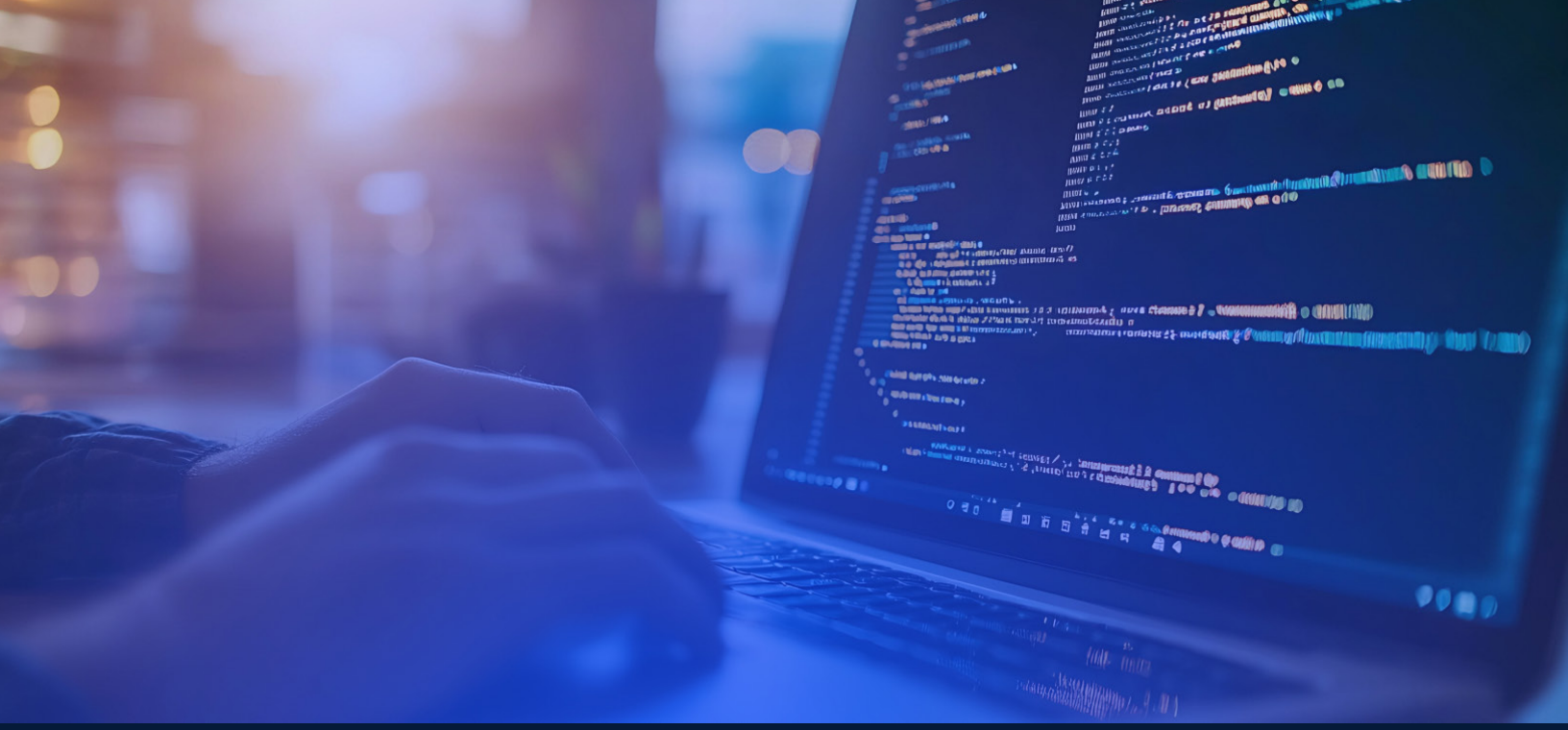

How to Choose the Best Managed Detection and Response (MDR) Partner.

