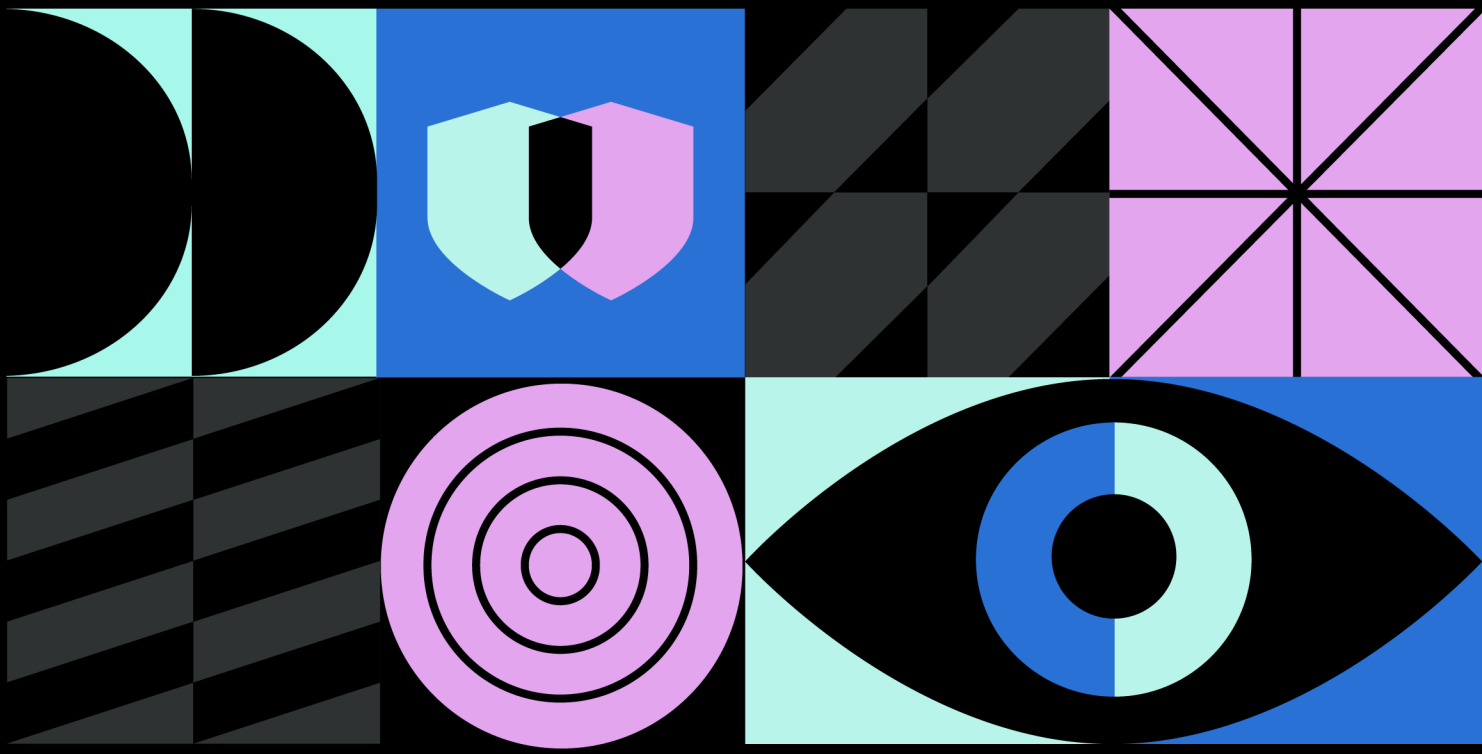
Coalition®



Coalition MDR Buyer's Guide

5 key questions to ask when evaluating managed detection and response services

Key questions to help you evaluate MDR services

Modern businesses face a sprawling landscape of cyber threats. New critical vulnerabilities emerge every day, straining overburdened teams and contributing to alert fatigue, while threat actors increasingly target common business tools that are essential to operation, like email accounts and remote access solutions.

Small and medium-sized businesses, in particular, are at a disadvantage when it comes to protecting against cyber attacks due to existing resource constraints and the high costs of enterprise security tools. As a result, businesses are often forced to accept higher levels of cyber risk.

