kaspersky

Kaspersky
Managed Detection
and Response

Interrompemos os incidentes antes que eles interrompam seus negócios

O Kaspersky Managed Detection and Response é um serviço liderado por especialistas que oferece monitoramento, detecção, investigação e resposta rápida a ataques cibernéticos sofisticados 24 horas por dia, 7 dias por semana, complementando seus controles de segurança existentes com detecção conduzida por humanos e inteligência global contra ameaças. O serviço fortalece imediatamente sua postura de segurança de TI e TO, independentemente do tamanho ou do setor de atuação da sua organização.

Principais benefícios

Proteção avançada e contínua em toda a sua superfície de ataque (endpoints, rede, nuvem e muito mais) desde o primeiro dia.

Um SOC pronto para uso, disponível 24 horas por dia, 7 dias por semana com uma equipe global de especialistas para eliminar a necessidade de construir, contratar pessoal e manter suas próprias operações de segurança internas.

Uma carga de trabalho reduzida para sua equipe interna de segurança, já que você delega o monitoramento, a triagem e a investigação para nós.

Segurança orientada a resultados que combina conhecimento humano, inteligência contra ameaças e IA para impedir incidentes antes que eles afetem seus negócios.

Aumente a resiliência da sua cibersegurança com proteção gerenciada 24 horas por dia, 7 dias por semana

O trabalho remoto, o rápido crescimento da troca de informações digitais, a crescente lacuna global de competências e o número cada vez maior de ameaças cibernéticas capazes de contornar os controles automatizados tradicionais estão colocando organizações de todos os portes sob pressão constante. Nesse ambiente, responder de forma rápida e eficaz a cada incidente é obrigatório.

Uma visão geral das ameaças cibernéticas de hoje[1]

1 Vetores de ataque inicial

31% contas válidas

13% relação confiável

39% exploração de um aplicativo voltado para o público

2 Organizando o entorno

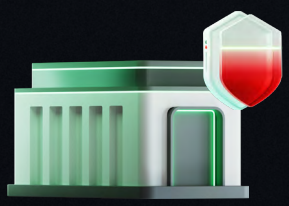
Os invasores muitas vezes usam ferramentas legítimas (como Mimikatz, PsExec, SoftPerfect Network Scanner) em infraestruturas que não contam com controles de configuração do sistema adequados.

3 Impacto

42% criptografia de arquivos

17% vazamento de dados

11% persistência instalada para impacto futuro



As evidências mostram que os invasores frequentemente retornam após um ataque bem-sucedido.

Duração do ataque

Rápido 45%	Moderado 20%	Duradouro 35%
até 1 dia	13 dias	253 dias

> O Kaspersky MDR detectou e interrompeu com sucesso um ataque de dia zero que, de outra forma, poderia ter causado graves problemas em nossas operações.

GTO Grandeza de México

Daniel Huerta Santos
Gerente de cibersegurança, Governo Estadual de Guanajuato

Saiba mais

1 Relatório do Kaspersky MDR and Incident Response

O que o MDR da Kaspersky oferece

Proteção contínua contra ameaças avançadas desde o primeiro dia

O Kaspersky MDR é ativado em minutos, sem necessidade de infraestrutura adicional, utilizando nossos analistas de SOC e inteligência contra ameaças para fornecer detecção em várias camadas em diversos domínios. Informado por bilhões de sinais de telemetria, ele permite a identificação proativa de ameaças, a investigação da causa raiz e a remediação completa e rápida, protegendo contra ameaças conhecidas e de dia zero desde o primeiro dia.

Operações de segurança lideradas por especialistas e aprimoradas por inteligência

Com o Kaspersky MDR, suas operações de segurança são gerenciadas por especialistas globais com vasta experiência prática e certificações líderes do setor. O trabalho deles é potencializado por mecanismos de Inteligência de Ameaças e IA líderes de mercado incorporados ao serviço, ajudando a enriquecer cada alerta, acelerar a detecção e reduzir o Tempo Médio de Resposta (MTTR).

