDR

O Kaspersky EDR é ideal se a sua organização busca:

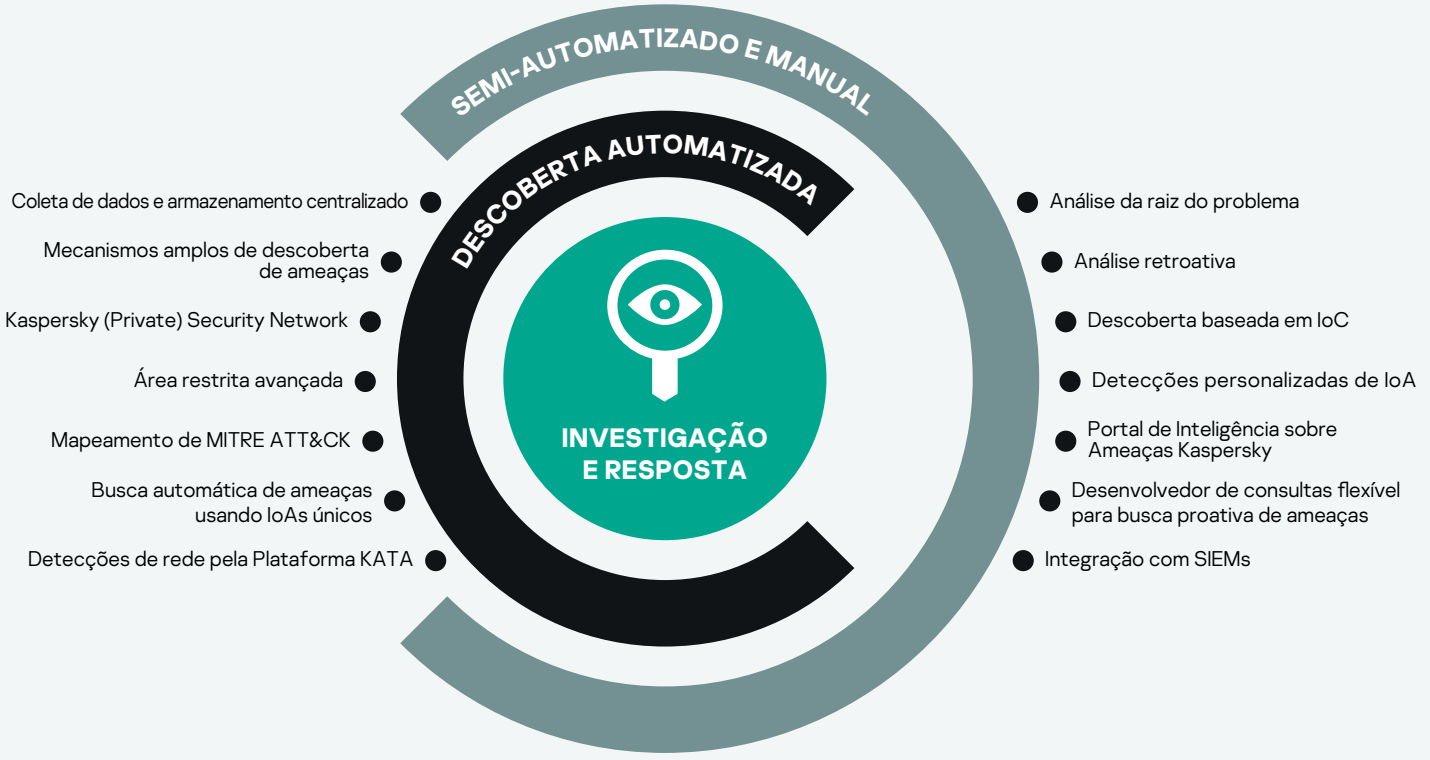
- Modernizar sua segurança com uma solução empresarial descomplicada para resposta a incidentes
- Automatizar respostas e identificação de ameaças - sem interrupção de negócios durante as investigações
- Melhorar a sua visibilidade de endpoints e detecção de ameaças através de tecnologias avançadas
- Entender as táticas, técnicas e procedimentos (TTPs) específicos empregados por criminosos para alcançar seus objetivos, possibilitando defesas e alocação de recursos de segurança com maior eficiência
- Definir maior unificação e efetividade de detecção de ameaças, gestão de incidentes e processos de resposta
- Aumentar a eficiência do seu SOC interno: não desperdice o tempo dele analisando logs de endpoint irrelevantes
- Auxiliar na conformidade reforçando logs de endpoint, avaliações de alertas e documentação de resultados de investigação

