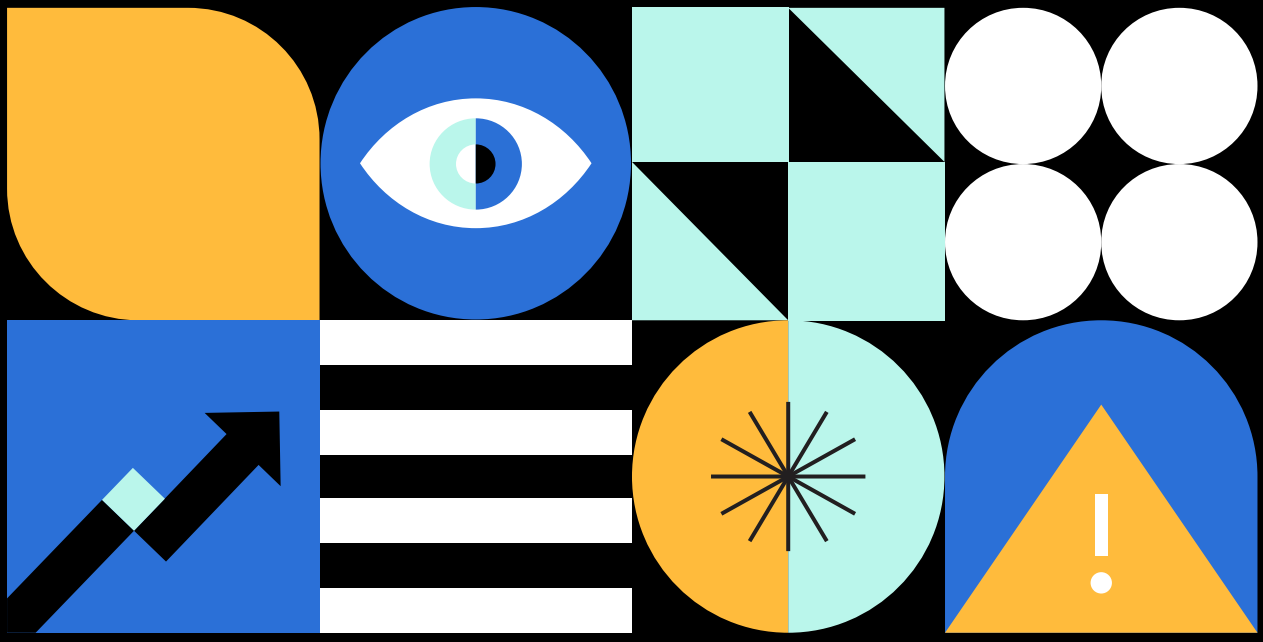
Coalition®

coalitioninc.com



A SECURITY LEADER'S GUIDE TO

Scaling Threat Detection & Response

Executive Summary

Now more than ever, businesses are looking for ways to reduce costs while staying better protected. This creates a challenge for small IT and security teams that must operate with limited staff and budgets while the number of reported security incidents is at an all-time high. As a result, managing cyber attacks can be more than an uphill battle; for some teams, it is an insurmountable task. Instead of trying to "do more with less," leaders can look to scale their cyber operations without adding headcount in ways that help them shift from reactive responses to active threat mitigation, particularly with managed detection and response (MDR).

Security defenders have a challenging job. Many found their roles upended in the face of the coronavirus pandemic, with teams, and data, transitioning away from traditional office-centric models to remote and distributed environments. The technologies that enabled businesses to survive lockdowns and closures were quickly exploited by cybercriminals, requiring constant vigilance on the part of defenders.

Years later, the surge in cyber attacks has not abated. Instead, attacks have become a mainstay in the daily news cycle with behemoth organizations, once thought to be relatively secure, like MGM and Caesars, suffering highly public compromises. With each incident, the security posture of the victim organization endures a reckoning, whether it be at the hands of threat actors, or speculation that poor hygiene caused the event.[1]

As incidents and data breaches become more common, security practitioners are held accountable not only to regulations but also to customers whose data is stolen or leaked by cybercriminals. Notably, the former Chief Security Officer (CSO) of Uber was tried and sentenced for covering up a data breach.[2] Yet, despite the increased scrutiny, many security and IT teams are stretched thin in fraught global and economic times.

