Buscar, detectar e responder continuamente às ameaças que atacam sua empresa

Kaspersky Managed Detection and Response

kaspersky bring on the future

Desafios enfrentados pelas empresas

55%

das empresas relatam que seus dispositivos próprios foram infectados com malware*

20%

das empresas enfrentam ameaças de APT**

18%

dos entrevistados relatam que a causa dos incidentes em suas empresas foi a falta de pessoal qualificado em segurança cibernética***

US$ 2.5 bilhões

Perdas extremas resultantes de um ataque cibernético bem-sucedido****

Aumente a resiliência da sua segurança cibernética com proteção gerenciada 24 horas por dia

O trabalho remoto, o rápido desenvolvimento de métodos de troca de informações, a crescente lacuna global de competências e o número crescente de ameaças cibernéticas capazes de contornar os controles automatizados tradicionais de prevenção e detecção estão colocando organizações de todos os tamanhos sob uma pressão implacável. É essencial que elas possam responder de forma rápida e eficaz.

O Kaspersky Managed Detection and Response (MDR) é um serviço que oferece proteção gerenciada 24 horas por dia contra ameaças cibernéticas e ataques sofisticados que as medidas de segurança automatizadas tradicionais ignoram.

A solução aumenta o nível de segurança de TI para organizações de pequeno e médio porte com falta de conhecimento em segurança cibernética, fornecendo um serviço pronto para uso para implantação rápida. Para equipes experientes com conhecimento avançado em segurança cibernética, o serviço oferece flexibilidade adicional, permitindo a elas delegar tarefas de detecção e classificação de incidentes a especialistas da Kaspersky ou obter uma opinião profissional adicional sobre incidentes que elas próprias detectaram.

O Kaspersky MDR fortalece e melhora a resiliência das organizações contra ameaças cibernéticas, otimiza os recursos existentes e ajuda a utilizar de forma eficiente os recursos existentes, além de otimizar investimentos futuros em segurança de TI.

Recursos principais

- Monitoramento contínuo e caça a ameaças 24 horas por dia, 7 dias por semana
- Visão geral de todos os recursos protegidos com seus status atuais
- Resposta orientada e automatizada
- Acesso direto aos analistas do SOC da Kaspersky
- API REST para integração com IRP/SOAR
- Console Web com painéis e relatórios
- Armazenamento de telemetria bruta por 3 meses
- Enviar incidentes personalizados
- Armazenamento do histórico de incidentes de segurança por 1 ano

* Economia da Segurança de TI, 2022
** Relatório do Analista do Kaspersky MDR, 2023
*** Relatório Kaspersky Human Factor 360, 2023
**** Relatório de estabilidade financeira global. A Última Milha: Vulnerabilidades e Riscos Financeiros, 2024

Fontes de telemetria e alertas para Kaspersky MDR

- **Kaspersky Endpoint Security for Windows**
- **Kaspersky Endpoint Security for macOS**
- **Kaspersky Endpoint Security for Linux**
- **Kaspersky Virtualization Light Agent**
- **Kaspersky Anti-Targeted Attack**

Como funciona

1

Os analistas do Kaspersky SOC investigam alertas de segurança e analisam proativamente eventos de telemetria recebidos de produtos Kaspersky instalados na rede do cliente. Esta telemetria está correlacionada à inteligência de ameaças cibernéticas da Kaspersky – baseada em mais de 25 anos de experiência na investigação de alguns dos ataques cibernéticos e campanhas direcionadas mais notórios do mundo – para identificar táticas, técnicas e procedimentos conhecidos, novos e emergentes utilizados pelos agressores. IoAs exclusivos permitem a detecção de ameaças ocultas sem malware que imitam atividades legítimas.

2

Como parte do processo de tratamento de eventos no Kaspersky MDR, mecanismos de inteligência artificial (IA) ajudam a reduzir o número de falsos positivos e a acelerar a investigação de incidentes pela equipe do SOC.

