



Ultimate Buyer's Guide to Managed Detection and Response



Table of Contents

Introduction: Choose the Right Path for Your Organization in Five Steps.....3

Step 1: Determine Whether to Buy or Build Your MDR Solution4

Step 2: Identify Which Type of MDR Best Fits Your Organization11

Step 3: Establish the Key Criteria to Consider in an MDR Provider17

Step 4: Ask the Right Questions to Evaluate an MDR Provider19

Step 5: Understand What to Expect From Your Chosen Path.....23

Conclusion: Advance Your Security25

Introduction:

Choose the Right Path for Your Organization in Five Steps

The managed services sector, particularly cybersecurity, has witnessed remarkable growth in recent years, with the Managed Detection and Response (MDR) market projected to reach \$6.29 billion¹ by 2030. Managed services, such as MDR, Managed Security Service Providers (MSSP), and similar solutions, have emerged in response to the demand. The accelerated growth of the MDR market mainly comes from increasing cybersecurity threats, the adoption of cloud computing, the shortage of cybersecurity talent, and the increase of the Internet of Things (IoT).

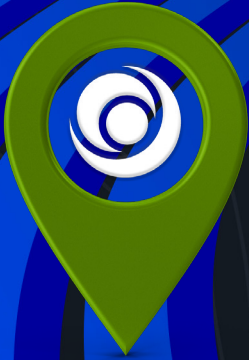
According to IBM's latest report², the global cost of a data breach was USD 4.45 million last year, a 15% increase over three years. As a result of this increase, organizations are investing in MDR services to help reduce their risk of attacks and irrefutable damage. In short, organizations need a cybersecurity partner to provide all-inclusive cybersecurity services.

To help you make informed decisions in this dynamic landscape, this guide will walk you through five key steps to navigate the MDR market and find the solution that best suits your organization's needs. From determining whether to buy or build your MDR solution to evaluating and working effectively with your chosen provider or in-house team, we will equip you with the knowledge and insights necessary to strengthen your cybersecurity posture.



According to IBM's latest report, the global cost of a data breach last year was

\$4.45 million²



Step 1

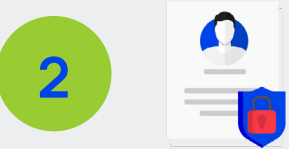


Determine Whether
to Buy or Build Your
MDR Solution

Step 1

When it comes to implementing an MDR solution, organizations often face the dilemma of choosing between building a Security Operations Center (SOC) in-house or buying a pre-existing MDR solution from a vendor. The decision between buying and building an MDR solution should not be taken lightly, as it could significantly affect your organization's overall cybersecurity posture and operational efficiency.

There are crucial factors that need to be carefully considered before making such a decision, including the organization's objectives and needs, budget, team expertise, technology, and availability.

Here Are Factors To Consider When Getting Started:

-  **Cybersecurity Budget**
-  **Security Team Expertise**
-  **Available Cybersecurity Technology and Scalability**
-  **IT Stack Scalability**

Step 1



Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Cybersecurity Budget

What you'll need to get started:

Daytime (9-5) And 24x7 Full-Time Employees

- You will need experienced security analysts to monitor and respond to security alerts around the clock to monitor security events and incidents in shifts.

Platform Hardware

- Depending on if you're operating on-premises, hybrid, or in the cloud, hardware costs for servers, networking equipment, storage devices, and other infrastructure components are needed to support the SOC's operations.

Software

- Licensing fees for security tools, SIEM (Security Information and Event Management) solutions, endpoint detection and response (EDR) software, and other necessary cybersecurity software.

Consultancy Support

- Engaging external consultants or experts to assist in setting up and optimizing the SOC infrastructure and processes.

Threat Intelligence Feeds

- Subscription fees for threat intelligence feeds to stay updated on the latest cyber threats and vulnerabilities.

Maintenance And Support

- Ongoing maintenance costs for hardware and software and support services for troubleshooting, updates, and upgrades.

Technology

- Investment in advanced technologies such as artificial intelligence (AI) and machine learning (ML) for more sophisticated threat detection capabilities.