Detectar e conter rapidamente as ameaças mais sofisticadas

O Kaspersky EDR oferece proteção de endpoint de alto nível e aumenta a eficiência de SOC, proporcionando descoberta avançada de ameaças e acesso a dados prospectivos mesmo em situações nas quais os endpoints comprometidos estão inacessíveis ou os dados foram criptografados durante um ataque. Recursos aprimorados de investigação através de nossos indicadores de ataque (IoAs) únicos, aprimoramento de ATT&CK MITRE e um desenvolvedor de consultas flexível, além de acesso à nossa base de conhecimento do Portal de Inteligência de Ameaças - tudo isso facilita a detecção efetiva de ameaças e a rápida resposta a incidentes, limitando e evitando danos.

Casos de uso:

- **Busca proativa de evidência de intrusos em toda a sua rede**
- **Rápida detecção e remediação de um intruso - antes que ele possa causar grandes danos e interrupções**
- **Rápida investigação e gestão centralizada de incidentes em milhares de endpoints com um fluxo de trabalho integrado**
- **Validação de alertas e incidentes em potencial descobertos por outras soluções de segurança**
- **Automatização de operações de rotina - a fim de ajudar a minimizar tarefas manuais, liberar seus recursos e reduzir a probabilidade de uma "sobrecarga de alertas"**



Gartner peerinsights customers' choice 2020™

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

A Kaspersky foi uma das únicas 6 fornecedoras mundiais a receber o reconhecimento Gartner Peer Insights Customers para solução de Detecção e Resposta de Endpoints (EDR) em 2020, com a maior classificação de qualquer fornecedor para nosso serviço e suporte - a maioria honraria que os clientes poderiam conceder ao Kaspersky EDR.

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

Reconhecendo a importância da análise de táticas, técnicas e procedimentos (TTPs) na investigação de incidentes complexos e do papel da MITRE ATT&CK no mercado de segurança atual:

- O Kaspersky EDR participou da MITRE Evaluation Round2 (APT29) e demonstrou um alto nível de desempenho na detecção das principais técnicas de ATT&CK do escopo Round2 aplicado em etapas cruciais dos ataques direcionados de hoje.
- As detecções do Kaspersky EDR são aprimoradas com dados do banco de conhecimento MITRE ATT&CK, para análise profunda de TTPs adversários.

Saiba mais em kaspersky.com/MITRE

Benefícios empresariais do Kaspersky EDR na organização:

- Ajuda a eliminar falhas de segurança e a reduzir o "tempo de espera de ataques
- Automatiza tarefas manuais durante a detecçãoe resposta a ameaças
- Libera TI e profissionais de segurança de TI para outras tarefas cruciais
- Simplifica a análise de ameaças e resposta a incidentes
- Reduz o tempo necessário para identificar e responder a ameaças
- Ajuda a possibilitar a conformidade integral

E, se você quiser ir além: Kaspersky Managed Detection and Response

Adicionar defesas totalmente gerenciadas, contínuas e personalizadas individualmente ao Kaspersky EDR significa que seus recursos de segurança de TI podem ser conservados ao descarregar tarefas de processamento relacionadas a incidentes à Kaspersky, ou nos contatando para avaliações especialistas e expertise na detecção de ameaças únicas quando sua equipe interna não possuir especialistas em segurança suficientemente qualificados para cuidar das situações específicas.

Para conhecer melhor o Kaspersky EDR, acesse:

kaspersky.com/enterprise-security/endpoint-detection-response-edr

Notícias sobre ameaças virtuais: securelist.com
Notícias sobre segurança de TI: business.kaspersky.com
Segurança de TI para PMEs: kaspersky.com.br/business
Segurança de TI para empresas: kaspersky.com.br/enterprise

www.kaspersky.com

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

Proven. Transparent. Independent.