

Coalition Managed Detection and Response

Help protect your business from cyber threats with 24/7 monitoring and unlimited remediation



Digital risks evolve as fast as technology. Your business' reaction time to a cyber attack can mean the difference between maintaining operations or experiencing a disruption.


Coalition Managed Detection and Response¹ (MDR) provides small and midsize businesses with the expertise and technology to shield themselves from advanced cyber risks. Coalition MDR offers around-the-clock threat detection and response capabilities, accelerating time-to-remediation and minimizing or eliminating the impact of a cyber incident.

Traditional risk management tools aren't always enough to detect or stop a cyber attack. MDR combines the alerting and identification capabilities of endpoint detection and response (EDR) or extended detection and response (XDR) technology with human cybersecurity experts.

Coalition MDR leverages insights from proprietary insurance claims, incident response, and cyber threat data to quickly triage the alerts most likely to result in an adverse cyber incident. Let our expertise become your advantage.



Businesses with MDR in place have a 50% faster mean time to respond, which dramatically minimizes the impact of a cyber incident.

 Source
Integrity 360, The Benefits of MDR



“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**

¹ Coalition MDR services are provided by Coalition Incident Response, Inc., an affiliate of Coalition.

Why Businesses Choose Coalition MDR

Keeping pace with new cyber threats can be a never-ending endeavor, especially for under-resourced security teams. Threat actors can easily exploit the sprawling landscape of devices that facilitate employee and customer access.

Coalition MDR can help your businesses address cyber risk head-on without breaking the budget. With tailored and affordable security solutions, we partner directly with your business to help respond and recover faster, minimize impact, and prevent future attacks.

Unparalleled expertise, around-the-clock protection

- ▶ **24/7 monitoring and response**
Off-hours are prime opportunities for threat actors. Our continuous threat detection and response helps you act faster while minimizing operational disruption and impact.
- ▶ **Incident response experts**
As a leading cyber insurance provider, Coalition often supports businesses through the worst kinds of cyber attacks. We bring unmatched expertise to help detect and remediate threats before they can become an attack.
- ▶ **Proactive security alerts to reduce risk**
Receive actionable alerts to help your business respond to threats before they become attacks. Coalition creates actionable alerts using proprietary data sources, including our Active Data Graph, enumeration of the public internet, a global network of honeypots, and our zero-day notification program.

Enterprise security tools, proprietary data sources

- ▶ **Leading EDR and XDR technology**
Coalition MDR uses SentinelOne for prevention, detection, and response capabilities across endpoint, cloud, and identity security. You can also bring your own license (BYOL) for CrowdStrike and Microsoft Defender.
- ▶ **Protection beyond endpoints with MDR Plus¹**
In addition to endpoint data, we can ingest telemetry from other sources to extend detection and response capabilities for better visibility: email, network, data platforms, identity and access management, configurations, and more.



Continued →

Why Businesses Choose Coalition MDR

Additional benefits for Active Cyber Insurance customers

- ▶ **Premium credits on select policies**
Businesses in the U.S. that use Coalition MDR are eligible for up to a 12.5% premium credit on cyber insurance policies provided by Coalition.²
- ▶ **Insurance-covered incident response**
If a covered event does occur, policyholders can access cost savings from our zero deductible response services when they engage Coalition Incident Response.³
- ▶ **Coalition Control™**
All policyholders receive access to [Coalition Control](#) for the duration of their policy to gain visibility into the cyber risks directly impacting their business.
- ▶ **Access to expert panel vendors and partners**
Cybersecurity is a team sport. Coalition policyholders can receive additional support and resources directly within the Control Marketplace.

Scalability and affordability, built for growing businesses

- ▶ **Powerful MDR at an affordable price**
Coalition MDR utilizes enterprise-grade technology at an accessible price point, and without the costly minimums of other providers.
- ▶ **Tailored to your business' infrastructure**
Use the technology provided by Coalition MDR or enhance your existing security tooling with our expertise. We can match our solution to your business' infrastructure.
- ▶ **Flexibility to scale and grow**
Add or remove endpoints, services, applications, or infrastructure as needed.



² 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 a MDR other than Coalition's MDR services may be eligible for a MDR premium credit. Contact MDRsales@coalitioninc.com for more information, including limitations and exclusions of this offering.

³ Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.

Why Businesses Choose Coalition MDR

Cyber risk management often begins with the endpoint. While EDR and XDR are important monitoring tools that can be enhanced by threat analysts who respond to events in real time. MDR is a cost-effective way for your business to add human expertise without adding headcount.

Coalition MDR

Every business' attack surface is different. As a Coalition MDR¹ customer, you can select from three distinct tiers to meet the needs of your business. All customers benefit from the following core features:



24/7 monitoring and unlimited remediation



30-minute service level agreement (SLA) for critical alerts



No minimum number of endpoints



Quarterly Security Reviews plus ad-hoc support for posture management

Coalition MDR Plus

If your business retains a substantial amount of data or operates in a highly regulated industry, you may need a service to monitor endpoints and external data sources. Coalition MDR Plus uses XDR technology to go beyond the endpoint with three distinct benefits:



Enhanced monitoring of critical data sources

In addition to endpoint data, Coalition MDR Plus ingests telemetry from other sources to extend detection and response capabilities for even better visibility. Examples include Office 365 logs, Azure AD/AD logs, firewall logs, and multi-factor authentication (MFA) and identity access management (IAM) provider logs.



Tailored rules and alerts

To further reduce false positives and alert noise, the Coalition MDR team writes customizable correlation rules to alert on suspicious activity quickly. Custom rules allow us to send alerts for the anomalous activity that presents the greatest risk to your business, such as suspicious logins or enabled guest accounts.



Taking action beyond the endpoint
















Along with monitoring beyond the endpoint, the Coalition MDR team also extends its remediation capabilities to address the systems of origin. Examples include locking compromised accounts and forcing password resets.

Coalition Email Security



Your email inbox likely contains business critical information that should be protected from cyber attacks, such as phishing or business email compromise (BEC). Coalition Email Security allows us to take quick action when we see indicators of an attack and lock accounts or enforce password resets before the threat actor can gain additional access.

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		

Ready to Create a Tailored MDR Solution?

Let our expertise become your advantage. We can help choose the right MDR solution for your business so that you are prepared to address sophisticated cyber threats before they become attacks.

Contact us at MDR@coalitioninc.com if you're interested in more information on pricing and other details of a potential partnership with us.