

Bitdefender's MDR Buyers Guide: 2025



How to Determine Which MDR is Right for Your Organization

So you've decided to partner with a Managed Detection and Response (MDR) provider. You have self-assessed your posture, identified security gaps, and are now choosing to invest in cybersecurity. With so many MDR options, each with its unique approaches and flavors, how do you determine which vendor is right for your business?

In this guide, we cover the different types of MDR providers available, their pros and cons, and questions you can ask to evaluate your organization's needs and align them with a particular vendor. We provide a phased approach to the evaluation, guiding you through the process to determine not only the right type of MDR, but the right vendor to meet your business and security needs.



MDRs Explained: A Trusted Security Partner That Helps Protect Your Environment

An MDR helps organizations address cybersecurity risks. It provides the manpower, expertise, and resources (which the customer organization likely lacks) to detect and respond to threats. In essence, an MDR serves as an outsourced Security Operations Center (SOC). Rather than building a team internally, organizations can hire an MDR to handle the same security functions.

MDRs are extremely flexible and can customize solutions to fit into your existing security infrastructure (tool stack, network design, endpoints, etc.) and fill security gaps as needed. They can provide support and services to match the needs of organizations of all sizes.

For instance, a company with a small (or no) IT security team might use an MDR as a full-stack SOC. A larger enterprise with an established internal security team, however, could use an MDR as an extension of their team to “beef up” the frontlines. They can offload specific security tasks, or get an additional pair of eyes in the network.

Most (we’ll dive into this later) can also provide services beyond detection and response, such as threat research and intel, detection engineering, proactive security guidance, and other offensive-type services.

MDRs are extremely flexible and can customize solutions to fit into your existing security infrastructure



Universal Evaluation Criteria

Before diving into some of the nuances between different MDRs, it's important to note that there are certain metrics and criteria that all MDRs should provide and adhere to. Here are a couple to help you during your evaluation process.

Metrics & SLAs

Before finalizing an MDR agreement, it's important to understand the metrics used to evaluate the quality of service being provided. Work with the MDR provider closely to understand the Service Level Agreements (SLAs) that define performance expectations around things like Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), false-positive rates, reporting and alert cadence, escalation timelines for critical incidents and whether the MDR offers real-time dashboards or updates to track performance.

However, it's also important to be wary of vendors whose SLAs seem a little too good to be true. While having extremely low MTTD and MTTR numbers can look good on paper, those can also be misleading. For example, extremely low MTTD numbers guaranteed in an SLA likely indicates the vendor is not performing deep enough investigations to make meaningful decisions on whether an alert or event is a real threat or false-positive.

Be careful prioritizing speed over quality. [While tracking various metrics are important](#), it's better to understand how the MDR works to provide you proper service to detect and stop threats.

Integration with Existing IT & Security Processes

Integrating into your existing processes is very important when evaluating MDRs. An MDR that can detect threats but can't integrate into your existing workflows and processes to help alert you and respond lacks the ability to provide the necessary capabilities to protect you from threats.

Does the MDR align with existing incident response playbooks, ticketing systems, and escalation workflows? For example, using platforms like ServiceNow or Jira to track incidents can reduce delays in remediation.

24/7 Coverage Clarification

Not all MDR services operate 24/7/365 by default. Some offer business-hours monitoring and only include extended coverage if purchased. Confirm coverage hours and whether incident response is available outside of regular business hours.

Compliance & Regulatory Considerations

Compliance obligations such as HIPAA, PCI DSS, GDPR, or CCPA often influence MDR selection. Buyers should evaluate whether the MDR provider can supply compliance-specific reporting, maintain audit-ready logs, and help fulfill mandated security controls. When it comes to compliance, you need security specialists.



The Two Primary Types of MDR

Most MDRs fall into one of two categories: Third-party tool/vendor agnostic or platform-native. The primary difference? Whether the MDR is a service built on top of a security provider's own platform or acts as a third-party, standalone service, you can integrate with other tools. So your first major decision will determine which route best fits your tech stack, security needs, and IT operations.



Here are some brief evaluation questions to kick off the process:

- ▶ What does your security stack look like right now, and what are your security goals for the future?
 - ↳ What tools do you have in your environment?
 - ↳ Are there tools you're looking at or open to transitioning to?
 - ↳ If you currently have multiple different security tools deployed in your stack, how much time do you spend managing each one?
 - ↳ How are you correlating threat data across different environmental tools? (For instance, sourcing event log data from various endpoints, network, and identity tools.)
- ▶ What's your budget for building an overall security program, and where do you put the costs in terms of spending priorities?
 - ↳ Who determines the budget? Are they flexible on allocation amounts?
 - ↳ Who is the final decision maker, and how are you navigating objections they may raise when deciding which tools or services to invest in?
 - ↳ Are the security leaders, other stakeholders, and final decision makers aligned on security and business needs?
 - ↳ Is reducing operational overhead or tool complexity a top priority for your team this year?
- ▶ How important is it that you invest in "best-of-breed" or "top-of-the-line" tools across each security category?
- ▶ Would consolidating around a single platform simplify your security stack? If so, how would those tools get operationalized and managed?
- ▶ How important is it to have detection and response capabilities fully optimized for your existing tools?
- ▶ Would having a single vendor responsible for both the technology and the service give you greater confidence in threat coverage and accountability?