One security control allows businesses of all sizes to address the risk of cyber attacks head on: **managed detection and response (MDR)**. With MDR, your business can add human expertise to scale its threat detection and response capabilities to respond to, and potentially prevent, cyber attacks.

> "By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment and mitigation capabilities."[1]

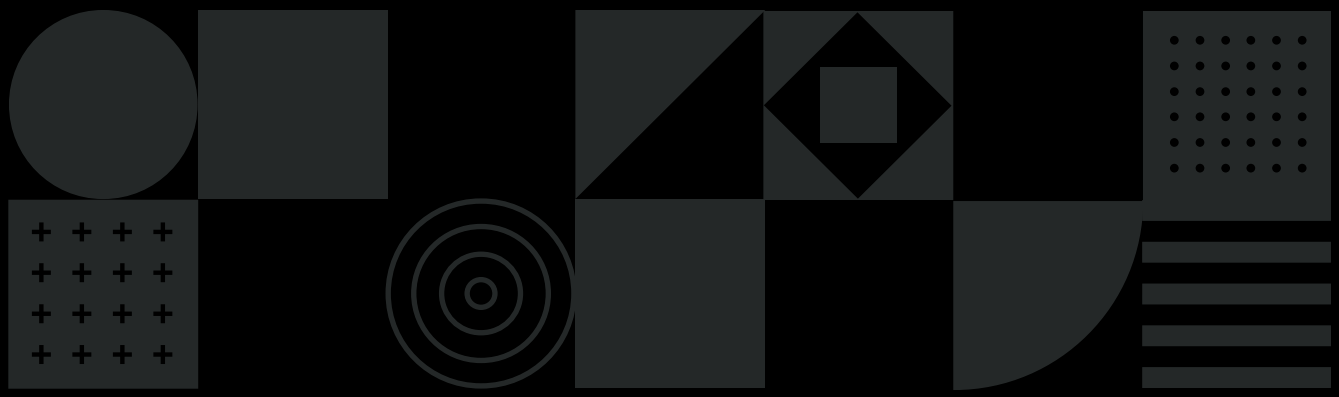
[1] Gartner, The Future of MDR, Where Next?

01

What factors can impact my MDR investment?

The size of your organization is an important consideration when evaluating MDR vendors. Some vendors may require your business to have a minimum number of endpoints to qualify for a contract. If your business falls below that threshold, you may end up paying for services you can't fully utilize.

It's also important to know if an MDR vendor has any device or software restrictions. Some organizations may already have an endpoint detection and monitoring (EDR) solution, but lack the 24/7 support to triage alerts and logs after hours. In this case, you may want to consider partnering with an MDR vendor that supports a bring your own license (BYOL) model or utilizes the same EDR solution your business is using.



02

How does the MDR service respond in the event of an incident?

Businesses with MDR in place have a 50% faster mean time to respond, dramatically lowering the impact of cyber incidents.[2] However, using an MDR vendor is only one part of the equation regarding response time. Your business also needs to consider an MDR vendor's process for responding to and remediating critical alerts.

First, determine the vendor's service-level agreement for escalating alerts. Your business should be made aware of alerts above a certain severity, usually high and critical, within a reasonable timeframe.

Another critical consideration is alert resolution. Some vendors may limit the number of alerts they will resolve. In this case, your business' existing IT or security team could be responsible for remediating the alert.

