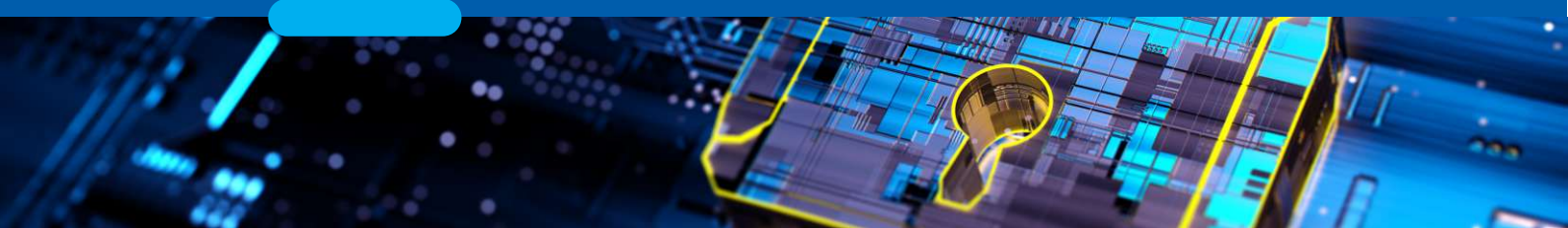

HUGHES®
An EchoStar Company

# POR QUE O SERVIÇO MDR PODE SER A SOLUÇÃO PERFEITA PARA SUA EMPRESA.



# INTRODUÇÃO

**Para pequenas e médias empresas que enfrentam ameaças cibernéticas críticas e persistentes com recursos e orçamento limitados, o serviço Hughes de Detecção e Resposta Gerenciada a ameaças cibernéticas (MDR) oferece um caminho para proteção.**

De acordo com o Relatório de investigações de violação de dados de 2021 da Verizon, **46% de todos os ataques cibernéticos afetam principalmente empresas com menos de 1.000 funcionários.** Sessenta e um por cento das pequenas e médias empresas (PME) foram alvo de um ataque cibernético em 2021. Conforme relatado pela Administração de Pequenas Empresas dos EUA, ocorreram mais de 700.000 ataques contra pequenas empresas, totalizando **US$2,8 trilhões em danos nesse mesmo ano.**

Por que as pequenas e médias empresas são alvos comuns? Porque muitas vezes faltam-lhes recursos, orçamento, experiência e pessoal para proteger adequadamente as suas redes – e os criminosos cibernéticos sabem disso. Eles sabem que, se forem suficientemente agressivos e persistentes nos seus ataques, provavelmente vencerão.

Felizmente, as pequenas e médias empresas não precisam agir sozinhas. **Os provedores de serviços de segurança gerenciados (MSSP) desenvolveram soluções, como recursos de detecção e resposta gerenciada (MDR), que são especificamente adaptadas para atender às necessidades exclusivas das pequenas e médias empresas.** O MDR fornece uma solução de segurança abrangente que combina tecnologia de ponta, analistas de segurança experientes e inteligência de ameaças em tempo real para detectar e responder a ameaças cibernéticas.

Neste e-book, exploramos detalhadamente as ofertas de MDR, incluindo o que é, como difere das soluções de segurança cibernéticas tradicionais, quais benefícios oferece, como pode ser implementado e o que o futuro reserva em termos de tendências e capacidades de MDR. **Com uma melhor compreensão de como o MDR oferece um caminho econômico para a proteção, uma PME pode determinar se ele pode ser adequado às suas necessidades de negócios.**

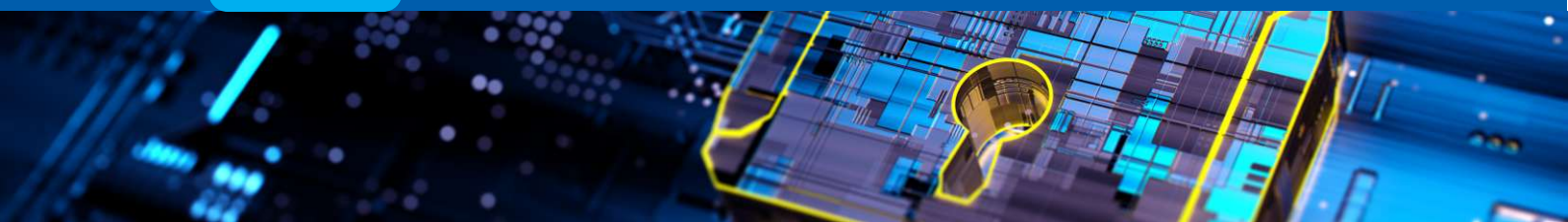
# O QUE É MDR?

## Então, o que é exatamente o serviço MDR e como ele difere das soluções de segurança tradicionais?

**O MDR é um serviço de segurança que combina recursos avançados de detecção e resposta a ameaças com serviços gerenciados, oferecendo uma solução de segurança mais completa e abrangente.** As soluções de segurança tradicionais, como firewalls, software antivírus e sistemas de detecção de intrusões, normalmente abordam apenas um único aspecto da segurança. As empresas devem, portanto, reunir proteção contra peças distintas e garantir que sejam mantidas atualizadas sobre as ameaças mais recentes, por meio de patches e atualizações.