A Buyer's Guide for CISOs

digital hands®

Table of Contents

Innovative threat actors are constantly adapting their tactics to the advancements in security defenses. They're now executing malicious activities like ransomware deployment within hours rather than weeks.[1] With information stealing malware, they can exfiltrate data from a device in mere seconds.[2] Speed is everything for defenders in this environment. Fast, effective response action can mean the difference between a quickly eradicated threat and a full-scale breach.

Effective response takes a mix of advanced technology, human expertise, threat intelligence, and advanced analytics. But many organizations don't have the in-house resources or holistic visibility to provide real-time, continuous threat detection and response. And those that do may be looking for ways to optimize and scale their security operations more efficiently.

All these factors are contributing to a brisk demand for managed detection and response (MDR) solutions. As digital transformation marches on — increasing the attack surface and the need for fast response to advanced threats — a growing number of organizations are turning to MDR vendors for advanced security services. But the MDR market is inconsistent, and many vendors that position themselves as MDR players only offer a limited set of capabilities.

This guide walks you through the MDR market differentiators and the recommended essential criteria that can help you evaluate your options.

[1] ThreatDown, Malwarebytes, June 2024
[2] Secureworks, Threat Analysis, May 2023

An MDR or *not* an MDR provider?

The key is in the 'R'

The MDR market is growing rapidly, buoyed by trends like remote work and growing complexities of hybrid security environments. Gartner estimates that there are more than 600 players in the MDR marketplace. Not all vendors in this diverse landscape live to the full definition of MDR, however.

The marketplace has four main categories of providers

Point solution technology vendors

These vendors specialize in automation to detect and respond to threats within their platform's domain, such as endpoints. While effective for addressing domain specific challenges, they don't necessarily integrate or correlate data across your full security ecosystem.

More critically, these technology providers don't manage or optimize the tools they rely on, such as firewalls or SIEMs, leaving your team responsible for upkeep and tuning. This can create a false sense of security, with blind spots in areas their platform doesn't cover and gaps in operational alignment that attackers can exploit.

[3] MSSP Alert, August 2023

Platform-centric MDR Providers

This emerging category touches on vendors that emphasize automated response actions but minimize—or sometimes entirely exclude—human expertise. These vendors often tout flashy portals and rapid response times but leave customers to manage critical actions themselves that go beyond what the automation can handle. Without human intervention, they struggle with false positives, nuanced triaging, and complex threats requiring human expertise for deeper investigation.

> Moreover, platform-centric providers prioritize their proprietary systems above all else, often neglecting proper onboarding and tuning of your tools. These providers write rules and detections for their global customer base or to streamline their own internal SOC operations-but not for your unique needs.

MSSPs offering evolved threat management services

Managed Security Service Providers (MSSPs) traditionally provide monitoring, device management, and compliance support. Many are transitioning to offer broader threat detection and response capabilities but may still rely heavily on more human-driven processes. This blend makes MSSPs appealing for organizations seeking operational stability while managing and optimizing their security environments.

Integrated MDR Service and Managed Security Service Providers

Leading providers combine MSS and MDR capabilities, recognizing that comprehensive response actions require not only automation but also the continuous upkeep and management of security technologies. These providers deliver integrated solutions that:

- Respond to threats across endpoints, networks, and other assets.
- Manage security infrastructure, such as firewalls and SIEMs, to ensure operational readiness.
- Offer human expertise to analyze, correlate, and validate incidents alongside automated responses.

Unfortunately, many so-called MDR vendors fall short by overlooking the R in MDR: response. And response requires more than just automation – it demands a team of 24/7 security operations professionals who can augment the automations and take action And response takes humans — a team of experts in a 24/7 “eyes on the glass” security operations center (SOC) who can respond to threats in real time, augmenting technology with human intelligence.

