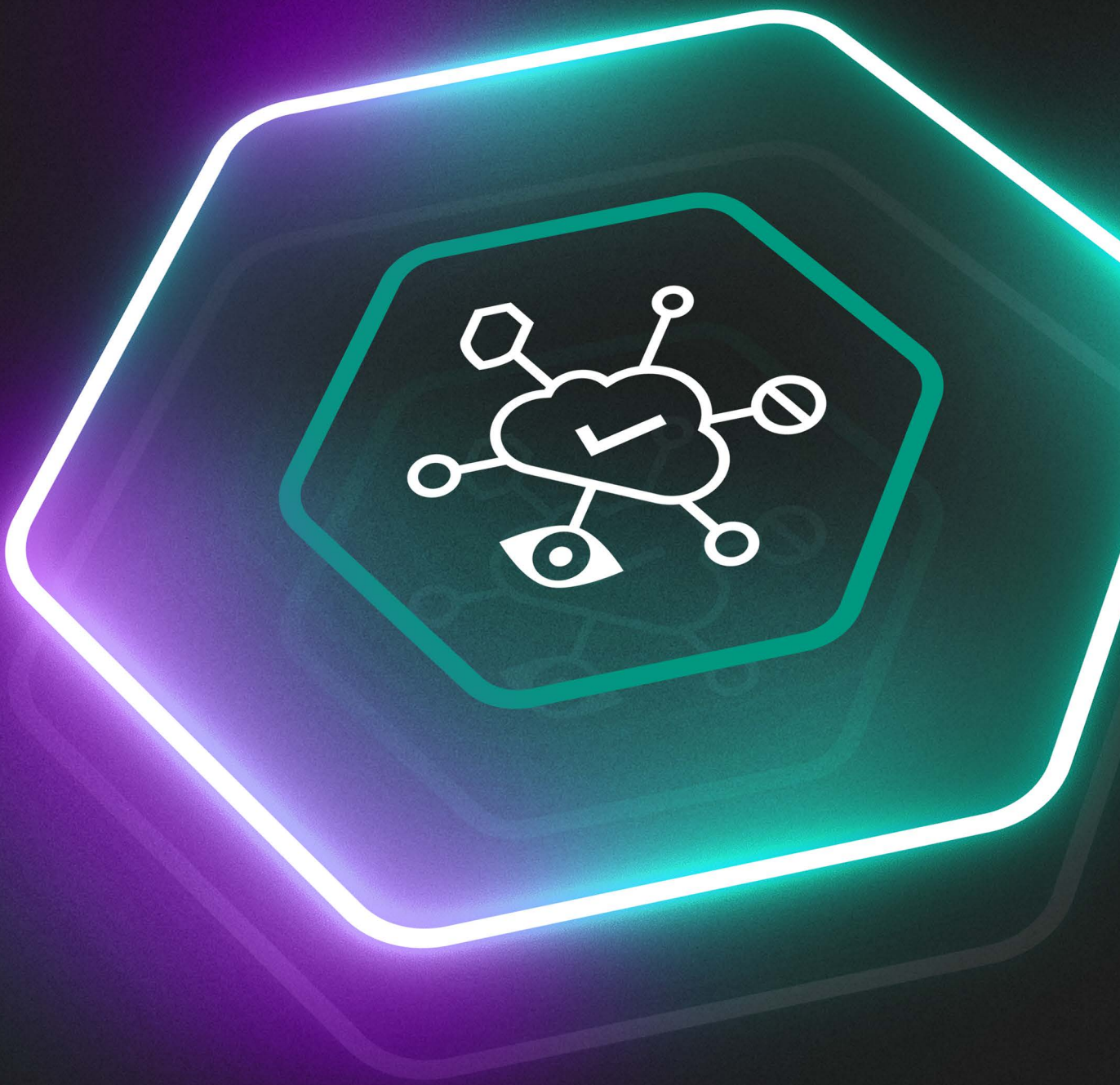

Kaspersky Endpoint Detection and Response

Expert

kaspersky BRING ON THE FUTURE

Uma única solução

O Kaspersky EDR Expert é uma solução única que pode ser gerenciada a partir de uma plataforma de gerenciamento central com base na nuvem e um console off-line em ambientes dispersos.

Kaspersky Endpoint Detection and Response Expert

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.

Primeiro, turbine suas defesas de endpoint

Os endpoints corporativos são onde dados, usuários e sistemas empresariais se unem para gerar e implementar processos corporativos. Esses endpoints continuam sendo o alvo principal para os criminosos virtuais.

