SOPHOS

EBOOK

EDR, XDR, MDR

Qual é a diferença? E qual é o mais adequado para o seu negócio?

SUMÁRIO

©2026 Sophos. Todos os direitos reservados.

EDR, XDR, MDR

Qual é a diferença? E qual é o mais adequado para o seu negócio?

Os líderes de TI e segurança enfrentam uma pressão crescente para fortalecer a resiliência cibernética sem sobrecarregar suas equipes ou orçamentos já limitados. Com o aumento do volume de ameaças e a sofisticação dos ataques, é fundamental fazer investimentos inteligentes em recursos de detecção e resposta a ameaças.

Quer você esteja operando em escala global ou gerenciando uma equipe mais enxuta, é fundamental alinhar sua abordagem de segurança com o perfil de risco e as realidades operacionais da sua organização. Para muitos líderes, escolher a abordagem certa de detecção e resposta também significa decidir se você mesmo vai gerenciá-la ou se vai trabalhar com um parceiro de confiança. Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) e Managed Detection and Response (MDR): cada um deles oferece vantagens exclusivas, mas o verdadeiro desafio é identificar qual deles agrega mais valor à sua organização. O EDR e o XDR são ferramentas que ajudam sua equipe na detecção, investigação e resposta mais rápidas. O serviço MDR oferece monitoramento e resposta 24 horas por dia, 7 dias por semana, por meio de analistas especializados, geralmente utilizando XDR e outras tecnologias.

Compreender o que diferencia essas abordagens — e como elas podem se complementar — é o primeiro passo para construir uma estratégia de segurança que proteja você hoje e o posicione para a resiliência amanhã.

Por que a detecção e a resposta são importantes

Uma proteção de endpoint robusta continua a ser a sua primeira linha de defesa. No entanto, agentes de ameaças sofisticados exploram credenciais legítimas, clonam usuários confiáveis e abusam de ferramentas de TI nativas para burlar as defesas. Esses ataques podem não parecer maliciosos para uma ferramenta preventiva, e é exatamente por isso que eles são bem-sucedidos.

Recursos de detecção e resposta, como EDR, XDR e MDR, preenchem essa lacuna crítica. Eles ajudam a identificar e neutralizar as ameaças que conseguem burlar as ferramentas de prevenção antes que se transformem em incidentes graves.

©2026 Sophos. Todos os direitos reservados.

O QUE É EDR?

O Endpoint Detection and Response (EDR) faz parte de uma estratégia de segurança contínua de endpoints. Ele ajuda as equipes a monitorar, detectar e responder a ameaças e incidentes de segurança em dispositivos de endpoint, como laptops, desktops e servidores.

Principais benefícios do EDR:

Oferece visibilidade em tempo real da atividade do endpoint, como execução de arquivos, comportamento de processos e movimento lateral, para que as equipes possam identificar e bloquear rapidamente as ameaças antes que se espalhem.

Detecta ameaças evasivas identificando indicadores comportamentais, ajudando você a detectar ataques que as ferramentas de prevenção tradicionais muitas vezes não conseguem identificar.

Automatiza ações de resposta, como o isolamento de endpoints afetados ou o encerramento de processos maliciosos, reduzindo o tempo de permanência e impedindo que os invasores avancem.

Descubra como o Sophos EDR pode proteger seus endpoints e servidores contra ataques avançados conduzidos por humanos, seja no escritório, na rede ou na nuvem.

©2026 Sophos. Todos os direitos reservados.

O QUE É XDR?

O Extended Detection and Response (XDR) aumenta a visibilidade das ameaças ao integrar dados de todo o seu ecossistema de segurança além dos endpoints e servidores. Inclui firewalls, e-mail, infraestrutura de nuvem, sistemas de identidade, soluções de backup e recuperação, ferramentas de produtividade, endpoints e servidores, entre outros. O XDR permite uma correlação mais eficaz de atividades suspeitas, ajudando a identificar ataques multivetoriais sofisticados que ferramentas isoladas podem deixar passar.