Attackers are harnessing automated tools and new technologies to move at astonishing speed. You can’t afford to waste time waiting for alerts to come your way, whether from a platform or a human. You need an expert team who can provide immediate response action — combining their experience, intuition, and expertise with an advanced security fabric, automations, threat intelligence, and advanced analytics.

What to look for in an MDR provider

There's much more to MDR than simply the underlying SIEM and SOAR platforms. When considering vendors, evaluate not only their technology but also their security operations and business model.

1. A truly composable security approach

In today's crowded MDR market, many providers fall short of delivering true composable security. They claim to be vendor-agnostic but often provide only basic API connectors that pull data without fully integrating or managing your tools, creating a false sense of security.

> These providers don't take responsibility for managing or tuning critical tools like firewalls, SIEMs, or endpoint solutions, leaving the burden on your team. If you part ways, you're often left with misconfigured, outdated technologies and disrupted workflows. Instead of strengthening your security posture, these solutions can erode it over time, adding complexity and limiting growth.

True composable security offers flexibility—enabling you to integrate, optimize, and manage tools that align with your business. It ensures your environment is scalable, resilient, and prepared for evolving threats.

2. Visibility into Your Security Posture

True visibility isn't just about tracking alerts—it's about transparency across your entire environment. It empowers every stakeholder, from the boardroom to the SOC, with the insights they need to make smarter decisions. Without it? You're stuck with an MDR provider that operates like a "black box," leaving you in the dark about critical actions and outcomes.

Effective visibility bridges the gap between tactical operations and strategic oversight. It helps you reduce risk, improve your security posture, and continuously mature your program. Look for a vendor with a portal that's user-friendly, collaborative, and accessible anytime, anywhere.

> For executives, it should offer high-level metrics—risk scores, MTTD, and MTTR—so they can see the big picture at a glance. For the SOC, it should act as a real-time communication hub, providing granular insights into incidents, attack vectors, affected devices, coverage, and kill-chain paths. But it's not just about data. Visibility should help you tell a story. A story about how your organization is reducing risk, containing threats, improving response times, and meeting compliance goals. The right MDR partner doesn't just hand you tools—they deliver meaningful progress you can see and share.

3. People Expertise

Your MDR provider's experts should feel like a natural extension of your security team—on-call 24/7 and equipped with the expertise to protect your environment. This team needs to include seasoned professionals with diverse skill sets: analysts, threat hunters, content creators, and incident responders, all working together to keep you ahead of threats.

But expertise isn't just about responding to incidents. Humans are critical to ensuring your technology stack is properly onboarded, tuned, and optimized. They select high-value data sources, craft effective detection rules, and configure your SIEM. They validate content, confirm parsing accuracy, and ensure that specific activities trigger meaningful alerts. They also review data to make sure it's actionable—not just noise.

> Your MDR partner's team should have deep knowledge of your specific technologies, ensuring your tools don't just function—they perform. Without this human touch, your security stack risks falling short of its full potential.

4. Customization Based on Your Needs

Your MDR partnership shouldn't feel like a "one-size-fits-all" solution. While most providers offer some level of customization, not all are willing to tailor their processes or automations to fit the specific needs of your organization.

> Choose a partner who lets you collaborate and decide how involved you want to be. Do you want certain response actions fully automated during off-hours but handled manually when your team is available? Should the external team take charge of critical incidents, or would you prefer to receive only the most urgent alerts to make decisions yourself? The right provider adapts to your workflows, not the other way around.

5. State-of-the-Art Technology

Although human intelligence is a core component of the MDR solution, technology is an important enabler. Many MDR vendors offer proprietary platforms—a security fabric—designed to overlay your existing security stack and enhance its capabilities.

A cloud-based platform with seamless integration and fully automated features enables the SOC team to make swift, informed decisions. It should pull in up-to-date threat intelligence from diverse feeds and map detections to best-practice frameworks like MITRE ATT&CK, ensuring comprehensive coverage and actionable insights.