## Por outro lado, o MDR proporciona uma abordagem proativa e integrada à segurança que é muito mais eficaz.

O MDR depende de tecnologias inovadoras, incluindo inteligência artificial (IA), aprendizado de máquina (ML) e inteligência de ameaças, para monitorar e analisar continuamente tráfego e eventos em busca de sinais de atividades maliciosas. Se uma ameaça for detectada, os analistas de segurança MDR investigam e respondem imediatamente à ameaça, minimizando o risco de uma violação e o impacto de um ataque. Ter as mais recentes tecnologias de detecção de ameaças, **juntamente com monitoramento e serviços gerenciados 24 horas por dia, 7 dias por semana, é o que abre o caminho para proteger a rede e os negócios.**



# A BASE DO MDR

**Gerenciamento de informações e eventos de segurança (SIEM):**
Coleta dados de log de eventos de diversas fontes para identificar atividades que se desviam da norma com análise em tempo real para realizar a ação de combate.

**Detecção e resposta de endpoint (EDR):**
Monitora continuamente os dispositivos dos usuários finais para identificar ameaças como ransomware e malware.

**Centro de Operações de Segurança (SOC) 24 horas por dia, 7 dias por semana:**
Oferece uma equipe operacional em tempo integral equipada com ferramentas e tecnologias para detecção e mitigação de ameaças em tempo real.

**Resposta a incidentes:**
Descreve os procedimentos formais para identificar, investigar e responder a ameaças potenciais para minimizar seu impacto.

**Monitoramento de Rede:**
Fornece visibilidade completa em tempo real, necessária para identificar indicadores precoces de comprometimento associados a um evento ativo de segurança cibernética.

# O PAPEL DO SOC NO MDR

Um aspecto relevante sobre MDR que é na maioria das vezes é proibitivo para as pequenas e médias empresas realizarem investimento na construção de um SOC dedicado com operações 24 horas por dia. Podem ser necessários milhões de dólares para criar um SOC e outros milhões em custos recorrentes anualmente para operá-lo. Mesmo recrutar, contratar e treinar uma equipe de segurança de TI costuma ter um custo muito proibitivo para pequenas e médias empresas.

**No entanto, com o MDR, as PMEs podem aproveitar as capacidades e serviços de um SOC sem investimentos volumosos.**

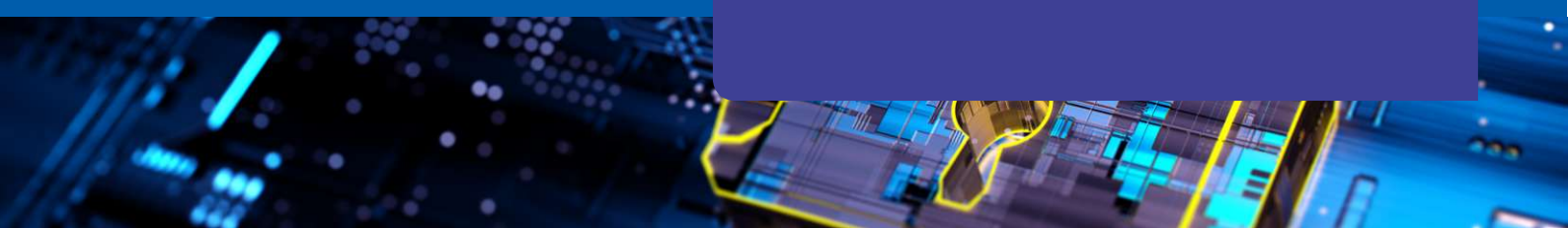
## Embora as equipes SOC possam ter configurações diferentes, a maioria inclui:

Analistas de segurança que atuam como socorristas de segurança cibernética. Eles estão na linha de frente, identificando e reportando ameaças e implementando mudanças para proteger a rede e a organização.

**Os engenheiros de segurança são os especialistas em software e hardware que implantam, mantêm e atualizam as ferramentas, tecnologias e sistemas envolvidos na segurança da infraestrutura crítica, bem como documentam os protocolos de segurança.**

Um gerente SOC dirige a equipe de analistas e engenheiros e orquestra quaisquer respostas às principais ameaças à segurança.