Step 1

Determine Whether to Buy or Build Your MDR Solution



Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path

When adding up these expenses, organizations may find that the initial capital outlay and ongoing operational costs of building an in-house SOC can be substantial. An organization's average annual cost to run an in-house SOC is \$2.86 million³.

When buying an MDR solution, organizations typically pay a predictable subscription fee based on the required services and level of support. This model eliminates the need for significant upfront investments in infrastructure, staffing, and ongoing maintenance. Moreover, MDR providers often have access to cutting-edge technologies and threat intelligence feeds, which can enhance the security posture of organizations without the need for internal development and management.



**An organization's
average annual cost to
run an in-house SOC is**

**\$2.86
million³**



What costs do I need to consider when buying vs. building an MDR solution?

Step 1

Determine
Whether to Buy
or Build Your
MDR Solution



Step 2

Identify
Which Type
of MDR Best
Fits Your
Organization

Step 3

Establish the
Key Criteria to
Consider in an
MDR Provider

Step 4

Ask the Right
Questions to
Evaluate an
MDR Provider

Step 5

Understand
What to Expect
From Your
Chosen Path



Security Team Expertise

Building a successful SOC team involves careful planning and consideration of the expertise and skills required to detect, respond to, and prevent security incidents effectively. Here are some key roles to consider when building a SOC team:

- Manager
- Engineers (Systems, Detection, and Content)
- Analysts
- Threat Intelligence Experts

Once you have assessed your team's expertise, you can identify the specific roles and skill sets needed to build a well-rounded SOC team. You may need to invest in training and upskilling your existing team members or recruiting new talent with the required skills and experience.

In addition to technical expertise, it is also important to consider soft skills such as communication, collaboration, problem-solving, and adaptability when building an MDR team. A diverse team with a mix of technical and non-technical skills can enhance the effectiveness and resilience of your security operations.

On the other hand, there is the option to outsource to a trusted vendor that can provide a ready-made team of experts (in addition to a threat research team) to manage security operations efficiently, allowing the internal team to allocate their time and resources to other important cybersecurity tasks.

This approach can help organizations optimize their resources and ensure that the expertise of their internal team is utilized effectively.



What expertise is required for a SOC? Do I currently have a team? And where do they need to spend their time?

Step 1

Determine Whether to Buy or Build Your MDR Solution



Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

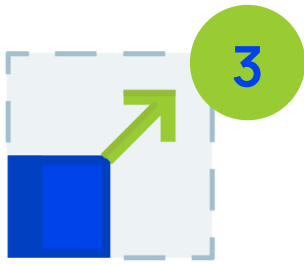
Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Available Cybersecurity Technology and Scalability

The cybersecurity landscape is dynamic, with threat actors constantly evolving their techniques, causing organizations to grow. Organizations that choose to build an in-house SOC must allocate resources for research and development to stay updated on vulnerabilities, emerging threats, and industry best practices. This includes investing in threat intelligence feeds, attending conferences, participating in information-sharing communities, and conducting regular assessments and audits. Such ongoing investments are necessary to ensure the in-house SOC remains effective and relevant, scaling to meet your business needs.



Time to Value:

90 min
to implement



30 sec
Triage



15 min
to remediate

In contrast, MDR vendors are built to help organizations take command of their security operations and compliance without the additional need for expertise. Time to value can consist of a 90-minute deployment, 30 seconds to triage, and 15 minutes to remediate threats. Working with an MDR vendor, you should expect consistent updates, new technologies, and innovations that evolve with the current threat landscape.

Regardless of the chosen approach, organizations must invest in technology to effectively build and maintain an in-house SOC. This investment includes maintaining and tuning rules, managing the technology, and ensuring seamless integration with existing infrastructure.

Step 1



Determine
Whether to Buy
or Build Your
MDR Solution

Step 2

Identify
Which Type
of MDR Best
Fits Your
Organization

Step 3

Establish the
Key Criteria to
Consider in an
MDR Provider

Step 4

Ask the Right
Questions to
Evaluate an
MDR Provider

Step 5

Understand
What to Expect
From Your
Chosen Path

Planning for scalability in your SOC should include adapting to evolving cybersecurity threats and accommodating your organization's expanding needs. This involves assessing the size and scope of your SOC and determining the necessary resources, such as the number of employees and tools, to support its growth.

