AS MAIORES VANTAGENS DO XDR

As soluções XDR refletem a evolução contínua dos produtos de cibersegurança. De facto, o XDR é o culminar da evolução dos produtos de cibersegurança, indo muito além do âmbito dos produtos de deteção e resposta de endpoint (EDR) e de deteção e resposta gerida (MDR).

O XDR oferece visibilidade sobre toda a superfície de ataque, abrangendo tanto ambientes de cloud como locais. Com o XDR, as empresas obtêm deteção e proteção aprimoradas contra ameaças, fazendo determinações precisas e em tempo real com base em pontos de dados recolhidos e consolidados numa série de pontos de entrada de ameaças.

Aqui estão quatro dos maiores benefícios do XDR e o que eles significam para o seu negócio.

1. Resposta mais rápida a incidentes

O XDR ajuda as empresas a identificar e responder a ameaças mais rapidamente graças às suas capacidades analíticas avançadas.

O que isto significa para o seu negócio:

Previne a propagação de ameaças e minimiza o impacto

Reduz a possibilidade de perda de dados

Reduz o risco de danos à reputação

Mas quão mais rápido é o XDR? Consulte a tabela abaixo para descobrir.

Quanto tempo demora normalmente a resolução

	Sem XDR	Com XDR
Resolução típica de BEC (apenas gateway)	1 - 2 meses	1 - 2 horas
Resolução de roubo de identidade	3 - 4 semanas	1 - 2 horas
Resolução de infeções por malware	3 - 4 semanas	~ 1 hora
Resolução de ameaças internas	3 - 6 meses	~ 4 horas
Resolução de extorsão sem XDR	Variável	< 24 horas

2. Visibilidade melhorada no seu ambiente de segurança

O XDR reúne a telemetria de todos os seus sistemas de servidores, redes, cloud, email e pontos de extremidade num único painel, eliminando silos.

O que isto significa para o seu negócio:

Oferece supervisão completa da superfície de ataque

Ajuda a identificar vulnerabilidades ou configurações incorretas com mais facilidade

Simplifica a conformidade e a elaboração de relatórios graças a registos de auditoria mais claros

3. Deteção de ameaças mais inteligente

O XDR utiliza AI, análises avançadas e algoritmos de aprendizagem automática, que o ajudam a repelir ataques complexos e em várias fases que as ferramentas tradicionais muitas vezes não detetam. Pode interromper tanto ataques conhecidos como ameaças desconhecidas de zero-day. Também fornece informações contextuais em vez de alertas isolados, fornecendo detalhes sobre tipos e técnicas de ataque.

O que isto significa para o seu negócio:

Mantém-no à frente das táticas complexas dos atacantes

Reduz a fadiga de alertas ao automatizar a deteção

Proporciona uma melhor compreensão das táticas, técnicas e procedimentos (TTPs) dos atacantes

4. Custos de segurança mais baixos

Como o XDR simplifica os seus conjuntos de ferramentas e utiliza a automação, torna as suas operações de segurança mais eficientes e menos dispendiosas.

O que isto significa para o seu negócio:

Redução da duplicação de pagamentos para ferramentas de segurança

O orçamento é libertado para investir noutras áreas

O ROI do investimento em segurança é maximizado

Estes não são, de forma alguma, os únicos benefícios do XDR. Para saber mais sobre as vantagens do XDR e como funciona, descarregue o nosso livro eletrónico XDR explicado: Uma abordagem estratégica à gestão de ameaças.

Barracuda

Copyright © Barracuda Networks Inc. • pt.barracuda.com