kaspersky

EDR vs MDR vs XDR

EDR
Endpoint Detection and Response

Identifica ameaças novas, desconhecidas e evasivas que estão burlando a proteção de endpoint e automatiza as tarefas rotineiras de segurança

MDR
Managed Detection and Response

Entrega proteção contínua e gerenciada contra as mais complexas e avançadas ameaças sem malware

XDR
Extended Detection and Response

Detecta proativamente as ameaças complexas entre múltiplos níveis da infraestrutura e automaticamente responde e contra-ataca estas ameaças

Como funciona

- Permite a detecção avançada e a caça por ameaças que passam despercebidas pelos mecanismos de prevenção
- Aprimora a visibilidade e visualização de ameaças
- Simplifica a análise de causa raíz
- Entrega uma resposta centralizada e automatizada

- Coleta a telemetria dos produtos de segurança, analisa proativamente os metadados da atividade do sistema quanto a quaisquer sinais de um ataque ativo ou iminente, e fornece resposta gerenciada ou guiada

- Integra múltiplas ferramentas e aplicativos de segurança
- Monitora os dados nos endpoints, redes, nuvens, servidores da Web, servidores de correio eletrônico e etc, para assim detectar e eliminar ameaças complexas
- Simplifica o gerenciamento da segurança de informações através da interação automatizada entre produtos

Para quem é destinado?

- Empresas com uma equipe interna de segurança de TI que requerem uma visibilidade detalhada de enpoint e resposta centralizada, a fim de reduzir as tarefas rotineiras manuais

- Empresas que procuram expandir suas capacidades internas de segurança de TI livrando-se das tarefas de detecção principal e de resposta
- As organizações que talvez não possam ter o orçamento ou equipe de especialistas disponíveis para desenvolver seu próprio SOC interno

Organizações com uma segurança de TI já estabelecida que desejam ter uma plataforma única que forneça:

- Uma visão coerente de tudo o que acontece na sua infraestrutura
- Caça às ameaças e inteligência de ameaça incorporadas
- Priorização superior de incidentes e menos alertas de falsos positivos

Valor comercial

- Fornece a equipe de segurança de TI a visibilidade e o controle unificado de que eles precisam para caçar ativamente por ameaças ao invés de esperar por alertas
- Maximiza a capacidade existente das equipes de segurança de TI ao automatizar uma variedade de processos de análise, investigação e resposta
- Impulsiona a eficiência de custos ao permitir que as equipes de segurança de TI trabalhem mais eficazmente sem ter de lidar com múltiplas ferramentas e consoles

- Resolve a crise de talentos da segurança cibernética assegurando proteção instantânea contra ameaças complexas
- Permite a terceirização de processos de gerenciamento de incidentes para destinar melhor os recursos limitados e custosos internos nos resultados críticos fornecidos
- Reduz os custos gerais com a segurança, sem a necessidade de implementar soluções complexas e empregar uma gama de especialistas em segurança internos

- Fornece proteção abrangente contra o cenário de ameaças em evolução
- A abordagem do ecossistema maximiza a eficiência das ferramentas de segurança cibernética envolvidas, economiza recursos, e reduz risco
- Simplifica o trabalho dos especialistas de segurança de TI e os fornece o contexto adicional necessário para investigar ataques de multi-vetores
- Minimiza o MTTD e MTTR - crucial em combater ameaças complexas e ataques direcionados
- Permite a resposta centralizada e automatizada em todo o processo tecnológico de segurança

Se a sua organização for experiente em termos de cibersegurança e quiser se beneficiar das capacidades do XDR, dê uma olhada em

Kaspersky Expert Security

Saiba mais