Remember that building requires additional investments in recruiting and training staff and acquiring new tools as the organization evolves. Additionally, managing the increasing amount of data ingested needs to be considered.



What technology do I have currently, and what will I need to stay updated with current threats?

When considering a build vs. buy approach, it is important to evaluate the costs, resources, and expertise required to manage and maintain a comprehensive security operation effectively. While building an in-house SOC may offer more customization and control, it can also be a costly and time-consuming endeavor. Therefore, many organizations opt to partner with a trusted MDR provider to alleviate the burden of managing their security infrastructure.

Step 1

Determine Whether to Buy or Build Your MDR Solution



Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

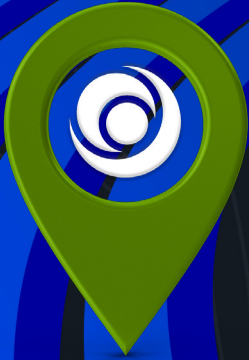
Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Step 2

Identify Which Type
of MDR Best Fits
Your Organization

Step 2

When exploring the landscape of MDR solutions, it's crucial to recognize the diverse categories available in the market. Whether you are currently using an MDR solution or embarking on the journey to find the right fit, it's essential to acknowledge that each organization's security posture is unique. Evaluating your current security status and future goals is the starting point for finding the most suitable MDR solution for your needs.

When assessing MDR solutions, key factors include the level of human expertise provided, the technologies utilized for threat detection, the range of services offered, and the solution's adaptability to your organization's evolving security landscape. By delving into these aspects, organizations can make informed decisions that align with their security requirements, enhance their security posture, and effectively defend against cyber threats.

Delve Deeper Into MDR Solutions

Not all MDR providers operate similarly; while they all aim to provide organizations with the necessary tools and services to detect and respond to security threats, the capabilities and offerings can vary significantly.

From the sources they pull security data from to the level of response services they provide, MDR providers differ in their approaches and focus areas. Understanding these differences is crucial for organizations looking to choose the right MDR provider that aligns with their specific needs and requirements.

There are multiple broad classes of MDR providers:

-  Pure-Play MDR
-  Managed Endpoint Detection (EDR)
-  Managed Security Information and Event Management (SIEM)
-  Managed Extended Detection and Response (XDR)

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization



Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Pure-Play Managed Detection and Response (MDR)

This category of MDR service providers relies on a proprietary mix of third-party security tools and solutions, such as endpoint, SIEM, cloud access, or others, to collect logs and alerts. These providers use a customized technology stack, which their 24/7 Security Operations Center (SOC) monitors. Most pure-play MDR providers cannot decouple their technology stack from their SOC service offerings. While effective at detecting and responding to threats, this closed-loop approach often limits their ability to offer co-management, work effectively with partners and customer providers, and leave customers reliant on their SOC to provide reports.

Pure-play MDR is right if your organization:

- Wants to stay up to date on current threats and technology without internal investment
- Does not have a mature cybersecurity program that can remediate advanced threats through existing resources and tools
- Is looking for coverage, detection, and response that is specific to the MDR provider's technology stack
- Wants guidance and recommendations on remediation steps

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization



Step 3

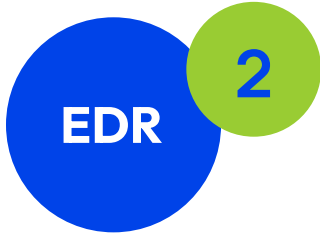
Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Managed Endpoint Detection and Response (EDR)

EDR is a fundamental tool for monitoring and detecting endpoint threats, serving as the cornerstone of any cybersecurity strategy. This solution utilizes software agents or sensors deployed on endpoints to collect data, which is then transmitted to a central repository for analysis.

