UNCOMMONX

What To Look For in a Managed Detection and Response Provider

What To Look For in a Managed Detection and Response Provider

Choosing a managed detection and response (MDR) provider can be difficult. Here are some aspects to consider and investigate during your search. These are in no particular order but all are important when making the right choice for your organization.

What the MDR provider offers

While some MDR suppliers offer just managed detection and response, others go beyond these, acting as true partner in the security maturity of their clients. From those, you can expect security maturity assessments, compliance testing and gap assessments, incident response, security consulting, and even assistance in training. Understand what they offer. It's also best to have all services through one vendor with a single point of contact in case there's ever a problem.

Primary and secondary security operations centers

Just as you ensure you have backups for all you do in IT, your MDR provider should have a primary and secondary (backup) security operations center (SOC). Murphy's Law dictates that bad things may happen. If they do, make sure the company that's taking care of security has planned contingencies. It's also a good idea to ensure their SOCs are geographically diverse and on different power grids.

Hours of operation

Some businesses only need Monday to Friday, 9:00 a.m. to 5:00 p.m. service. Others need full 24/7/365 coverage. Decide what you need and choose an MDR provider that offers it. There will be costs associated with whatever level of service you seek.

SLAs/SLOs

In this category, vendors vary greatly. A good amount of the work done by an MDR provider is automated, but the important work is often pushed from automation into the hands of experienced, living and breathing techs and engineers at the SOC. Read the service levels and ask questions about how alerts are escalated, and, more importantly, how they are communicated to and throughout your organization.

Security assessments

A full-service MDR supplier will have a professional services team that can help identify gaps in both security and compliance within your organization. They will have experience not only in security but also in IT and running organizations. Ideally, they can not only identify areas that need improvement but they can also guide you through the process of completing any necessary changes.

Additionally, it is helpful to have a provider that thoroughly understands attack surfaces, how they are manipulated, what threat actors' goals are, and how to respond to and mitigate these threats. A full-service provider will not only understand your daily environment but will be able to help with security maturity and incident response.

Incident response

If your MDR provider doesn't offer incident response support, then they are a fire alarm – not a fire department. When they handle malware, botnet attacks, and ransomware attacks every day, MDR providers have built up the muscle and discipline necessary to not only respond to incidents, but they can also help prevent them. A top MDR supplier will also triage and fix all attacks.

If your MDR supplier and your incident response vendor are the same company, it will speed time to resolution for whatever incident occurs. They know your network inside and out, and there's no need to go searching for a separate incident response vendor while engaged in an incident. In this case, one provider can make a big difference in effectiveness and overall costs.

Machine learning and AI-based technology

These aren't just today's buzzwords. Machine learning, done right, will help reduce costs and speed processes, reducing the time to resolution. AI-based software can do the same. In dealing with millions of security events each month, the more interactive the MDR provider is with tools like artificial intelligence and machine learning, the lower your costs can be.

Machine learning and AI are more effective than monitoring by people alone. This automation results in fewer false positives and quicker incident resolution. This also means that since the vendor doesn't need to hire as many techs and engineers, they can often offer better rates to its clients.

Diverse toolset management

Since your infrastructure is not static, search for an MDR vendor that can work with a variety of tools (O365, AWS, Azure, G-Suite, etc.) Also, if they don't currently offer a plugin for the security software you have today, ask it they will create one. The best providers can and will do it quickly.

Scalability

Companies like yours are growing top- and bottom-line revenue each year. There are constant mergers and acquisitions. It's difficult to see beyond the next 12 to

18 months. Be sure your MDR provider can handle any size growth you achieve. MDR providers with experience understand this concept and are prepared for the unexpected. In fact, they plan on it!

Established company

When interviewing MDR vendors, it's important to know how long each has been in business. In my experience, there's a very large learning curve when it comes to understanding not only what customers want and how they need it but also in being able to deliver on those wants and needs. A minimum of five years is what I've seen in organizations that are able to deliver at the appropriate level for clients.

Experienced security team

Ask potential MDR providers how long their security personnel have been in the security industry and in IT overall. The answer will vary widely between organizations, but 10 years or more overall is a good number. The point is to make sure they have the best qualified, proven experts and not just people right out of school. Experience and knowledge make a huge difference in the security field.