Answer these questions, and you'll understand what type of provider best suits your needs. Now let's lay out some pros and cons of each MDR type to help align the results from your responses above.

Third-Party / Vendor-Agnostic MDR

Here are your standalone services. Built to integrate with other vendor security software, they often don’t have their own tools. Instead, they support your current security ecosystem via integration.

So, rather than transitioning you to their platform, they can sit on top of your currently deployed tools. From there, they ingest data, perform their own investigations, and monitor threats.

PROS	CONS
Broad technology compatibility	Shallower tool-specific integrations
Faster time to value	Dependence on customer tools
Independence and objectivity	Risk of service interruption
Ease of evaluation and switching (migrating) tools	Complex Pricing Models
	No ownership of response capabilities

Pros

The primary benefit of vendor-agnostic MDRs is their flexibility. They can integrate with and support your existing environment now and into the future. In other words, no matter the security tools you have in your environment, these MDR vendors can likely integrate and support them (almost) immediately.

They are also more future-proof. Considering switching from your current EDR or another tool to a competitor? These MDR providers can continue supporting you during and after that transition. If you value that level of flexibility and foresee continuing to invest in a variety of security tools, then these types of MDRs are your best option.

But flexibility isn’t the only advantage here. One of the most compelling value-adds of vendor-agnostic MDRs is their independence and objectivity. Because they support a wide range of third-party tools and don’t have their own endpoint or network protection products to push, they don’t have an incentive to steer you toward a particular product line that might not suit your needs.

This independence is clearly apparent in two critical ways:

- ▶ How they detect and respond to threats.
- ▶ The guidance they provide along the way.

You can expect unbiased detection and response workflows via vendor-agnostic MDR. They’re not built to showcase a particular tool but to stop real threats as quickly and accurately as possible. You’re also more likely to receive security guidance and recommendations tailored to what’s best for your environment.

Cons

While vendor-agnostic MDRs’ flexibility is a major selling point, this approach also has some pitfalls. Heavy reliance on third-party tools can ultimately introduce friction, challenges, and, in some cases, risk.

Not all integrations are created equal, nor do they take the same amount of time to build and deploy. There’s a broad spectrum of depth across MDR providers. Anyone can hook into a public API to ingest alerts from a security tool, **but is that enough?**

If your MDR only consumes pre-filtered alerts based on severity, how much real value is being added? While that simple level of alert triage might be enough for some businesses, it could fall short for what's needed to detect and respond to today's advanced threats.

Some vendor-agnostic MDRs do go further. They partner with the security tool vendors to build deeper integrations that pull in raw telemetry and network or user log data (rather than just alerts).

In these scenarios, the MDR can run its own analysis, investigate suspicious behaviors independently, and identify threats that may have slipped through native detections. While that's a significant leap in capabilities, it also means a larger investment and commitment.

Here's where the reality check comes in: Deep integrations take time. Some could take months or even a year to build. So, not every tool you use today will be fully supported, especially if it's a less widely adopted product. And even if it does eventually get supported, it could take a while to develop.

Now you have to ask: What happens if your MDR doesn't support a key tool in your environment? Are you willing to wait for them to build the integration? Should you switch to a tool they do support? Neither option is ideal in terms of speed or security.

And let's not forget the fragility of third-party integrations over time. Most security vendors aren't obligated to notify their partners when they update APIs, add new telemetry sources, or roll out features.

So when they do make changes, the partner (in this case the MDR), often finds out the same way you do - after the fact. That's an awareness delay and a lapse in coverage. Any broken workflow could be a security gap in your detection and response capabilities.

Bottom line: While vendor-agnostic MDRs offer impressive flexibility and independence, they're also more exposed to the pace and unpredictability of other vendors' development cycles. The more complex and diverse your toolset, the more moving parts your MDR has to track, making it harder to ensure consistently high-quality security coverage across your environment.

The Question of Breadth vs Depth

If you decide a vendor-agnostic MDR provider is the right choice, the next step is to determine which provider best fits your environment. A key difference in this arena is breadth versus depth.