Enquanto o EDR analisa profundamente os endpoints, o XDR amplia a visibilidade e liga os pontos entre todos os sistemas. Ele apresenta uma visão holística de um ataque, facilitando a detecção de ameaças multiestágio e multivetor que, de outra forma, passariam despercebidas.

Principais benefícios do XDR:

Correlaciona sinais entre múltiplos vetores de ataque para descobrir padrões e priorizar alertas de alta fidelidade. Isso reduz o ruído e coloca em foco ameaças complexas e multissistêmicas.

Otimiza os fluxos de trabalho de investigação para que sua equipe possa responder com mais rapidez e confiança. Os analistas obtêm uma visão clara de como um ataque se desenrolou — e como evitar que aconteça novamente.

Oferece suporte a fluxos de trabalho de investigação e resposta com ferramentas alimentadas por IA que aceleram a análise e a remediação e oferecem uma resolução mais rápida e precisa dos incidentes.

Descubra como o Sophos XDR habilita a detecção, investigação e resposta a atividades suspeitas em todo o seu ecossistema.

©2026 Sophos. Todos os direitos reservados.

O QUE É MDR?

O Managed Detection and Response (MDR) é um modelo orientado a serviços que combina IA com analistas humanos especializados para fornecer 24 horas diárias de monitoramento, caça a ameaças e resposta a incidentes. Ele é especialmente valioso para organizações que operam apenas em horário comercial ou que enfrentam lacunas na cobertura do SOC, dificuldades com pessoal ou complexidade crescente.

O MDR pode funcionar como uma solução totalmente terceirizada ou uma extensão cogerenciada de sua equipe interna, ajudando a reduzir o tempo de permanência e evitar incidentes, como ransomwares, antes que se agravem.

Principais benefícios do MDR:

Cobertura 24/7. As ameaças não aparecem só das 8h às 18h: 88% dos ataques de ransomware ocorrem fora do expediente. O MDR garante cobertura 24 horas diárias.

Acesso a analistas de segurança especializados que compreendem o comportamento dos invasores e agem com determinação. Esses especialistas lidam com incidentes diariamente, priorizando e contendo ameaças para manter o bom funcionamento do seu negócio.

Livre-se da fadiga de alertas e triagem manual. O MDR elimina o ruído, para que sua equipe possa se concentrar em iniciativas estratégicas, em vez de perseguir falsos positivos.

Resolução rápida nos momentos importantes. Em incidentes de alto risco, como ransomwares, as equipes MDR podem detectar e conter as ameaças antes mesmo que as equipes internas saibam de sua existência, evitando interrupções e reduzindo riscos.

Descubra como o Sophos MDR, com sua plataforma aberta e alimentada por IA e analistas especializados, pode complementar sua equipe e atendê-lo onde você estiver em sua jornada de segurança.

©2026 Sophos. Todos os direitos reservados.

QUANDO CONSIDERAR EDR, XDR OU MDR

Solução	Considere se...	Não é a melhor opção se...
EDR	• Você precisa de detecção e resposta de endpoint robustas. • Você deseja elevar suas defesas além das ferramentas de endpoint preventivas. • Você está construindo uma defesa em camadas que dê suporte à futura integração de XDR ou MDR.	• Você precisa de visibilidade ampla de todo o seu ambiente (nuvem, identidade, rede, backup, etc.). • Você espera detecção e resposta 24/7 sem terceirizar ou aumentar o quadro de funcionários.
XDR	• Você precisa de uma visão unificada de todos os principais vetores de ataque, incluindo endpoint, firewall, rede, nuvem, identidade, backup e ferramentas de produtividade. • Você deseja uma correlação mais rápida das ameaças e a redução da fadiga de alertas. • Você deseja maior retorno do investimento em segurança e tecnologia de TI existente e futura.	• Você pretende monitorar apenas endpoints e servidores. • Você precisa de mais suporte do que a sua equipe pode oferecer. • Você não possui os recursos internos necessários para gerenciar uma plataforma XDR.
MDR	• Você precisa de detecção e resposta a ameaças 24/7 conduzidas por especialistas. • Você está enfrentando fadiga de alertas, escassez de talentos ou esgotamento mental. • Você quer um parceiro proativo para investigar e neutralizar ameaças em seu nome. • Você deseja melhorar sua classe de bônus do seguro de proteção digital, reduzindo prêmios e aumentando a cobertura.	• Você já possui operações de segurança estabelecidas, com uma equipe completa e recursos internos, oferecendo cobertura robusta 24 horas por dia, 365 dias por ano. • Você não está pronto para terceirizar partes de suas operações de detecção e resposta.