**Os provedores de MDR que oferecem Centro de Operações de Segurança como Serviço (SOCaaS) geralmente possuem recursos adicionais. Por exemplo, podem ter profissionais para estabelecer estratégias e políticas relacionadas com a segurança, gerir incidentes à medida que ocorrem e comunicar requisitos e ações no caso de uma violação significativa de dados. O MDR, portanto, fornece às PMEs acesso a profundo conhecimento e infraestrutura que, de outra forma, estariam fora de alcance por questões de investimento**



HUGHESCIBERSEGURANÇA

HUGHES
An EchoStar Company

# OS BENEFÍCIOS DO MDR

O MDR foi projetado para complementar as soluções de segurança existentes e integrar-se com firewalls, sistemas de detecção de intrusão e outras tecnologias de segurança existentes. Assim, o MDR preenche lacunas de segurança da rede e fornece uma solução mais abrangente. Para as pequenas e médias empresas, isso representa uma série de benefícios:

**Detecção proativa de ameaças em tempo real e recursos de resposta rápida que minimizam os riscos e impactos de um ataque.**

Tecnologias avançadas, como IA e ML, permitem que o MDR forneça uma abordagem mais eficaz para proteger a rede.

**Especialistas dedicados para proteger a empresa contra ameaças.**

Proteção acessível que elimina a necessidade de uma PME investir em seus próprios equipamentos, software e equipe de segurança caros.

**Capacidade de escalar para atender às necessidades de uma empresa à medida que ela cresce.**

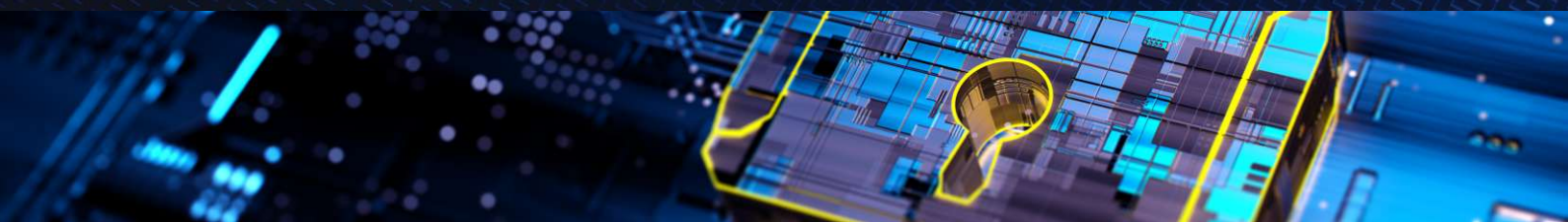
Tranquilidade em saber que os sistemas e dados estão protegidos!

**Embora a implementação do MDR exija planejamento e coordenação cuidadosos, a escolha do fornecedor certo pode permitir que a transição seja suave e contínua. Para a maioria das implementações, um provedor de MDR que:**

1. Avalie a postura de segurança atual da empresa, o que inclui a avaliação das tecnologias, processos e pessoal de segurança existentes.
2. Desenvolva um plano para delinear tecnologias, processos e pessoal específicos necessários para a implementação.
3. Instale e configure a tecnologia, incluindo a plataforma MDR, para proteger a rede e os dados da PME.
4. Treine o pessoal essencial da PME no uso da plataforma MDR e dos processos envolvidos na resposta a ameaças cibernéticas.
5. Monitore e mantenha os sistemas de segurança de rede para proteger as pequenas e médias empresas contra possíveis ameaças e ataques.

# O QUE O FUTURO NOS RESERVA?

Embora o MDR ofereça proteção robusta para pequenas e médias empresas atualmente, diversas tendências prometem melhorar continuamente o serviço de MDR, incluindo as seguintes:



1. Maior integração com outras soluções de segurança. À medida que as tecnologias evoluem, espera-se que o MDR se integre a soluções de segurança adicionais, como Network Detection and Response (NDR), Secure Service Edge (SSE) e outras.

2. Inteligência avançada sobre ameaças. À medida que os algoritmos de IA e ML incorporam inteligência de ameaças mais avançada, o MDR melhorará continuamente sua capacidade de identificar e responder a ameaças em tempo real.

3. Orquestração, Automação e Resposta de Segurança (SOAR). Com o tempo, ferramentas e algoritmos avançados permitirão que o MDR se torne mais automatizado, eliminando os processos manuais envolvidos na análise e resposta a incidentes. Isso aumentará a velocidade e a precisão da resposta às ameaças.

4. Maior foco na segurança da nuvem. À medida que mais pequenas e médias empresas adotam tecnologias de nuvem, os provedores de MDR precisarão se concentrar em como proteger a infraestrutura, os sistemas e os dados da nuvem.

5. Maior adoção que leva a custos mais baixos. Com cada vez mais empresas adotando o MDR como sua principal solução de segurança, a concorrência no mercado aumentará. A boa notícia é que a adoção do MDR levará a soluções de custo mais baixo.

Dado o cenário atual de ameaças cibernéticas complexas e em rápida mudança, as pequenas e médias empresas devem proteger proativamente suas redes. Qualquer coisa menos os coloca em risco. Mas com o MDR, as PMEs não precisam mais se preocupar em serem alvo de ataques cibernéticos. **Em vez disso, podem ter a certeza de que possuem os recursos, a experiência e o pessoal necessários para proteger adequadamente as suas redes.**

# Quer saber mais sobre inovação em Cibersegurança e **como nosso time pode ajudar sua empresa?**

hughes.com.br

HUGHES®
An EchoStar Company