Eficiência operacional e previsibilidade de custos

- O Kaspersky MDR elimina a complexidade e o custo de construir um SOC interno do zero, um processo que pode consumir seu orçamento e atrasar melhorias de segurança significativas por meses ou até anos.
- Se você já possui seu próprio SOC (Centro de Operações de Segurança), o serviço assume a responsabilidade pelo monitoramento 24 horas por dia, 7 dias por semana, triagem de alertas e classificação de incidentes, liberando seus analistas para se concentrarem em trabalhos estratégicos de maior valor agregado.

Casos de uso

- Proteção completa 24 horas por dia, 7 dias por semana, para organizações sem SecOps
- Gerenciamento conjunto de SecOps para reforçar as equipes internas de cibersegurança
- Proteção avançada para infraestrutura de TO
- Proteção contínua dedicada para sistemas incorporados

30 minutos
é nosso MTTR médio [2]

30%
de todos os alertas processados pelo AI Auto Analyst [1]

até 15 minutos
é o tempo necessário para ativar o Kaspersky MDR

até 2 anos
é o tempo necessário para montar operações de segurança internas do zero

70%
das equipes de segurança enfrentam dificuldades para acompanhar o número impressionante de alertas gerados por suas ferramentas de segurança [3]

Monitoramento

- Endpoints
- Networks
- Estações de trabalho de ICS
- Cloud
- Sistemas integrados

Compatibilidade com aplicativos EPP de terceiros

Detecção

Detecção multicamadas

- Tecnologias de detecção para endpoints
- Enriquecimento da inteligência de ameaças
- AI Auto Analyst
- Identificação proativa de ameaças

~30% de todos os alertas recebidos processados pelo AI Auto Analyst [1]

> 3 mil regras de detecção

Resposta a incidentes

30 minutos
Tempo médio para resposta*

Todos os modos de resposta

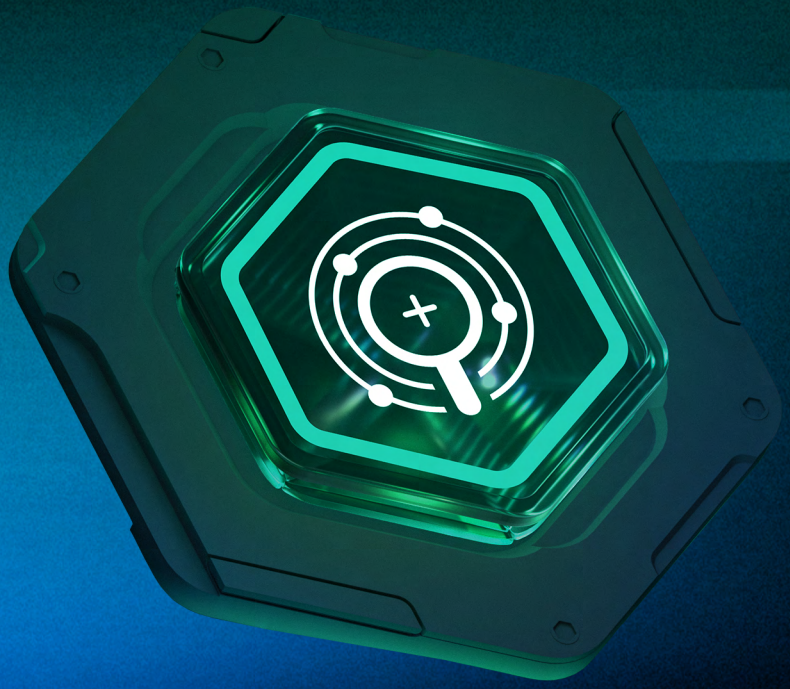
- Aprovação manual
- Pré-aprovada
- Recomendações

Analistas de segurança | Engenheiros de detecção | Profissionais de resposta a incidentes | Pesquisadores de ameaças | Engenharia reversa | Caçadores de ameaças | Analistas de Digital Footprint Intelligence | Engenheiros de automação de segurança | Analistas forenses

proteção 24/7 pelo Kaspersky SOC

2 De acordo com nossos relatórios anuais de analistas de MDR

3 Um retrato do profissional de segurança da informação moderno, 2024



Kaspersky Managed Detection and Response

Agende uma demonstração

www.kaspersky.com.br

#kaspersky
#bringonthefuture