Of course, hand-wringing about burnout in cybersecurity has increased, with Gartner predicting that nearly half of cybersecurity leaders will leave the field by 2025. And attrition among existing practitioners only compounds these challenges.[3]

1. Ilascu, Ionut. "MGM casino's ESXi servers allegedly encrypted in ransomware attack." Bleeding Computer, Published September 14, 2023.
2. Justice.gov, Former Chief Security Officer Of Uber Sentenced To Three Years' Probation For Covering Up Data Breach Involving Millions Of Uber User Records, Published Friday, May 5, 2023
3. Gartner, Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025, Published February 22, 2023

Endpoint Management with the Power of a 24/7 Security Operations Center, Minus the Expense

One of the key challenges defenders face is the sprawling landscape of devices that need access to critical business data. Traditional security measures, such as antivirus and firewalls, have become insufficient. To employ best practices of cyber risk management, organizations should understand the totality of their attack surface, and that often begins with monitoring their endpoints.

Research from Enterprise Services Group shows that the diversity of devices used to access critical business assets can present challenges in managing and securing endpoints. In a survey of 380 security professionals, nearly a third of organizations reported one or more endpoint-related cybersecurity incidents. Yet, over half of security leaders reported that 11-20% of their endpoints were unmanaged.[4]

Endpoint detection and response (EDR) tools can detect suspicious activities, however, these solutions output a high volume of logs and require human intervention to review for false positives and to respond to confirmed anomalous activity. Several EDR tools are now stretching beyond the endpoint to monitor other common data sources (email, firewall, AD/authentication source, etc.) — known as extended detection and response (XDR) — and correlate this XDR data alongside EDR data for enhanced detection capabilities. This leads to an even higher volume of alerts and an even greater need for human intervention, frequently resulting in alert fatigue for under-resourced teams. And unfortunately, both EDR and XDR tools also lack the ability to intervene in the event of a malicious attack. This means while they can —and will— alert on various outside threats, the effectiveness stops once an attacker has penetrated an organization's network.

In contrast, MDR is a cybersecurity service that combines human expertise and advanced tools with automation. MDR combines all of the alerting and detection capabilities of EDR and XDR with human threat hunters who are able to respond to threats in real time. Not all organizations are able to staff and run a security operations center (SOC), but with MDR, you have the power of a SOC without having the expense of headcount and tooling. For many teams, MDR can offer comprehensive threat detection, mitigation, and response capabilities without adversely impacting their budget.

> **To employ best practices of cyber risk management, organizations should understand the totality of their attack surface, and that often begins with monitoring their endpoints.**

4. Gold, Jon. "Growing number of endpoint security tools overwhelm users, leaving devices unprotected." CSO Online. Published February 8, 2023

5 Reasons Security Leaders Choose MDR

1. Minimize the impact of cyber attacks and avoid reinfection

MDR tools leverage artificial intelligence (AI) and machine learning (ML) to catch anomalous and known malicious activity. Essentially, they can spot a threat actor in the act of compromising a network and evict them mid-attack. Once spotted, the team behind the MDR service can cut the connection of a remote session, virtually isolate impacted machines, and revoke privileges for compromised attacks. Not only does this stop the threat actor in their tracks, but it preserves forensic evidence for triage and review, helping to determine the root cause and prevent future compromises.

2. Monitoring and response, 24/7

Security and IT teams know anyone can buy a product, but the actual value of MDR services is the team performing the response. With MDR, the human threat hunters behind the software have service-level agreements (SLAs) on how quickly to respond and when to alert the businesses they support. Historically, companies see an uptick in cyber attacks on holidays or weekends when they are traditionally lightly staffed. MDR helps to mitigate this concern by creating a 24/7 SOC.

3. Add expertise *without* adding headcount

While a SOC is a tremendous value add in today's dynamic threat landscape, setting up an equivalent service can be cost-prohibitive. Many companies would likely need to fully outsource the team or hire several new employees. In addition to labor costs, companies would need to purchase the technology to run the SOC and allow time to start operations.[5] MDR provides small to medium-sized organizations with a scalable, cost-effective way to get the expertise they need to proactively monitor and mitigate their cyber risks and threats.

4. Vulnerability scanning

Today, businesses face a growing number of critical and zero-day vulnerabilities, with some cyber experts speculating that the "hot zero-day summer" of 2023 may be the new normal rather than a trend.[6] With such volume, vulnerability management can quickly leave even the most prepared teams beleaguered and overwhelmed. Because MDR services are behavior-based instead of signature-based, they can identify malicious activity and walk backward to determine the point of compromise, even if the threat actor is using a zero-day.