©2026 Sophos. Todos os direitos reservados.

CONSIDERAÇÕES ADICIONAIS ANTES DE DECIDIR

Ao ponderar suas opções, há alguns fatores críticos que podem determinar se EDR, XDR ou MDR é uma boa opção e qual parceiro pode cumprir o prometido.

A inteligência de ameaça é importante

A eficácia de qualquer solução de detecção e resposta a ameaças depende da qualidade da inteligência de ameaça que a alimenta. Quanto mais amplas, profundas e atuais forem as informações, mais rápido será detectar e bloquear as ameaças. Certifique-se de que qualquer fornecedor que você considerar possa explicar a fonte e o escopo de seus dados sobre ameaças.

O serviço deve ser mais do que uma promessa

Mesmo a melhor tecnologia pode deteriorar sem um suporte ágil. Quer você faça a autogestão ou recorra a um parceiro para serviços gerenciados, é importante saber que terá ajuda disponível quando precisar. Pergunte aos fornecedores como o suporte funciona na prática: quem responde, com que rapidez, o que está incluído e como obter ajuda durante um incidente ativo.

O custo nem sempre é o que parece

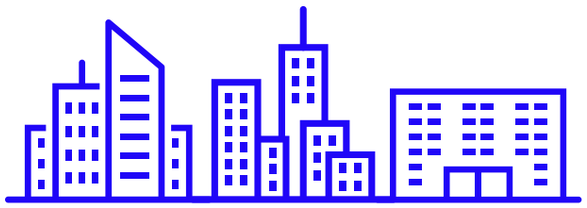
Não presuma que um caminho é inerentemente mais caro. Os preços variam muito, dependendo de como cada solução é implementada e assistida. Concentre-se nas suas necessidades específicas e considere o seu quadro de funcionários atual e os investimentos existentes, incluindo possíveis trocas de tecnologia e o custo de recursos internos versus terceirizados.

As soluções de detecção e resposta, particularmente MDR, podem influenciar os custos do seguro de proteção digital. Atualmente, muitas seguradoras favorecem as organizações que possuem monitoramento e resposta a ameaças 24/7, o que pode resultar em prêmios reduzidos ou melhores condições de cobertura.

Uma análise abrangente do ROI que leve em consideração a economia operacional, a redução de riscos e até mesmo os benefícios do seguro pode ajudá-lo a descobrir o custo real e o verdadeiro valor de cada abordagem.

©2026 Sophos. Todos os direitos reservados.

CONCLUSÃO



US$ 1,53 milhão

O custo médio para recuperar-se de um ataque de ransomware — sem computar os pagamentos de resgate.*

40%

das organizações atingidas por ransomware afirmam que a falta de expertise em segurança cibernética contribuiu para o ataque.*

Os riscos são altos demais para basear-se em suposições.

Escolher a estratégia certa de detecção e resposta não se resume apenas à tecnologia, mas também a capacitar seus funcionários, proteger suas operações e construir uma defesa cibernética resiliente e duradoura.

*Relatório Sophos O Estado do Ransomware 2025

©2026 Sophos. Todos os direitos reservados.

SOPHOS
DEFEAT CYBERATTACKS

SAIBA MAIS SOBRE AS SOLUÇÕES E SERVIÇOS DA SOPHOS

A Sophos ajuda você na detecção e resposta às ameaças atuais e à medida que suas necessidades de segurança evoluem.

Fale com um especialista da Sophos e vamos trabalhar juntos para encontrar a solução certa para a sua empresa.