O Kaspersky Endpoint Detection and Response (EDR) Expert fornece visibilidade abrangente de todos os endpoints na sua rede corporativa, além de defesas superiores, possibilitando, assim, a automação de tarefas rotineiras de EDR para descobrir rapidamente, priorizar, investigar e neutralizar ameaças complexas e ataques como os de APT.

Desafios atuais

As equipes de segurança de TI não têm a visibilidade e a transparência necessárias para monitorar os endpoints com eficiência. A detecção de um incidente pode levar semanas ou até meses a mais do que deveria, simplesmente porque ele é muito difícil de ser visto e entender exatamente o que aconteceu, como aconteceu e como corrigi-lo.

Ineficiência. Forçando os analistas a trabalhar entre múltiplos consoles descentralizados torna tudo lento e também cria oportunidades para erro humano. E o mesmo serve para quando obrigam profissionais de segurança de TI a operar manualmente processos de detecção rotineiros.

Ausência de inteligência relevante. A inabilidade de operacionalizar a inteligência de ameaças e a falta da visão clara das táticas, técnicas e procedimentos do adversário que podem dificultar a priorização de alertas e a investigação e resposta adicional.

Com o Kaspersky EDR Expert, sua organização pode

1 Controlar e monitorar de forma eficaz todos os seus endpoints

Ao ser capaz de ver o quadro completo, de onde a ameaça foi originada, como ela se espalhou, quais hosts ela afetou, e o que exatamente poderia e deveria ser feito para prevenir as consequências.

2 Racionalizar o trabalho de sua equipe de TI

A rapidez e a precisão na contenção de ameaças e na solução de incidentes em todas as infraestruturas distribuídas são possibilitadas por meio de ações centralizadas e automatizadas, que ajudam a racionalizar o trabalho da sua equipe de segurança de TI. Diga adeus aos recursos adicionais de alto custo, ao tempo de inatividade dispendioso e à perda de produtividade.

3 Caçar e mitigar as ameaças com êxito e rapidez

Os dados originais e os vereditos são agregados centralmente e os recursos de investigação são aprimorados por meio de nossos indicadores exclusivos de ataque (IoAs), por meio do enriquecimento do MITRE ATT&CK e de um criador de consultas flexível, além do acesso à nossa base de conhecimentos do Portal de inteligência contra ataques. Tudo isso facilita significativamente a caça eficaz de ameaças e a rápida resposta aos incidentes, para a limitação e prevenção aos danos.

Desafios atuais

Problemas na investigação e resposta. Apenas entender que algo está acontecendo na infraestrutura e que a solução de segurança da informação detectou uma ameaça potencial não garante que as ações subsequentes serão eficazes. É importante ser capaz de responder à ameaça de forma eficaz em tempo real e ser capaz de investigar completamente o incidente para prevenir a recorrência.

Desperdício de recursos caros. Os analistas não podem focar completamente em ameaças complexas se eles são forçados a desperdiçar tempo tratando de alertas triviais que deveriam ser tratados automaticamente por uma solução de proteção de endpoint eficaz. Além de ser um desperdício de recursos, isso pode levar ao cansaço do analista e que importantes alertas não sejam percebidos entre todo o 'ruído'.

Com o Kaspersky EDR Expert, sua organização pode

4 Responder mais rápido e com maior eficiência.

Investigação guiada e uma resposta mais rápida e precisa que são cruciais para lidar com ataques complexos e do tipo APT. O Kaspersky EDR Expert fornece um fluxo de trabalho racional com o gerenciamento centralizado de incidentes e a investigação guiada entre todos os endpoints na rede corporativa.

5 Obter o valor máximo de sua solução e de seus especialistas

Não há razão para contratar analistas caros para trabalhar com sua solução EDR e seu EPP se você os deixa tratando de alertas que não requerem os conhecimentos deles. Nossas soluções de EDR são baseadas na nossa mais testada, mais premiada solução EPP, que trata automaticamente da ampla maioria de alertas e liberando os analistas para focar naqueles que realmente requerem sua atenção e especialização. Nossos produtos EPP e EDR trabalham juntos como uma solução única, através do mesmo agente de endpoint.