Managed EDR is right if your organization:

- Wants to enhance its endpoint security capabilities beyond anti-virus
- Requires identification of threats beyond traditional preventative security measures
- Is in the early stages of developing a strong cybersecurity strategy
- Aims to establish a solid foundation for a scalable security architecture

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization



Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Managed Security Information and Event Management (SIEM)

Given the expertise and dedicated resources required to manage endpoint and SIEM solutions properly, many customers outsource management to an MDR or managed IT service provider. Over the last few years, leading providers now offer a managed service based on their core technology offering. This managed service provides updates and operations, detection investigation, and specific response services based on the capabilities of its core technology offering.

Managed SIEM is right if your organization:

- Has a dedicated security team with expertise in investigating and responding to security alerts
- Invested in security tools to streamline workflows
- Values the flexibility and control provided by managing investigations and responses in-house
- Requires specific compliance or security policies

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization



Step 3

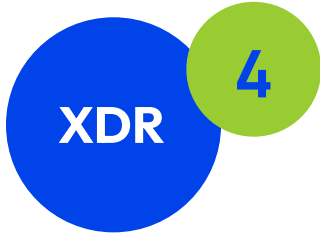
Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Managed Extended Detection and Response (XDR)

XDR expands EDR features to safeguard beyond just endpoints, covering a more comprehensive range of devices. This solution spans the entire infrastructure, integrating security data from various sources for comprehensive analysis and efficient workflows across an organization's security environment. It improves the detection of advanced and obscured threats and facilitates a unified response. Opting for a managed XDR solution also grants access to skilled professionals proficient in threat hunting, threat intelligence, and analytics.

Managed XDR is right if your organization:

- Aims to improve advanced threat detection, accelerate comprehensive threat analysis, investigation, and hunting from a single platform
- Wants to improve visibility caused by disconnected security
- Is looking to extend its lean team and seeks to reduce response time
- Wants to optimize ROI across all security tools

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization



Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Step 3

Establish the Key
Criteria to Consider
in an MDR Provider

Step 3

If choosing to outsource an MDR solution is most feasible for your organization, the next step is to carefully evaluate potential providers to ensure the chosen solution meets the organization's specific needs and requirements.

The capabilities and functions of MDR providers can seem overwhelming, so how do you choose one that makes sense for your organization and cybersecurity strategy? First, to ensure your organization's protection, verifying the efficiency of an MDR solution before investing in it is crucial. This means making sure that the capabilities fit your needs and understanding that not all solutions are created equally. Here is a list of considerations when evaluating:



Detection:

What methods are used to identify threats? Are they applying machine learning or artificial intelligence to detect advanced threats?

Investigation:

Will they alert you when things seem malicious? Do they investigate and confirm for you? Investigations depend on the available telemetry, and it is essential to clarify if the provider will investigate alerts or simply notify you.

Response:

What does the host containment look like? Do they isolate systems, preventing the spread? Or block network traffic?

Remediation:

What type of guidance and/or recommendations will you receive, and in what method?

There are several other factors to consider when choosing an MDR. For example, understanding the service level agreements and communication methods for incident response is crucial. For instance, can you access the same portal as the provider to stay updated on the incident? Can you directly interact with the security analyst to discuss the incident? Also, it is important to evaluate the provider's reporting capabilities and determine if extracting the required information is easy.

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Step 4

Ask the Right
Questions to Evaluate
an MDR Provider

Step 4

Now that we have discussed the various categories of MDR and what to consider when selecting a provider, it is important to understand the next step in the process - evaluating potential MDR providers for your organization. Asking the right questions can help ensure your chosen provider meets your unique needs and provides the required support and protection. By first understanding your organizational requirements and then asking targeted questions, you can navigate the MDR market more effectively and ultimately make a more informed decision.

What security signal are you able to monitor and protect?

Cybercriminals attempt to be sneaky to avoid detection. Sometimes, they leave tiny breadcrumbs that are easy to overlook, but when you connect all your security data, those breadcrumbs turn into a trail that leads an analyst to uncover what happened. It's like shining a light on every nook and cranny of your cybersecurity landscape. It's not uncommon for cybercriminals to bypass a security signal before finally being caught and the more monitoring an MDR provider can provide, the better.