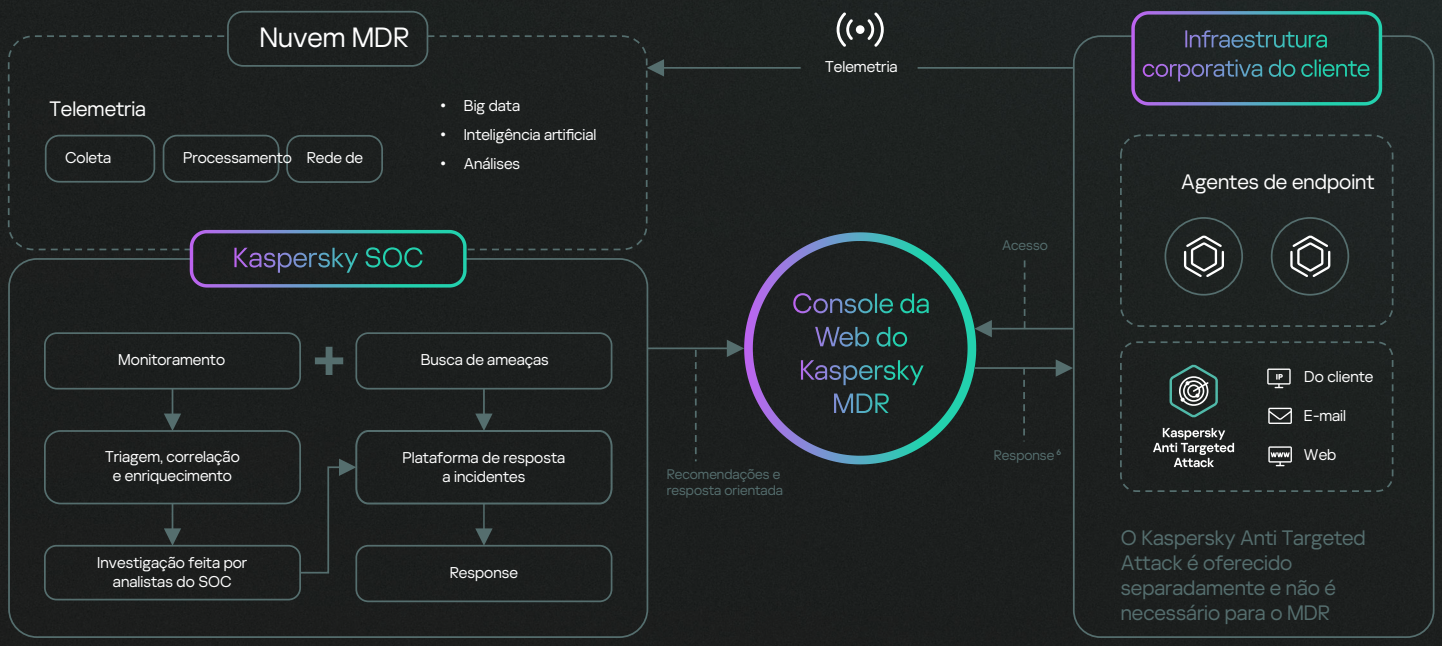
3

Quando uma ameaça potencial é detectada, o Kaspersky MDR a classifica por nível de gravidade e notifica o cliente por e-mail e/ou Telegram. Sempre que possível, a análise da causa raiz ajuda a identificar a origem do ataque e fornece recomendações sobre como conter, responder e mitigar as ameaças detectadas.

4

Os clientes podem optar por delegar parcial ou totalmente os recursos de resposta* à equipe do Kaspersky SOC. Quaisquer dúvidas relacionadas ao incidente podem ser discutidas via chat no console web do Kaspersky MDR.

Arquitetura do Kaspersky MDR



O Kaspersky MDR é compatível com soluções antivírus de terceiros. Iniciativas de resposta automatizadas quando o cliente as aprova no portal do Kaspersky MDR (se o cliente não o fizer, o portal MDR solicitará autorização antes que a resposta automatizada entre em ação).

* Se uma análise mais aprofundada do incidente for necessária e você tiver uma assinatura ativa do Kaspersky Incident Response, o incidente poderá ser entregue à equipe do Kaspersky GERT para investigação.

Propostas de valor

A tranquilidade conquistada graças à proteção contínua até mesmo contra as ameaças mais complexas e sofisticadas

Todos os principais benefícios de ter seu próprio SOC sem precisar ter trabalho nem arcar com as despesas de montar um

Custos de segurança reduzidos em geral – não há necessidade de contratar e treinar vários profissionais de segurança de TI caros para cobrir todas as bases

Reoriente seus recursos internos de segurança de TI para lidar com outras questões críticas para os negócios

Reconhecimento global e histórico incomparável

A Kaspersky participa de uma ampla variedade de testes independentes e trabalha em estreita colaboração com empresas líderes globais de análise. A Kaspersky é reconhecida mundialmente como líder em segurança cibernética, e o Kaspersky MDR, assim como todos os nossos produtos, recebeu vários prêmios. Os poderosos recursos de detecção e resposta do Kaspersky MDR são complementados pela experiência mundialmente reconhecida de uma das equipes de caça a ameaças mais bem-sucedidas e experientes do setor: a equipe altamente qualificada e experiente do Kaspersky SOC.

Kaspersky Managed Detection and Response

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture