BINARY DEFENSE™

GUIDE

MDR Buyer's Guide

How to Choose the Right MDR Solution

BINARY DEFENSE™

Table of Contents

BINARY DEFENSE™

Managed Detection and Response, or MDR, combines people, processes, and technology to continuously monitor and analyze business environments.

BINARY DEFENSE™

What is Managed Detection and Response?

Managed Detection and Response, or MDR, combines people, processes, and technology to continuously monitor and analyze business environments. When anomalies or potential threats are detected, MDR solutions take immediate action commensurate with threat severity.

This combination ensures the efficient threat detection that traditional security measures might miss. The primary function of MDR centers on swift detection, accurate analysis, and prompt response to cyber threats.

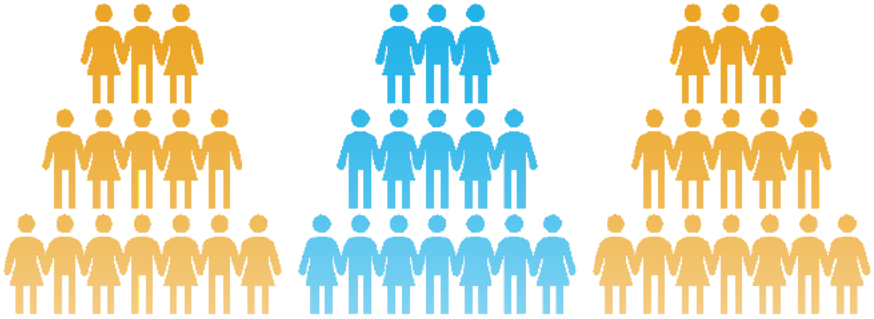
MDR solutions prioritize real-time threat identification and emphasize post-incident analysis. The analysis process helps organizations understand the nature of the threat and fortify future defenses.

In essence, MDR establishes a proactive cybersecurity approach with a focus on immediate responses and long-term security enhancements.

The importance and benefits of MDR

Every enterprise, regardless of its core function—be it manufacturing, finance, or software—is susceptible to cyber threats. Amidst a community fraught with fear-based marketing and doom-and-gloom talking points, it's worth pointing out that most people are aware of the threat environment. Bad actors are bound to attack—it's effectively countering attacks that matters most. Ensuring the security of organizational data and systems is known to be a major undertaking. Plus, while cybersecurity is critically important, its execution doesn't usually align with the revenue-generating operations of most businesses.

In the same way that homeowners don't tend to do their own plumbing or electrical, organizations don't usually do their own cybersecurity because its intricacies warrant expert support.



Building an internal MDR mechanism demands considerable resources. An organization looking to run a 24/7/365 Security Operations Center (SOC), along with an integrated Security Information and Event Management (SIEM) system, needs an in-house team of around 9-10 dedicated experts. The commitment is substantial and can detract from primary business goals. MDR services offer an optimal solution by merging expert intervention with state-of-the-art security technology.

Choosing the right MDR partner, then, is a pragmatic business decision. In a realm as complex and dynamic as cybersecurity, expertise is indispensable—and MDR is a cost of doing business.

BINARY DEFENSE™

Components of MDR

While each component of MDR has its distinct function, the overarching value is in how these components work together.

Threat Hunting and Intelligence

Part of cybersecurity's foundation is anticipating and understanding malicious activity. By gaining insights into the motives and methods of bad actors, organizations can better fortify defenses.

- **Objective:** Understand, anticipate, and react to the behavior of adversaries.
- **Function:** Collect and interpret information about how threats operate, their objectives, and methods.
- **Operationalization:** Make intelligence actionable. The value is not just in knowing, but in how information informs the defense strategy.

Detection Engineering

Simply recognizing threats isn't sufficient. Intelligence must drive real-world defense actions. This is where the art and science of detection engineering comes into play.

- **Objective:** Translate intelligence into actionable alerts to counter potential threats.
- **Function:** Leverage all available datasets, platforms, and possible intrusion points to craft precise detection mechanisms for adversarial activities.
- **Operationalization:** Ensure that identified threats immediately trigger a well-defined response, minimizing any potential damage.

Security Operations Center (SOC)

A centralized hub, the SOC, is where threats meet their match. Here, analysts evaluate, prioritize, and counter the myriad of alerts, ensuring each is addressed appropriately.

- **Objective:** Centralize response to identified threats and manage them efficiently.
- **Function:** Triage, analyze, and prioritize events based on their potential impact. Confirm benign from malicious activities.
- **Operationalization:** Provide immediate actions and recommendations in response to the identified events, ensuring threats are neutralized or mitigated swiftly.

By gaining insights into the motives and methods of bad actors, organizations can better fortify defenses.