In addition to understanding what your provider or team can ingest, it's essential to know if you can connect your current technology or if you must use the provider's technology (in some cases you are limited to their existing integrations).

What metrics and reporting do they offer to help organizations effectively track and understand their security posture?

MDR providers should give access to various reporting capabilities to help organizations track and understand their security posture. These include incident reports, threat intelligence reports, performance and efficacy metrics, compliance reports, trend analysis, executive dashboards, and ad-hoc reporting. These reports can give organizations valuable insights into their security landscape and help them understand their security state effectively. Organizations need to discuss their reporting requirements and expectations with potential providers to ensure alignment and obtain the most relevant and useful information for tracking and understanding their security posture.

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider



Step 5

Understand What to Expect From Your Chosen Path

What type of visibility will I have into my environment?

MDR providers act as an extension of your team, giving you 360-degree visibility. You should be able to see what alerts are being investigated, why alerts were closed, and the details of an active investigation. Initially, this may look like check-ins to start to trust the provider, but then it will evolve into the benefits of having an extended team. This allows you to dedicate your time to building a proactive approach to security, understanding your risks, and implementing changes.

If you are in a regulated industry, how will they help you comply with frameworks like PCI DDS, FFIEC, and HIPAA Assessments?

Proving compliance can become a time-consuming process. With all your data in one location, pulling the required data to show compliance should be easy. Your MDR team should be providing support for your day-to-day tasks so you can focus on improving your security posture. Being able to run compliance reporting throughout the year can provide insights into which areas of your security program require improvement to reduce risk. Like other reporting capabilities, you should have direct access to evaluate and understand your compliance needs.

How do they provide scalability and flexibility to accommodate growing business needs?

A scalable MDR solution should seamlessly adapt to increased data volume, diverse threat landscapes, and connecting to new or additional security technology. Simple pricing and licensing are critical in meeting the evolving demands of a growing business and provide scalability. It's important that your provider can streamline your security program into a centralized location by offering key components such as threat hunting, vulnerability management, incident response, and more. Another thing to consider as your business grows and your security evolves is the flexibility to choose who manages the platform.

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

[Ask the Right Questions to Evaluate an MDR Provider](#)



Step 5

Understand What to Expect From Your Chosen Path

Do they use machine learning to detect anomalies in an environment?

Machine learning (ML) and Artificial Intelligence (AI) are becoming more commonplace words in cybersecurity. As cybercriminals evolve their tactics and techniques to evade security controls and the shift to the cloud, they can easily go undetected. MDR providers should have a team of data science and threat researchers who identify these new methods and build machine learning models based on this activity to develop detections. Additionally, the security platform your provider uses should include user entity and behavior analytics to create behavioral profiles for users so it can detect when behaviors deviate from the baseline.

What is the onboarding process? How long will it take to be fully up and running?

The onboarding process should be simple and only take a few hours. Deployment and tool integration should be intuitive. Initial support with an onboarding call will help guide you through a smooth setup. A straightforward onboarding process not only accelerates security enhancement and return on investment but also showcases the provider's commitment to efficiency and effectiveness. It also usually indicates a provider's ability to deliver a Proof of Value, enabling you to experience their capabilities firsthand.

What does customer support look like?

A dedicated customer support representative within your MDR provider is a direct link to assistance and quick resolution when you have questions. With a dedicated customer success manager, you gain a partner who advocates for your interests. This focused support enhances collaboration, builds trust, and helps you maximize your security investment. Some MDR providers also offer a dedicated post-sales engineer as additional support.

By considering these questions and your unique circumstances, you will be better equipped to find the right provider to meet your specific criteria and maximize value to your organization.

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

[Ask the Right Questions to Evaluate an MDR Provider](#)



Step 5

Understand What to Expect From Your Chosen Path



Step 5

Understand What
to Expect From Your
Chosen Path

Step 5

After implementing MDR services, it is essential to clearly understand what to expect from your chosen provider or in-house team. Here are key aspects to consider in terms of post-implementation expectations:



Comprehensive Threat Monitoring: Your MDR provider or team should continue to offer comprehensive monitoring of your network, endpoints, and cloud environments, ensuring proactive detection of emerging threats and vulnerabilities.