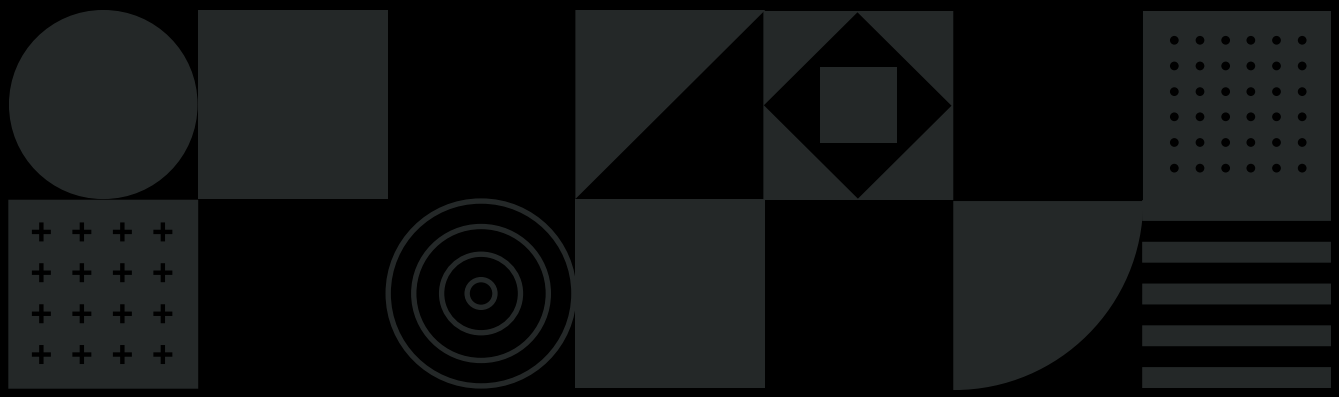
[2] Integrity360, The Benefits of MDR

03

Which technologies and data sources can MDR monitor?

Every business' attack surface is different. If your business operates in a highly regulated industry, you may need additional monitoring beyond the endpoint.

Some MDR vendors use technologies like extended detection and response (XDR) or security information and event management to ingest telemetry from additional sources, such as log data from firewalls, email service providers, and identity and access management tools.



04

How will the MDR service integrate with my existing IT team?

Standing up an in-house 24/7 security operations center (SOC) is cost-prohibitive for many businesses. MDR can level the playing field for your business by supplementing existing resources without the expense of additional headcount or technology.

MDR can also provide enhanced support for businesses that use a managed service provider (MSP). An MSP can provide critical support for businesses without in-house security expertise, but the MSP may not offer 24/7 monitoring or have incident response capabilities. Businesses that leverage an MSP for their daily IT and security needs can layer an MDR service to ensure they receive around-the-clock protection from dynamic cyber risks.

> "The average time to detect a security incident is 32 days for organizations with a SOC and no MDR, compared to just 10 days for those using MDR."[3]

[3] Integrity360, The Benefits of MDR

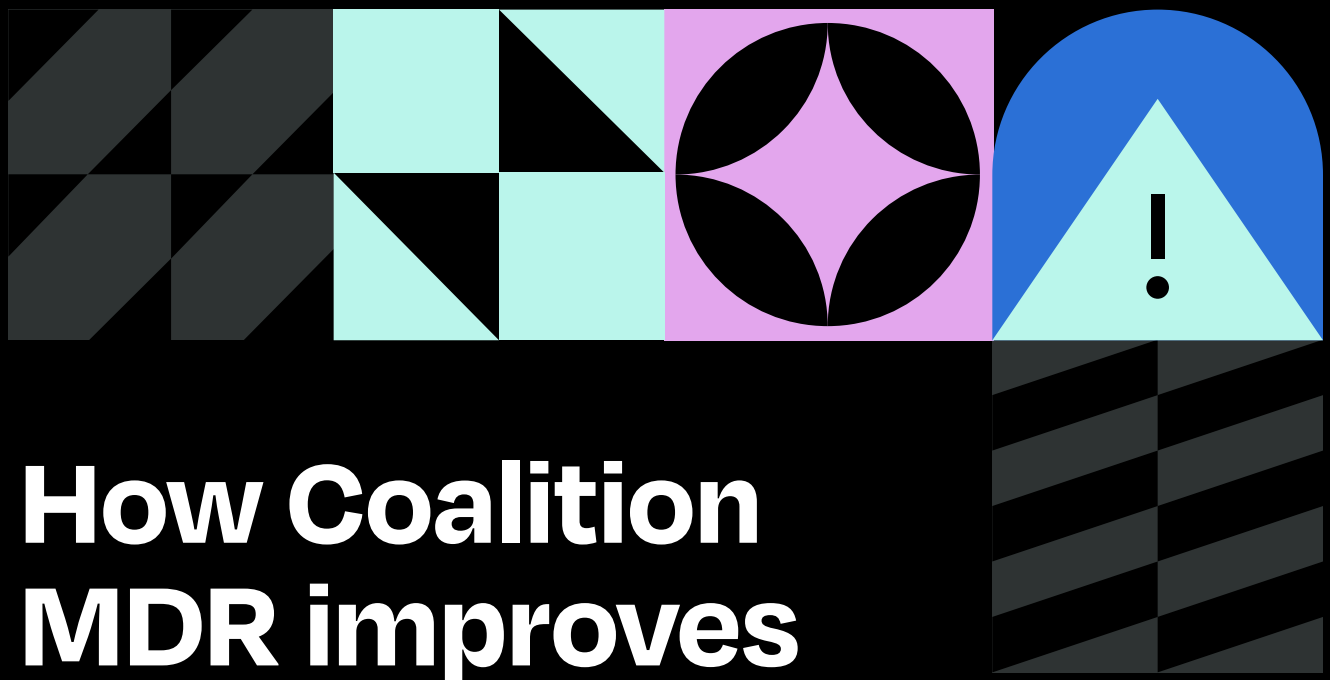
05

Does the MDR vendor provide any additional benefits?

Cyber risk is now the most significant concern for business leaders globally.[4] The good news is that some MDR services can offer customized security guidance to help improve your business' overall security posture.

If you're looking to improve your business' security posture, look for an MDR vendor that provides sufficient detail regarding the events and incidents they resolve, such as access to event logs, event reports, and incident response reports. Some MDR vendors will go above and beyond standard incident response reporting and provide tailored threat intelligence and additional guidance.

[4] Allianz, Allianz Risk Barometer 2024



How Coalition MDR improves business resilience

When you choose Coalition MDR, our expertise becomes your business advantage — the same expertise that has helped many clients detect and mitigate attacks before they resulted in significant financial losses.[5]

Coalition MDR leverages the power of SentinelOne for prevention, detection, and response capabilities. We combine this technology with insights from Coalition's proprietary data on insurance claims, incident response, and cyber threats to quickly triage and respond to alerts.

Unlike traditional MDR services that lack comprehensive response capabilities or impose extra expenses, Coalition MDR is designed to be comprehensive and tailored from the start. We partner and scale with growing businesses to offer distinct service tier options to best meet their needs.

As part of our holistic approach to cyber risk management, your business receives a customized Quarterly Security Review meeting with Coalition experts that's designed to strengthen your security posture. And should the worst happen, your business has access to a streamlined escalation process with Coalition Incident Response (CIR), which can help reduce the severity of a cyber event.

[5] Coalition Security Services MDR services are provided by Coalition Incident Response, Inc., an affiliate of Coalition.

Enhanced protection opportunities

If your business needs monitoring and protection that goes beyond the endpoint ...

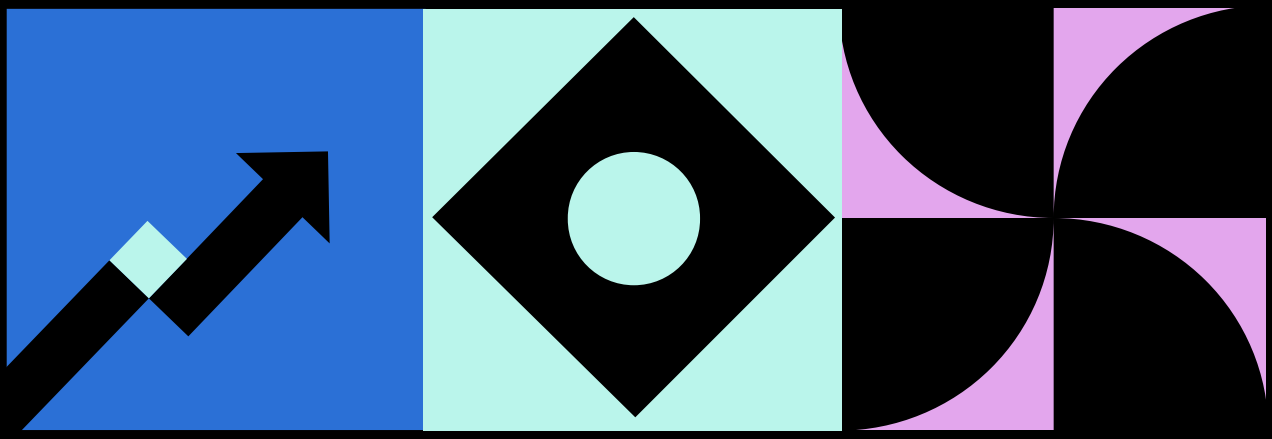
Coalition MDR Plus uses XDR technology to help protect more than just endpoints and provide more holistic monitoring and response capabilities. We can ingest telemetry from other sources for even better visibility and extend our unlimited remediation to support these additional data sources. Coalition MDR Plus customers also benefit from tailored rules and alerts, which help to reduce false positives and decrease alert fatigue for security and IT teams.

If your business needs added protection against phishing or business email compromise ...

Coalition Email Security allows us to take quick action when we see indicators of an attack, lock accounts, or enforce password resets before the threat actor can gain additional access. We watch over your inbox to help safeguard business data and other critical information.

"When something like a ransomware attack happens, you start rethinking and double-checking everything. And knowing there is another team, always watching, and capable of catching what our previous providers missed ... It's like a security blanket for security folks. We know there's a truly expert team watching our backs now."

Chief Technology Officer, Coalition MDR Customer



Premium credits for Coalition policyholders

Businesses that use Coalition MDR are eligible for up to a 12.5% credit applied to the cost of their cyber insurance policy premiums.[6] The premium credit is currently available on U.S. Surplus Cyber policies provided by Coalition and must be applied before the policy is bound or prior to renewal.

The premium credit is available to businesses that use any of the following MDR solutions:

- Coalition Managed Detection & Response
- CrowdStrike Falcon Complete
- SentinelOne Vigilance Respond or Vigilance Respond Pro

[6] Eligibility for credit is determined at time of quote or renewal that occurs after January 1, 2024, and based upon policyholder information and risk profile. Exclusions and limitations apply. Customers with MDR other than Coalition MDR may be eligible for a MDR premium credit. For more information, limitations, and exclusions of this offering, contact mdrsales@coalitioninc.com.

Coalition MDR Key Features at a Glance

Feature	Coalition MDR	Coalition MDR Plus	Coalition Email Security
24/7 monitoring, incident detection and management	✓	✓	✓
Unlimited remediation for alerts	✓	✓	✓
30-min response time for critical alerts	✓	✓	✓
No minimum number of endpoints	✓	✓	✓
Quarterly Security Review	✓	✓	✓
Detailed notification w/findings for alerts	✓	✓	✓
Eligible for Active Insurance Premium Credit	✓	✓	
Threat hunting capabilities	✓	✓	
Vulnerability alerting and scanning	✓	✓	
Endpoint log monitoring	✓	✓	
BYOL options for Crowdstrike and Microsoft Defender	✓		
Custom rules and alerts derived from Coalition proprietary data		✓	
Extended logging and monitoring of additional data sources		✓	
Email protection		✓	✓
Raw data protection period	30 days standard/up to 1 year		

Prevent more cyber incidents and respond faster to attacks

Businesses of all sizes and industries should plan for how to protect themselves from a cyber attack. Coalition has helped hundreds of thousands of businesses protect themselves from cyber risk with Active Insurance — and now we're taking it a step further.

Coalition MDR is designed to meet the needs of your businesses and help you remediate the cyber risks that are most likely to result in financial loss. Businesses choose Coalition MDR for our around-the-clock monitoring, industry-leading technology, affordable solution, and expert remediation.

Let our expertise become your advantage

30 minutes
Average response time for critical alerts

24/7
Active monitoring

No minimum
Endpoints to sign up

100%
Critical/high alerts resolved with no extra fee

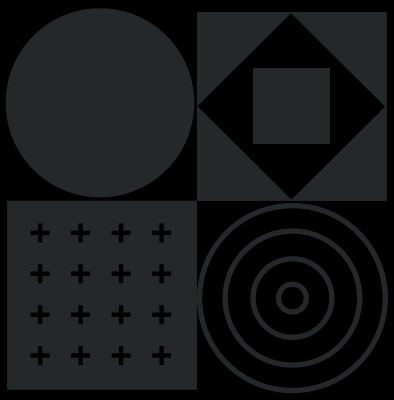
100%
Access to all alerts and logs

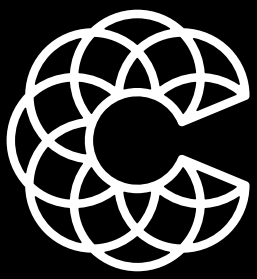
12.5%
Premium credit for Coalition policyholders

Ready to schedule a call?
Speak with a Coalition expert

Want to go deeper on cybersecurity?
Explore all our tools and services

Interested in learning about us?
See all that Coalition has to offer





Coalition®

coalitioninc.com