How to Select an MDR Service That's Right for Your Company

How to Select an MDR Service That's Right for Your Company

DIANA KELLEY, CO-FOUNDER AND CTO

Managed detection and response has become an increasingly popular tool for companies looking for ways to beef up their security strategies. But MDR comes in many different flavors, depending, in part, on the appropriate response levels required.

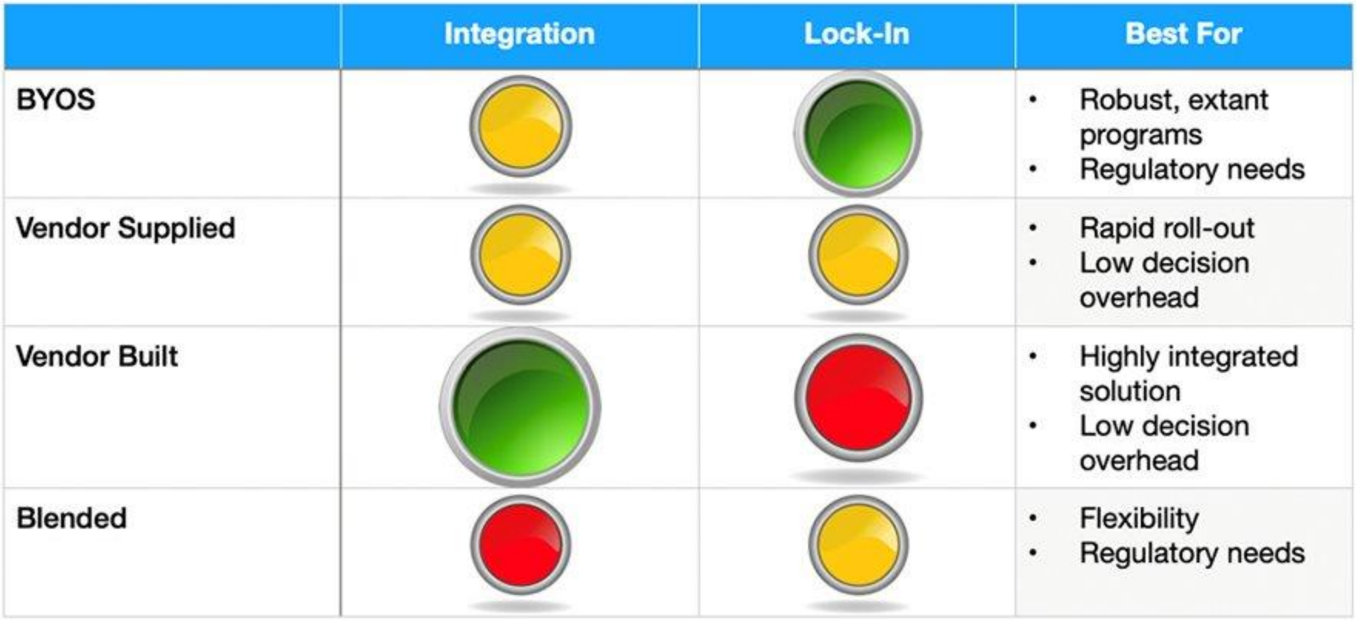
MDR AND THE 4 STACKS

One of the first major decisions to make when selecting an MDR service is whether you want the provider to supply the product stack or prefer using your own MDR stack. There are four main approaches to consider:

1. **Bring your own stack (BYOS).** In a BYOS model, you know which offering you want -- or, in the case of regulatory requirements, need -- and you're seeking an MDR vendor that can work entirely on your own stack. This is a popular approach with companies that have deployed products they already like, as well as for entities that must use specific tools for regulatory or other oversight purposes.
2. **Vendor-supplied.** The MDR supplier uses software from known and trusted vendors it then implements and manages for you. This is a great option for companies that don't have a set of tools in place or are looking to change out their stack.

In this handbook:

3. **Vendor-built.** This is a common model, where a vendor layers in its MDR offering over its own tools. This approach usually reaps the best rewards for integration between products used since they are all from the same vendor. But this can also result in tight lock-in if your organization wants to change products or service providers.
4. **Blended.** This option mixes in the best of both worlds. Many companies opt for a vendor that can support the right balance of built/supplied and provided MDR software.



	Integration	Lock-In	Best For
BYOS	🟡	🟢	• Robust, extant programs • Regulatory needs
Vendor Supplied	🟡	🟡	• Rapid roll-out • Low decision overhead
Vendor Built	🟢	🔴	• Highly integrated solution • Low decision overhead
Blended	🔴	🟡	• Flexibility • Regulatory needs

MDR SERVICE SELECTION CRITERIA

Once you've determined the best stack model, it's time to think about the MDR services you want. To do this, revisit your goals for hiring an MDR provider in the first place. A short list of the some of the most common reasons is provided below. It's a great starting point for adding in your own unique requirements.

- **Existing team augmentation.** For small companies, *augmentation* may mean *being* the security team. But even larger companies employ MDR, citing a variety of reasons that include providing coverage when hiring can't keep pace and acting as a second pair of eyes when assessing alerts and looking for indicators of compromise (IOCs).
- **Proactive threat hunting.** Most security operations center (SOC) analysts track down alerts and IOCs, both of which are definitionally reactive. If you want to be more proactive but don't have the expertise, look at the MDR provider's threat hunting skills, as well as its ability to discover indicators of attack.
- **Integrated threat intelligence.** Got plenty of threat intelligence feeds but no time to use them? MDR providers can help by providing aggregated and curated threat intelligence feeds that are pertinent to your organization and network. Many provide integrated threat intelligence in their offerings to make endpoint protection agents more responsive to unknown attacks.
- **Correlation of alert feeds.** If part of your problem is too many sensor and alert feeds in the SOC and no way to tie them together, a provider that can collect and correlate may be right for you. Just make sure the provider is familiar with the products your organization is using and has connectors to bring the appropriate signal into its dashboards or control consoles.

- **Work-from-anywhere endpoint visibility.** If getting a handle on your endpoints is your top priority, look for a vendor that specializes in endpoints. Don't forget to make sure they can cover the endpoints that matter to you, including laptops, mobile and servers. Most providers cover Windows on laptops and iOS/Android for mobile, but if you're a Mac or Unix shop, don't forget to confirm those are covered as well.
- **Remediation and response.** The "R" in MDR is one of the main drivers for MDR adoption. Determine how invasive you want the remediation action to go, and ensure your provider can deliver at the level you need.

MAKING THE RIGHT CHOICE TO SELECT AN MDR SERVICE

Armed with answers to stack, goals and service questions, you're ready to build your request for proposal (RFP) and contact vendors. Even if you don't want to conduct a formal RFP, be sure to put down what you want in writing because it will help in two important ways. First, it will help vendors respond to your specific requests rather than listening to boilerplate responses that may not relate to your situation. Second, once vendor pitches start to roll in, the RFP will help you assess responses and determine the best one.

Whether your company is large or small, finding the right MDR partner can help improve organizational resilience, reduce response times and keep your company safer.