> The best MDR providers deliver a platform that not only integrates with a wide range of security technologies—including those they don't manage—but also empowers your team to execute response actions effectively. This flexibility ensures your security ecosystem remains cohesive and ready to tackle evolving threats.

What to Look for in a SOAR

A SOAR (Security Orchestration, Automation, and Response) platform is the backbone of an effective MDR solution, tying together data, workflows, and automation to streamline security operations. By aggregating and correlating data from various sources, SOAR provides analysts with actionable intelligence to quickly detect, analyze, and respond to threats. It's the ultimate enabler for SOC professionals to manage complexity and act with precision.

A SOAR should:

- ✓ **Enable proactive threat hunting** by providing the workflows that help surface real threats and search for indicators of compromise
- ✓ **Support centralized incident management** by consolidating data into a single, accessible view to enable fast triage and response and allow analysts to view relevant data so that they don't have to swivel seat between technologies
- ✓ **Aggregate threat intelligence** from multiple threat intelligence sources for enriched alerts and investigations
- ✓ **Automate repetitive tasks** such as alert categorization, prioritization, and detail gathering to free up human expertise for the more complex threat investigations
- ✓ **Support remediation and recovery** efforts so you can quickly contain the damage from an incident and restore operations

What to Expect from Your Partner

Whether you're working with an incumbent or evaluating a new vendor, how can you ensure they're delivering on their promises? Your MDR provider should consistently meet the outcomes you hired them for. **Here's what to look for during the critical detection and response phases:**

Data Enrichment and Analysis

Data enrichment combines machine and human intelligence to turn raw information into actionable insights. The process begins with your provider selecting the right logs and data sources to monitor and aggregate—decisions that set the foundation for effective detection. Poorly investigated alerts can overwhelm your SOC with noise or leave critical threats undetected. While a well-tuned SIEM surfaces the most important alerts, it's human expertise that asks the key questions: What does this alert mean? What's the best response? **SOAR platforms take analysis further by correlating data from diverse sources and layering in threat intelligence.** The best MDR providers subscribe to multiple high-quality intelligence feeds, enriching their understanding of potential threats and ensuring more accurate detections.

Response Processes

When seconds matter, you need a partner who can deliver response at machine speed. Automation plays a critical role in this, but not every response should be automated. Your MDR solution must fit seamlessly into your business model and align with your organization's unique risk tolerance. Your MDR provider should offer flexibility, letting you choose which actions are automated and how. For instance, automation might isolate endpoints, block malicious IPs, or force multi-factor authentication resets. **Meanwhile, human analysts can handle nuanced threats that require deeper investigation. This balance ensures speed without sacrificing accuracy.**

Communication Procedures

A partner who's an extension of your in-house team needs to have outstanding communication skills and understand both your industry and your unique threat landscape. This team, in fact, should understand your environment as well as you do — or even better than you. When every second counts, a vendor who routes you to offshore support and to a que of numerous requests may not deliver you the best outcomes. Nor is this vendor likely have deep knowledge of your environment to offer customized support. Look for a partner who also offers flexibility in terms of division of responsibilities. **While your MDR partner should lead the charge in most cases, they should work closely with your team to ensure alignment and clarity on critical actions. This shared accountability guarantees a unified, efficient response when it matters most.**

Remediation and Recovery

While remediation and recovery are typically the responsibility of your IT team, your MDR provider should play a supportive role during this phase. For instance, the external team can identify a compromised endpoint and isolate it from the network. If the device is infected, your team would follow your internal recovery procedures for rebuilding the device, restoring the data from backup.

8 Questions to Ask Potential Partners

1. What is your average time to value?

Onboarding sets the tone for the entire partnership. Ask how quickly they can integrate your environment without disrupting operations. A solid MDR partner should ensure your tools are properly tuned and optimized from day one, not just bolted on. If they can't explain how they'll handle your setup without headaches, it's a red flag.