Some MDRs prioritize connecting with *as many* security tools as possible (**breadth**). This route works well if you already have a large tool stack and want broad support across your entire ecosystem. The trade-off? Many of these integrations are surface-level. They prioritize ingesting alert data but can't necessarily analyze raw data or use more advanced response features.

Alternatively, other MDR vendors prioritize **depth**. They may only support a few tools, but go much deeper into the ones they do. This means they can collect and analyze raw telemetry, run advanced detections, and take more meaningful action when threats are found. The results usually have better detection accuracy and fewer false positives. Be advised, however, that if you have a less common security tool, it may take time for the MDR to build that integration.

The right fit ultimately depends on your needs. A breadth-focused MDR is the way to go if you aim to centralize alerts across a complex toolset. But if you're looking for stronger investigation capabilities and more proactive threat detection, a depth-focused approach delivers better results (even if it supports fewer tools).



Platform-Native MDR

Platform-native MDRs build their services out using their own security tool ecosystem (rather than third-party tools). Because they’re delivered directly by the security platform provider, these services are deeply integrated into that vendor’s ecosystem. They leverage proprietary APIs, telemetry, and automation workflows that are often unavailable to third parties. However, some have expanded support to other third-party tools to provide a broader range of coverage and meet their customers “*where they are.*”

Platform-native MDRs are either sold as an add-on to existing licensing or bundled into a broader solution, providing packaging and cost-saving incentives.

PROS	CONS
Deep integration with the vendor’s tools	Limited to a single vendor’s ecosystem
Optimized telemetry access	No or limited support for third-party tools
Streamlined deployment	Potential bias in guidance
Access to proprietary features	
Bundled pricing	

By keeping everything under a single platform, the provider can handle deployment, configuration, and ongoing service.

Pros

The biggest benefit of platform-native MDRs is the depth of integration with their security tools. When your vendor and service provider are the same, any back-end communication between the SOC analysts and tool development teams along with the data flow between security tools and MDR platform will be far more efficient and collaborative since it’s managed “*under the same roof*” and not via third parties.

First, the MDR can work directly with the software developers on the integration. So any updates, added features, or other new capabilities are factored into the MDR service *during* the development stage, rather than reacting after release. There’s also the benefit of mutual collaboration.

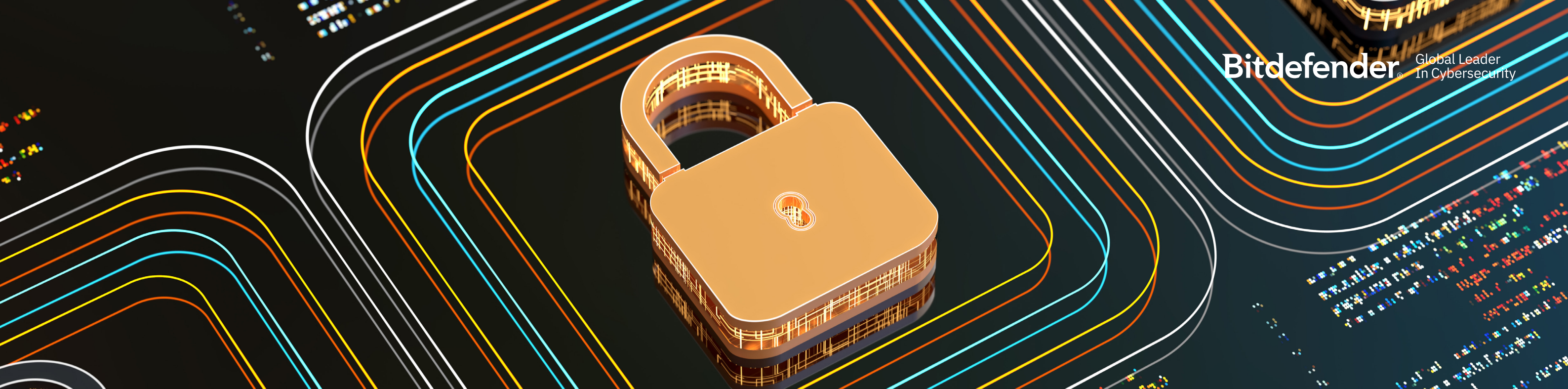
The MDR team can provide ongoing feedback on the tools to guide future updates or general improvements for the software itself. For instance, a developer can incorporate new data (supplied by SOC analysts) on tactics, techniques, and procedures (TTPs) to improve a tool’s detection abilities so the MDR can function better.

This direct communication means a deeper integration enabling the MDR to leverage proprietary telemetry, behavior analytics, and response capabilities that are often inaccessible to third-party providers. The result:

- ▶ Context-rich threat detections
- ▶ Faster correlation between data sources across the tech stack
- ▶ Quicker containment when an incident occurs

Rather than relying on high-level alert data or API-limited access, platform-native MDRs can ingest raw, high-fidelity telemetry, which improves visibility, reduces false positives, and allows the provider to take precise, informed response action quickly.