O Kaspersky EDR Expert é ideal se a sua organização busca:

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

O Kaspersky EDR Expert dá a você o poder de:

- **Detectar ameaças usando os melhores e mais avançados métodos. A determinação do perfil da atividade do agressor potencial é uma forma eficiente de deter atividades maliciosas em uma infraestrutura.**

O Kaspersky EDR Expert permite que indicadores de comprometimento centralizados **(IoC)** sejam carregados de fontes de dados de ameaça e oferece suporte à verificação de IoC programada automática, facilitando o trabalho dos analistas

Com o nosso mecanismo de indicadores de ataque **(IoA)**, o Kaspersky EDR Expert consegue descobrir ações suspeitas usando o conjunto único de IoAs gerado pelos caçadores de ameaças da Kaspersky, fornecendo recursos de busca de ameaças automática em tempo real

Para fornecer a você uma imagem mais precisa do que está acontecendo, um arquivo ou processo pode ser enviado ao **Sandbox** para análise comportamental, tanto manualmente quanto automaticamente

Detecções IoAs e Sandbox são mapeadas para **MITRE ATT&CK** para obter mais análises das táticas, técnicas e procedimentos do adversário. Eventos individuais na ramificação do incidente são enriquecidos com o contexto de conhecimento MITRE, incluindo a identificação das táticas usadas do MITRE definido e visualização do evento no gráfico do incidente

Recomendações de contra-ataque

A análise automática de todos os eventos de endpoint, correlacionada com os dados de inteligência adquiridos, proporciona a você evidentes descrições de eventos, exemplos e recomendações de contra-ataque.

- Investigar a causa do incidente e prevenir qualquer recorrência. O Kaspersky EDR Expert oferece proteção de endpoint de alto nível e aumenta a eficiência de seu SOC, proporcionando 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 IoAs únicos, aprimoramento de MITRE ATT&CK e um desenvolvedor de consultas flexível, além de acesso à nossa base de conhecimento do Portal de Inteligência de Ameaças - tudo facilita a detecção de ameaças e a rápida resposta a incidentes, limitando e evitando danos de maneira efetiva.
- Escolha uma opção de armazenamento de telemetria conveniente para perícia. Um banco de dados centralizado armazena telemetria de endpoint por 30 dias por padrão e objetos e vereditos sem limite de tempo, isso significa que a análise de perícia pode ser feita sem contar com a disponibilidade do endpoint. Se você perceber que precisa de mais tempo de retenção de telemetria, isso pode ser aumentado para 60 ou 90 dias. Nas instalações locais, cabe a você determinar o período de armazenamento de dados, dependendo da capacidade e características do seu hardware.
- Responda da maneira que é melhor para você. Seus especialistas de segurança de TI estão equipados com ferramentas que permitem responder com um clique através do console de gerenciamento central, reduzindo o número de tarefas manuais, e diminuindo o tempo de resposta de horas para minutos.
- Trabalhe com tranquilidade e eficiência. A árvore de atividades do endpoint e as ferramentas de visualização com clique para baixo da árvore de eventos permitem que seus investigadores facilmente alcancem elementos de dados interessantes durante a avaliação de trajetória da ameaça ou se aprofundem para detalhes de mais informações. Vincular eventos e consolidar alertas ajuda a revelar o impacto completo de um ataque.

Como funciona?

Prêmios e reconhecimentos

Os produtos Kaspersky são avaliados regularmente por empresas globais de pesquisa, e a nossa capacidade de ajudar nossos clientes a se proteger contra ataques virtuais é amplamente reconhecida e comprovada. Nós somos os fornecedores de segurança virtual mais testados e premiados.

O Kaspersky Endpoint Detection and Response obtém maior classificação em testes no SE Labs

O Kaspersky EDR obteve a maior premiação AAA nos testes do SE Labs' Enterprise Advanced Security (anteriormente conhecido como Breach Response Test). A solução foi observada por sua habilidade de detectar ataques direcionados e complexos, por acompanhar o comportamento malicioso desde o início ao fim do ataque e por não gerar nenhum falso positivo. Durante a avaliação, o produto foi exposto às ferramentas, técnicas e procedimentos usadas por grupos de ameaças avançadas.

A Kaspersky foi considerada uma das principais atuantes em segurança de endpoints modernos para corporações e PEM pela IDC MarketScape

Para ajudar as organizações a avaliar as melhores plataformas de proteção de endpoint e as soluções de detecção e resposta de endpoint para suas necessidades, o IDC MarketScape avaliou dados submetidos por fornecedores MES entre abril e setembro de 2021, para posicionar as capacidades das empresas.

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.

Kaspersky Endpoint Detection and Response Expert

Saiba mais

www.kaspersky.com.br

Para saber mais sobre como o Kaspersky EDR Expert pode fortalecer sua equipe de segurança de TI, entre em contato!