2. How do you ensure my technologies stay tuned over time?

Getting started is one thing—staying optimized is another. Your MDR provider should actively monitor and adjust your tools, like firewalls and SIEMs, to keep them running at peak performance. The right partner doesn't just react to changes; they adapt, keeping your defenses sharp as your environment evolves.

3. How do you measure and demonstrate value?

If you can't prove ROI, what's the point? Your provider must offer clear metrics that matter: reduced risk, MTTD, MTTR, and whether you're adequately covered against the latest threats. Are they helping you identify and respond to threats effectively? Are they reducing the severity and impact of attacks? Most importantly, are they improving your overall security posture?

A strong MDR partner should provide actionable insights that translate into business value. This includes detailed dashboards for your SOC and high-level, executive-friendly reports for the board. If they can't show you how their efforts are moving the needle, they're not delivering what you deserve.

4. How do you handle critical incidents and keep me informed?

When it hits the fan, you need a partner—not just a vendor. Your MDR provider should act as an extension of your team, with a clear escalation process that ensures you're never left guessing. You shouldn't be stuck in a support queue or handed off to analysts or engineers who don't know your environment.

Expect a partner who understands your setup inside and out and approaches each escalation as a chance to strengthen your defenses. Every incident should be treated as an opportunity to improve your security posture against similar threats in the future.

5. What flexibility do I have to adjust the engagement model?

Your business isn't static, and your MDR provider shouldn't be either. Ask how they'll adapt their approach to your evolving needs, whether that's tweaking automation, increasing human oversight, or adjusting to changes in your risk tolerance. The best partners meet you where you are—and grow with you.

6. What environments do you protect?

Not every vendor can handle the complexity of hybrid environments. Your MDR solution needs to work seamlessly across on-premises systems, public clouds, private clouds, and everything in between. If they can't provide consistent protection across all your assets, they're not the right fit.

7. How do you ensure you have the right data?

Your detections are only as good as your data. A capable provider will audit your logs to ensure parsing is accurate and actively monitor for gaps. If they can't tell you how they'll prioritize high-value sources or fix data issues, they're leaving your defenses to chance.

8. What kind of expertise does your team have?

Technology is only as good as the people behind it. Your MDR provider's team should bring deep expertise and continuous training to the table. They need to know the latest threats, understand your unique environment, and ensure continuity even if turnover happens. Anything less isn't enough.

Final Thoughts

When you're looking for a new trusted partner, think in terms of the outcomes you want from your relationship.

- Do you want a platform with bells and whistles you'll never use because they don't apply to your unique environment? Or do you want a responsive, flexible team whose priority is to keep you secure — a team who's focused on safety and security outcomes rather than being hung up on the number of their AI response actions?
- Do you just want machine automation? Or do you want technology-enabled human experts who can respond at machine speed?
- Do you want someone who can detect and respond to threats and call it a day? Or do you want a partner to provide strategic guidance?

While the marketplace is teeming with MDR providers, few rise to the top with the combination of industry expertise, best-in-class technology, flexibility to meet you where you're at, and a concierge approach to service delivery. Find a partner who can deliver on all these criteria of excellence — and continues to improve and evolve as the threat landscape changes.

About Digital Hands

Digital Hands is a cybersecurity service provider that blends Managed Detection and Response (MDR) capabilities with Managed Security Services (MSS) to protect your organization's most critical assets. With more than 20 years of experience, we have provided security services behind the scenes of many leading security vendors globally. We deeply care about our customers and serve as an extension of their security teams, helping them stay ahead of cyber threats with precision, automation, and expertise. Our composable approach to security and combination of best-in-class people and technologies allow us to deliver smarter solutions that support our customers wherever they are on their security journey.

There's a reason why our tagline is Get There First: it's our mission. Speed is still everything in today's landscape. When you partner with us, you get a proactive partner who goes beyond SLAs to keep you ahead of every threat — every time.

Learn more at digitalhands.com