By keeping everything under a single platform, the provider can handle deployment, configuration, *and* ongoing service. As the customer, this means a linear process for minimal downtime (common during maintenance periods) and better overall tool performance, closing any possible security gaps while improving your threat coverage.



We can't forget about the cost savings platform-native MDRs provide. Most platform-native MDRs are bundled or sold as a discounted add-on to existing licensing, lowering your total costs. And in a world loaded with budget-conscious C-Suite leaders, this offers an affordable way to access the tools and security expertise required for robust threat protection.

Most organizations have made a shift. Where once investing in the most top-of-the-line tooling was a priority, it's now about moving to single-platform security vendors to cut costs without sacrificing protection.

And with the complexity of modern (ever-growing) IT environments, the required security tools continue expanding. So, having in-house expertise to manage, maintain, and fully operationalize the security stack is becoming harder to come by.

Cons

Now for the drawbacks. Being tied to a single vendor means less flexibility in the tools you can use in your security environment. Future migrations or transitions are significantly more difficult if you encounter a problem with your security platform and want to switch it out.

Similarly, going with a platform-native MDR means change. Say you have different, unsupported security tools. In this case, you'll need to transition to the vendor's specific suite of tools before getting the MDR up and running, adding additional complications and time to deploy.

The capabilities from tool to tool could also differ significantly. For example, security companies that began with endpoint security will likely have solid endpoint protection and response (EDR) tools, but may lack coverage in other areas like network and identity management. It's up to you to decide how significantly this affects the overall protection the vendor and MDR service can offer compared to other options.

What Other Services Are on Offer?

If you choose the platform-native MDR route, the next step is to evaluate the provider market. Much of your decision criteria will revolve around how each platform's capabilities compare. Since our focus is on MDR, let's focus on the service aspect.

For most of the *"end-to-end platform"* companies, it comes down to the type and amount of services offered (either as part of the MDR or in conjunction with it). As Jeff Pollard, Vice President and Principal Analyst at Forrester has noted: ***"But detection and response is no longer enough for providers; customers now demand that their MDR providers become more proactive. An MDR provider's ability to positively influence the security of its customers now matters as much as its ability to find threats."***

Pollard has frequently found that while customers are satisfied with the quality of MDR service, they often wish those providers had additional support and capabilities beyond reactive detection and response. And you may agree with this sentiment. During discovery conversations, it's always worth asking: ***"What else can they help you with beyond detection and response?"***

Look for offerings that extend the value of the MDR relationship (*threat intel and research, data and brand protection in the dark web, exposure and attack surface management, advisory services, and proactive guidance*, etc.) These additional capabilities are game-changers for teams looking to mature their security programs while keeping internal workloads manageable.

Choosing the Right MDR

There's no one-size-fits-all MDR. The right choice depends on your current IT environment, compliance requirements, future plans, internal security expertise, and overall risk tolerance. It's all about finding a partner that aligns with how you operate and grow your security program. The evaluation process should be rooted in such, guided by the trade-offs between different MDR models.

Assess your technology stack, team's bandwidth, and appetite for standardization versus flexibility in your SOC. Consider whether you're best served by a tightly integrated, all-in-one platform or a modular approach offering broader compatibility.

- ▶ What level of partnership do you expect?
- ▶ Are you seeking complete hands-on remediation, or primarily alert filtering and guidance?

We covered a lot of the questions you should be asking above. But here are a few to get your evaluation started today:

- ▶ Is an end-to-end security platform right for your organization?
 - ↳ Or would you rather have a variety of top-quality tools for each environmental area (endpoint, network, SaaS, identity, cloud, etc.)?
 - ↳ Which is a priority for you: depth of integration or breadth of coverage?
- ▶ How much does budget play into the decision-making process, and how much will you allocate to security needs?
- ▶ Would your organization and security team benefit from additional services beyond detection and response? If so, which ones?

Answering these lets you filter through the noise and narrow down your search. This is more than a procurement choice; it's an operational commitment. The right MDR provider should help you detect, respond, and recover faster while also strengthening your long-term security posture.

So, whether you're starting fresh or re-evaluating your current partner, match their model, capabilities, and culture with the direction your security program is heading. After all, the stronger the alignment, the more value your MDR investment will deliver.



Romania HQ

Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

US HQ

6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309

T: +1 954-776-6262

bitdefender.com

Trusted. Always.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 200 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Release Date: September 2025

For more information, visit <https://www.bitdefender.com>.

All Rights Reserved. © 2025 Bitdefender.

All trademarks, trade names, and products referenced herein are the property of their respective owners.