Advanced Threat Detection: Expect your provider to stay up-to-date on the latest technologies and techniques for advanced threat detection, leveraging AI, machine learning, and behavior analytics to protect your organization against evolving cyber threats.



Timely Incident Response: Post-implementation, your provider should maintain efficient incident response procedures to swiftly contain and mitigate security incidents, minimizing any potential impact on your organization.



Customized Services: Your chosen MDR provider should adapt their services to align with your evolving security needs, including any changes in compliance requirements, industry regulations, or organizational growth.



Transparent Reporting and Communication: Consistent and transparent reporting on security incidents, vulnerabilities, and remediation efforts should continue to be provided, ensuring you are informed of the security posture and ongoing efforts to protect your organization.



Continuous Improvement: Your MDR provider or in-house team should demonstrate a commitment to ongoing training and skills development to stay ahead of emerging threats, continuously improving their capabilities to safeguard your organization's assets effectively.



Collaboration and Partnership: Post-implementation, maintaining a collaborative and open partnership with your MDR provider or in-house team is crucial. Foster ongoing communication, trust, and cooperation to ensure a proactive and practical approach to cybersecurity.

By setting clear post-implementation expectations and collaborating closely with your chosen MDR provider or in-house team, you can ensure that your organization remains resilient against cyber threats and continuously enhances its security posture.

Step 1

Determine Whether to Buy or Build Your MDR Solution

Step 2

Identify Which Type of MDR Best Fits Your Organization

Step 3

Establish the Key Criteria to Consider in an MDR Provider

Step 4

Ask the Right Questions to Evaluate an MDR Provider

Step 5

Understand What to Expect From Your Chosen Path



Conclusion: Advance Your Security

The journey towards finding the right MDR solution for your organization is not a one-size-fits-all approach. Whether you are already using an MDR solution or are looking to implement one for the first time, it is crucial to assess your current security posture and identify your organization's specific needs and goals.

Understanding the different categories of MDR, navigating the build vs. buy decision, and knowing what to look for in an MDR provider are key steps in this process. Asking the right questions when evaluating MDR providers and considering the benefits and considerations of consolidating tools into a centralized platform can help you make an informed decision.

Finding the right MDR provider for your organization requires careful consideration, research, and alignment with your unique requirements. By assessing your current cybersecurity landscape and future objectives, you can ensure that the MDR solution you choose is tailored to your organization's specific needs and helps you enhance your overall cybersecurity posture. Remember, every organization's security journey is different, and finding the best solution starts with understanding where you are today and where you want to be tomorrow.



For additional help, contact us today, [schedule a demo](#), or [sign up for a free trial](#). Learn more about how Adlumin's Managed Detection and Response Services and Security Operations Platform can empower your team to illuminate threats, eliminate cyber risk, and command authority.

Authors

Jen Thompson, Director of Product Marketing at Adlumin

Brittany Holmes, Corporate Communications Manager at Adlumin

1. <https://www.fortunebusinessinsights.com/managed-detection-and-response-market-108618>

2. <https://www.ibm.com/reports/data-breach>

3. <https://www.securitymagazine.com/articles/98722-building-a-security-operations-center-soc-on-a-budget>

Adlumin is the security operations command center that simplifies complexity and keeps organizations of all sizes secure. Its innovative technology and seamless integrations create a feature-rich platform that includes everything a sophisticated security team needs, while empowering channel resellers, service providers and organizations of any size with the collaboration and transparency required to establish a coordinated and mature defense.

With a vendor-agnostic approach and preexisting integrations, Adlumin's Security Operations Platform obtains security telemetry from across an organization to provide greater insights into security alerts and streamline workflows. Organizations can use Adlumin's Security Operations Platform on their own or get full transparency and visibility while utilizing the 24/7 monitoring and response services provided by the Adlumin Managed Detection and Response (MDR) team. Whether organizations manage the platform on their own or with MDR, Adlumin consolidates all security needs for a unified experience.