Industry knowledge and experience

This refers to the amount of experience serving clients in a specific industry. If you're in finance, ask how long the MDR vendor has been servicing financial clients and how many they serve. The most effective MDR suppliers will have experience associated with servicing customers in your industry over time.

Security framework experience and compliance

The best MDR providers will have experience with all major security and compliance frameworks. Most of the IT and security leaders I speak with have some compliance standard or framework they need to satisfy. Experience in your necessary framework is vital to your organization's overall success. Regardless of the compliance or security framework you build your security upon (NIST CSF, ISO 27001 and ISO 27002, SOC2, NERC CIP, HIPAA, GDPR, FISMA, etc.), make sure your MDR provider has experience in it and understands it.

Ask suppliers you interview if they do have this experience. See if they understand what is required from a compliance standpoint. Determine if they can comply with what you need (records retention, file monitoring, privacy concerns, etc.) and have a history of doing it. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is recognized as the standard for cybersecurity. Your provider should test against and provide analysis in relation to this or another appropriate security framework. They should also have tools to help you understand how you stack up in each of the categories, where you're strongest, and where you need to improve (your gaps).

Asset inventory – device threat versus the National Vulnerability Database

Understanding what's on your network and the threats they pose is key to staying ahead of threat actors. A qualified MDR provider will help identify all devices on your network when they arrive and when they leave. They will also cross-reference those devices and operating systems versus the National Vulnerability Database. This allows you to determine threat levels and make decisions about quarantining.

Peer comparison

This is difficult, but ideally, an MDR needs to be able to help you understand how you're doing versus your peers when it comes to cyber preparedness and maturity. They do so by comparing your strengths, weaknesses, and drive security maturity and budget versus your peer group in specific industries and fields. That rating can help you drive funding for security with your board of directors. Showing that you rate higher than your competitors can also help promote your company to existing and prospective customers.

Assistance in board of directors communications

Ask your MDR provider if they can and will assist with presentations and/or communications to the board of directors. Do they stand behind the information, services, and guidance they offer when it counts?

Dashboards and reports

You'll want to see what's important to you and your team via an always-on online dashboard. Ask if your MDR provider can deliver specialized reports. Ask about the process to obtain these reports and how long it will take. Having access to detailed security updates and status quickly is important.

Situational awareness

In monitoring your network for threats, what is the reach for the MDR vendors threat intelligence? How many threat feeds are they using? Are they global or just national? The average MDR vendor has three to five threat intel feeds. Look for a vendor with at least 10, and look for a combination of free, paid, and proprietary sources to have a good mix and well-rounded view.

The better and more far-reaching the supplier's view of the threat landscape, the better prepared they – and you – will be to understand threats to your environment. The MDR provider will also be able to detect threats and respond faster to dangers.

Security awareness and phishing

Understanding your organization's exposure in relation to business email compromise is a key to good cyber hygiene. According to Verizon's 2021 Data Breach Investigation Report, 43% of all BECs involve phishing or pretexting, which is up 11% year-over-year. Your staff needs to understand how attackers work and how to report possible compromise within your organization. They are your frontline defense.

Price and value

Know your budget and, if it comes down to it, where you are willing to make trade-offs in wants versus needs. Only you can understand the value your MDR provider can deliver for the organization. As a final point of price negotiation, ask each of the finalists if the price they've given is the best they can deliver and will they match a competitor's price for the same services. Pricing is usually not set in stone, and if they aren't somewhat flexible here, they may be inflexible on other terms and services.

To learn more about how a managed detection and response provider can help you, visit UncommonX.

About the author

John Guzman is Sales Director for North America at UncommonX. His experience includes over 30 years of development of strategic sales plans, sales growth, and customer satisfaction/retention nationally and globally. He has over 20 years of security and cloud experience assisting Fortune 500 and Global 2000 clients and clients of all sizes build their network and infrastructure securely. He is an accomplished public speaker and published author. He has worked for industry leaders like AT&T, Verizon, Nuspire Networks, and Delta Risk/Motorola Solutions, winning multiple companies' President's Award for Sales and Service. He has consulted for KPMG and Accenture and holds multiple certifications in cloud infrastructure, sales, and security.

Contact Us Today, Be Safer Tomorrow

Talk to our experts today about your specific needs. Call **866-405-9156**, email us at **sales@uncommonx.com** or visit us at **uncommonx.com**.