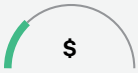
5. *For more information, please reference the chart below.*
6. *Blake, Andrew. "As 'hot zero-day summer' rolls on, experts think this might be the new normal." SC Magazine, Published August 1, 2023*

5. Improve your cybersecurity ROI

Cybersecurity is expensive. From hiring, training, and retaining talent to procuring the required technology, the costs can add up. Typically, the cost of setting up an enterprise-grade SOC can be in the millions after factoring in headcount, software, and training. MDR is a scalable choice at a fraction of the cost. Additionally, the cost of a business-interrupting cyber incident or cyber insurance claim is also high. After a brief respite in 2022, they are rising again. Ransomware claims severity rose 61% in 2023 to an average loss amount of $365,000.[7] For many organizations, an MDR service provides the additional capabilities needed at a fraction of the cost of a cyber insurance claim or an in-house SOC.

Coalition Incident Response (CIR)[8] handles nearly 1,000 cases a year. When providing digital forensics for ransomware or business email compromise (BEC), CIR often found logs and alerts the policyholder did not take action on. MDR customers benefit from both 24/7 real-time alerts and a team of humans to respond, whether they build it in-house or find a security partner.

How Proactive Cybersecurity Leaders Justify MDR Investment

SOLUTION APPROACH	AVG. COST	ORGANIZATION SIZE	ADDITIONAL BENEFITS
Coalition Security Services Managed Detection & Response (MDR)[9]		Ideal for small to **medium-sized businesses**; scales well from small to medium number of endpoints.	Pairs well with Coalition's Active Cyber Insurance
Comparable Outsourced Vendor Solution[10]		Likely prioritizes **enterprises or large-scale contracts**, often requiring 1k+ endpoint minimums.	Vendor support
Standing Up an In-House 24/7 SOC[11]		Ideal for **larger established enterprises** with any number of endpoints.	In-house monitoring and response capabilities

> **Coalition Security Services MDR customers benefit from both 24/7 real-time alerts and a team of humans to respond, whether they build it in-house or find a security partner.**

7. *2023 Cyber Claims Report Mid-year Update*
8. *Incident response services offered to policyholders via a firm panel are provided by Coalition Incident Response, an affiliate of Coalition Inc*
9. *Coalition Security Services MDR services are provided by Coalition Incident Response, an affiliate of Coalition, Inc.*
10. *The True Cost of Setting Up and Operating a 24×7 Security Operations Center (SOC)*
11. *The True Cost of Setting Up and Operating a 24×7 Security Operations Center (SOC)*

Coalition: A Leading Name in Cyber Insurance & Cybersecurity Solutions

While much has been written about the volatile nature of cyber attacks, the reality is that security teams must plan for them in a digitized economy. As such, companies can no longer pretend they are not a potential target for a cyber attack and should utilize technical solutions that can help their security and IT teams succeed.

Teams may be wary of committing to another technical solution. However, MDR is a meaningful complement to any cyber risk strategy that helps teams cover their organization's attack surface and respond to malicious activity in real time — the benefit of the expertise without the added headcount.

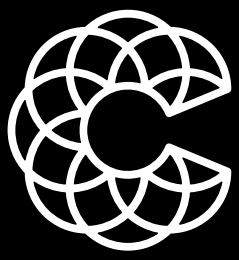
The mission at Coalition[12] has always been to protect the unprotected. Coalition Active Insurance is designed to help prevent digital risk before it strikes by combining the power of technology and insurance to help organizations identify, mitigate and respond to digital risks. By leveraging Coalition's insights on vulnerabilities, exploits and attacks, Coalition Security Services[13] MDR helps organizations stay one step ahead of emerging threats and possible events with around-the-clock threat detection and response.

We pride ourselves on our ability to help teams detect and respond to any incidents quickly and effectively, working closely with them to investigate, remediate, and communicate about any detections in a collaborative manner. Should you choose Coalition Security Services for your MDR, you can be confident that your organization can better defend itself against even the most sophisticated and elusive threats.

Learn more about MDR and other key Security Services offerings at coalitioninc.com/coalition-security-services.

Companies can no longer pretend they are not a potential target for a cyber attack and should utilize technical solutions that can help their security and IT teams succeed.

12. *Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC # 29530). See licenses and disclaimers.*
13. *Coalition Security Services MDR services are provided by Coalition Incident Response, an affiliate of Coalition, Inc.*



Coalition®

coalitioninc.com

help@coalitioninc.com

55 2ND STREET, SUITE 2500
SAN FRANCISCO, CA 94105