Components of MDR (cont.)

Analysis on Demand and Incident Response

Some incidents demand heightened attention and expertise. Tailored analysis and response services cater to these unique challenges.

- **Objective:** Provide specialized attention to intricate or high-priority events.
- **Function:** Dive deeper into challenging incidents that require advanced expertise or pose a significant risk.
- **Operationalization:** Rapidly contain, scope, and remediate identified threats, working closely with stakeholders for optimal outcomes.

Continuous Security Posture Improvement

Learning from the past and adapting for the future defines an organization's cybersecurity resilience. The iterative process ensures defenses evolve and strengthen over time.

- **Objective:** Strengthen security measures based on prior incidents and evolving threats.
- **Function:** Post-event analysis and review to identify areas of improvement in defense mechanisms, tools, and processes.
- **Operationalization:** Regularly refine and adjust strategies, processes, and tools based on lessons learned and emerging threat intelligence.

Digital Risk Protection Services in MDR

As digital threats evolve, so must the strategies to counter them. Incorporating counterintelligence into MDR allows organizations to predict, adapt to, and mitigate dynamic challenges.

- **Objective:** Enhance MDR strategies with a deeper understanding of evolving digital risks.
- **Function:** Predict and adapt to potential threats, using counterintelligence as a tool to foresee and counteract emerging challenges.
- **Operationalization:** Dynamically adjust strategies to stay a step ahead of adversaries, ensuring the organization's defense remains robust and adaptable.

BINARY DEFENSE™

The MDR Market

Industry Perception

The Managed Detection and Response (MDR) market has become a focal point in the cybersecurity domain. As cyber threats proliferate and diversify, perceptions of what constitutes effective MDR are changing.

While some industry players maintain a more limited, endpoint-centric view of MDR, the broader industry is gravitating towards a comprehensive outlook. With increasing frequency, forward thinking MDR vendors are championing a broader, more integrative approach that leverages existing technological assets and integrates into the fabric of customers' security teams.

MDR vendors are championing a broader, more integrative approach that leverages existing technological assets and integrates into the fabric of customers' security teams.

Common MDR Solution Approaches

MDR market diversity is underscored by its varying solution approaches. Presently, three distinct approaches stand out:

Technology & engineering-based

Championed primarily by OEMs, this approach puts technology at the forefront. It's characterized by:

- Acquiring diverse, often newer technologies
  Integration of platforms and features
- A philosophy centered on seamless tech interoperation.

MSSP

Rooted in service delivery, this method leans on the scalability of human resources. It predominantly revolves around:

- Providing routine, sometimes lower-tier services.
- Adherence to replicable processes.
- A potentially repetitive service delivery mechanism.

Pure MDR

This paradigm bridges the above two, combining technology with service adaptability. It focuses on:

- A fusion of tech and service strengths.
- Emphasis on results and comprehensive defense.
- Shift from isolated solutions to integrated cybersecurity strategies.

The MDR Market (cont.)

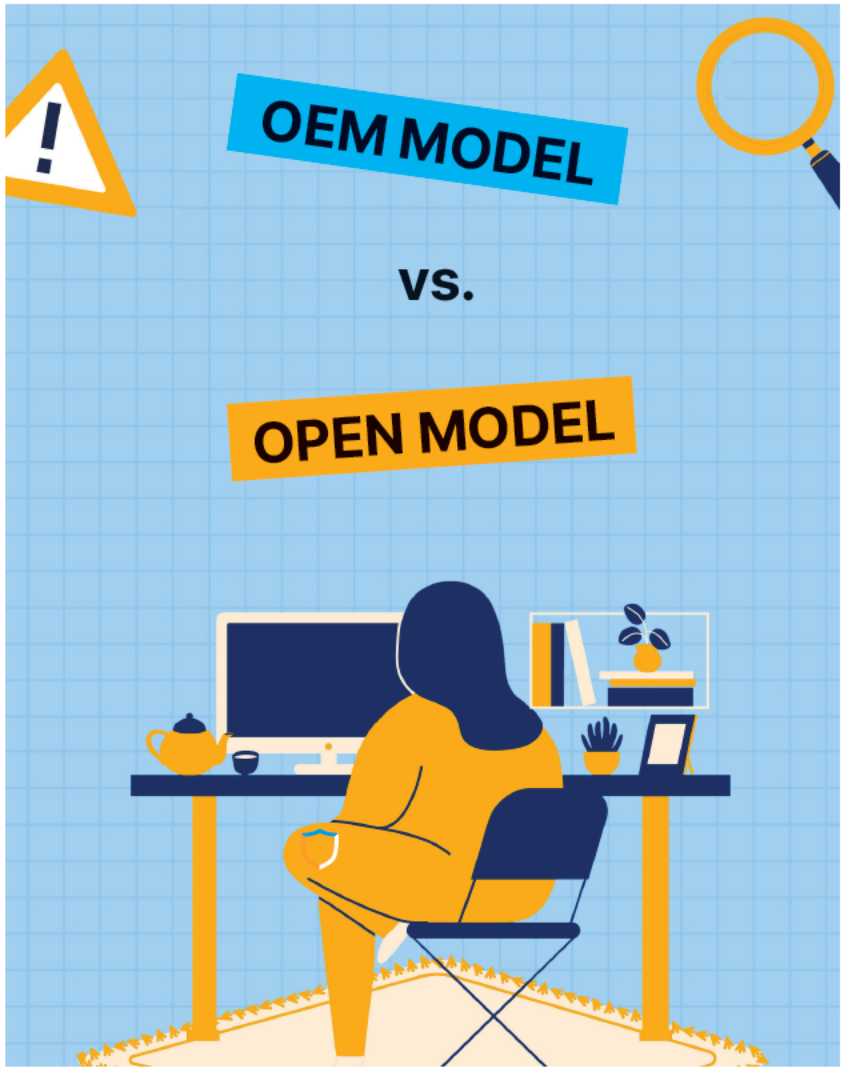
A closer look into how these solutions are typically delivered offers further insight, generally falling into one of two primary models:

- **OEM model**
  OEM MDR delivery leans heavily on proprietary solutions. Many vendor roadmaps have evolved from managed EDR solutions to full-scope MDR services. However, these offerings are intrinsically tied to OEM technologies, potentially necessitating clients to pivot to one ecosystem.

- **Open model**
  In contrast, this more flexible model centers on integration. Recognizing the significant existing technology investments of customers, their approach is:

  - Centered on complementing existing infrastructures.
  - Prioritizing customization over standardization.
  - A more flexible, customer-oriented strategy.

The MDR market landscape presents organizations with a pivotal choice: migrate to a new suite of solutions or align with a provider that synergizes with existing technologies. In either case, the decision is not solely about selecting a service or platform but choosing a strategic direction for cybersecurity.



BINARY DEFENSE™

Critical MDR solution features

Selecting an MDR provider requires understanding critical features and ensuring potential partners align with these priorities. By focusing on these objectives, organizations are better positioned to bolster cybersecurity defenses and effectively counter threats.

Here are the critical features enterprises should prioritize when considering an MDR provider:

Threat Hunting and Intelligence

- Forms the foundation of cybersecurity by understanding risks and threats.
- Gathers vital information about adversaries, their methods, and objectives.
- Emphasizes operationalizing intelligence to make it actionable.

Detection Engineering

- Transforms intelligence about adversaries into tangible alerts.
- Utilizes risk-based scoring and alerting systems to pinpoint potential threats.
- Integrates multiple datasets and platforms for a holistic view of potential attack paths.
- Correlates events between different solutions, offering a cohesive threat perspective.

SOC (Security Operations Center)

- Operates as the first line of defense, acting on the actionable data.
- Triage events, differentiating benign from malicious instances.
- Implements immediate preventative actions, from password changes to blocking communications.
- Delivers recommendations based on event analysis to help improve future responses.

Analysis on Demand and Incident Response

- Offers specialized expertise during high-priority events or breaches.
- Works alongside clients to contain, scope, and remediate incidents.
- Provides rapid response capabilities to minimize potential impact.

Security Posture Improvement

- Not a static service; emphasizes continual improvement.
- After event analysis, evaluates the effectiveness of current tools and processes.
- Identifies areas of strength and potential vulnerabilities for both the client and the MDR service.
- Recommends upgrades, updates, and adjustments to improve future defenses.

Relevant Metrics

- Prioritizes context-rich metrics over mere volume statistics.
- Seeks to answer critical questions: Why is this event significant? How did we succeed or fail? How can we improve?
- Measures the effectiveness of the defense, looking for consistent maturity and growth in the client's security posture.

BINARY DEFENSE™

How to choose an MDR solution

The right provider will work seamlessly with a company's existing infrastructure while proactively mitigating potential threats. However, choosing the right MDR provider is contingent upon a comprehensive understanding of their technology, operations, and business partnership potential.

MDR solution checklist

TECHNOLOGY

+ Platform Compatibility

- Can the provider integrate with your Security Information and Event Management (SIEM) platform?
- Can the provider work effectively with your Endpoint Detection and Response (EDR)?
- How efficiently can they bridge your different technological platforms?

+ Data Management

- Will the provider need to extract and hold your data, or can they operate while you retain data sovereignty?
- Is there a mechanism in place to ensure data integrity and confidentiality?

+ Environment and Infrastructure

- Does the provider offer support within your existing environment, without necessitating drastic changes?
- Is there assistance available to manage your platforms effectively?

+ Platform Management

- Some providers delve into SIEM management, a potential drawback for businesses not looking for Managed Security Service Provider (MSSP) attributes.
- On the other hand, platform management can alleviate challenges for companies and can be a valuable addition to the MDR service.

+ Customization and Enhancement

- Can the provider assist in the development of custom use cases tailored to your business needs?
- Is there support for the implementation of controls, mitigations, and remediations following incident detection?

OPERATIONS

+ Availability

- Is the provider available 24/7, ensuring consistent monitoring and swift response?
- Are there dedicated personnel available for communication, or are resources shared among multiple clients?

BINARY DEFENSE™

How to choose an MDR solution (cont.)

OPERATIONS (CONT.)

+ Skill sets
- What is the range of skills available to you from the provider?
- Does the provider offer expertise in areas such as forensics, threat hunting, incident response, and detection engineering?

+ Response and reporting
- What is the typical response time from the provider following an incident?
- Beyond ticketing, what type of data and context is provided to the client regarding threats and responses?

+ Additional capabilities
- Beyond core MDR functionalities, what additional capabilities does the provider offer?
- How does the provider define and approach investigations?

BUSINESS PARTNERSHIP

+ Billing and charges
- Understand the provider's billing method. Is it monthly, quarterly, or annually?
- Are there transparent guidelines on how charges are calculated?

+ Engagement frequency
- How often does the provider engage in meetings, updates, and reviews?
- What mechanisms are in place for you to communicate concerns or issues to the provider?

+ Flexibility
- Gauge the provider's adaptability in delivering and structuring services tailored to your needs.

When evaluating MDR providers, it is essential to have clarity on your organization's specific needs and how the potential provider can fulfill them. With this checklist, businesses can make informed decisions, ensuring a partnership that enhances their security infrastructure and aligns with their operational and business objectives.

BINARY DEFENSE™

MDR with Binary Defense

Who we are

Binary Defense operates at the forefront of the battle against cyberattacks, grounded in its unwavering mission to make the world a safer digital realm. Recognizing the profound implications of cyber threats that can derail major enterprises or expose vast amounts of sensitive data, the company continually reinforces its commitment to cybersecurity excellence.

What we do

Binary Defense firmly believes that technology, in isolation, is insufficient to thwart cyberattacks. Instead, it's the harmonious melding of expert teams with deep insights into cyber attackers' methodologies, tried and tested processes, and cutting-edge technology that delivers robust protection against threats. With a 24×7×365 Security Operations Center (SOC) at its core, Binary Defense extends far beyond just sending alerts. They provide an encompassing protective shield, wherein their SOC analysts undertake exhaustive investigations to furnish clients with a comprehensive picture of their threat landscape. Trust is the cornerstone of their strategy. By embracing a transparent and consultative approach, they ensure clients are consistently updated on their security stance, with a ticketing system that sheds light on every ongoing investigation.

Binary Defense firmly believes that technology, in isolation, is insufficient to thwart cyberattacks.

BINARY DEFENSE™

MDR with Binary Defense (cont.)

MDR — The Binary Defense Way

> "The most valuable part of Binary Defense is its team of cybersecurity analysts. Their analysts filter out the noise and only forward the critical threats that require a response instead of false positives."
>
> – VP of IT at Manufacturing Company

Managed Detection and Response (MDR)
Binary Defense's MDR service amalgamates human acumen with technology. It's engineered to heighten visibility and declutter the intricate web of security challenges. The analysts, ever-vigilant, not only preemptively detect threats but also fathom the unique intricacies of each client's environment, offering actionable recommendations.

Visibility and strategy
By synergizing Threat Intelligence, Technology, and Tradecraft with benchmark industry protocols, Binary Defense crafts solutions that squarely address today's security conundrums. They adopt an Open XDR Approach, enabling clients to retain their existing tech ecosystems, and dovetail with controls across varying platforms.

SOC monitoring and investigations
Their SOC, operational without interruption, meticulously filters out false alarms and probes deeper into events that mandate a closer examination, ensuring clients are always a step ahead.

Response and containment
Binary Defense distinguishes itself by escalating not just threats but offering tactical and strategic countermeasures. If needed, a broader spectrum of response capabilities, encapsulating Analysis-on-Demand and Incident Response services, is at the client's disposal.

Continuous improvement
The wealth of insights gleaned from SOC observations and threat intelligence research is consistently funneled back into refining client environments, bolstering defenses, and ensuring they remain on the cutting edge of cybersecurity.