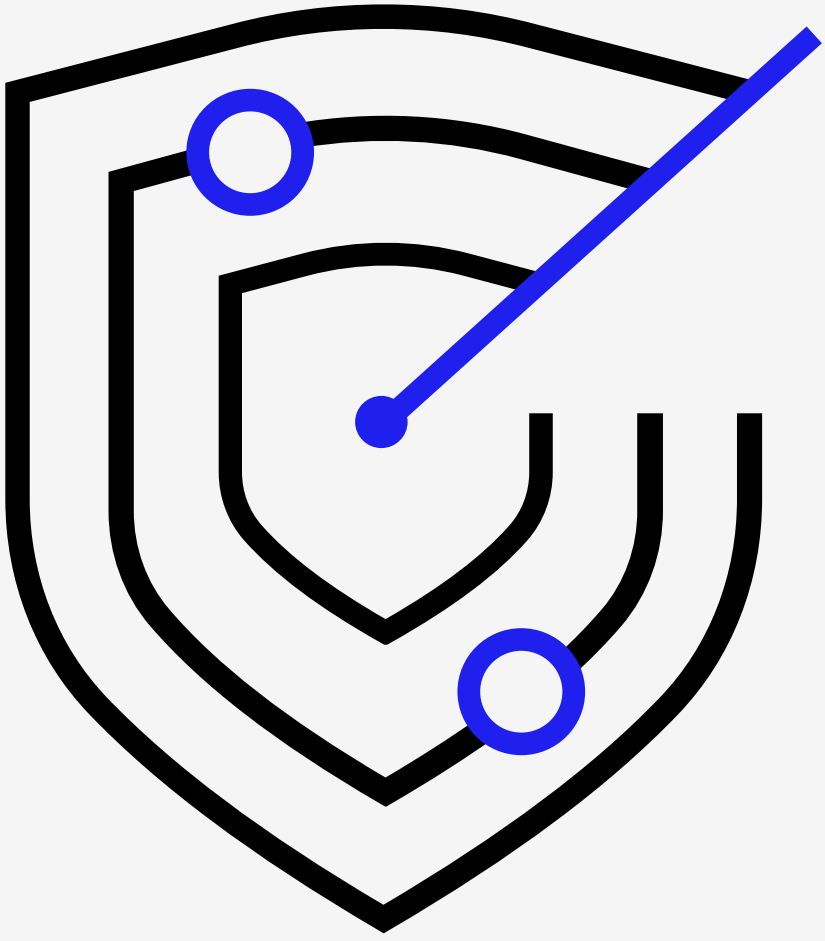
at bay

The Managed Detection and Response (MDR) Buyer's Guide for Small Businesses

How to identify your security needs, evaluate vendors, and understand MDR capabilities that best fit your business



at-bay.com

Table of Contents

Introduction

Cybercrime is projected to cost businesses $10.5 trillion annually by 2025[1] — and most businesses, especially those without dedicated security resources, face serious risks. The average loss for a small or medium-sized business due to a cyber incident over the past five years was $278,000[2].

Unfortunately, staying safe is not as simple as it used to be. Legacy antivirus solutions fall short in their protection against rapidly evolving threats and businesses now need 'round-the-clock protection and surveillance.

> Over **50%** of cyber insurance claims in the past two years could have been mitigated by an MDR solution.
>
> *At-Bay claims data from Q4 2021 - Q3 2023*

For large enterprises, the solution is fairly obvious, if costly: assemble a team of in-house cybersecurity experts. For businesses without those big budgets, this route is too expensive and complicated.

Managed Detection and Response (MDR) services help businesses stay secure and reduce cyber risk at a fraction of the cost and hassle of hiring an in-house team. Using a combination of seasoned security experts and cutting-edge software, MDR services provide a layer of protection many businesses are unable to afford.

And, we know it works. At-Bay data shows that over 50% of cyber insurance claims in the past two years could have been mitigated by an MDR solution. In this guide, you'll find everything you need to know about MDR services, the technology they use, and how to shop for the right vendor.

---

[1] Cybersecurity Ventures, "*Cybercrime To Cost The World $10.5 Trillion Annually By 2025*"
[2] NetDiligence, Cyber Claims Study 2023 Report

What is Managed Detection and Response?

Managed Detection and Response (MDR) is a specialized service that provides companies with an advanced layer of security to detect, investigate, and actively respond to cybersecurity threats. This service provides a convenient alternative for companies whose non-specialist IT or operations teams may be struggling to keep up with security monitoring among their many other tasks.

How Does an MDR Work?

Endpoint Detection and Response (EDR) detects threat

Managed Detection and Response (MDR) analysts triage and analyze threat

MDR analysts remediate threat and provide guidance

Analysts close incident and log threat for future tracking

Security analysts are the cornerstone of MDR services. They combine their deep security knowledge with strategies that stop cyberattacks before they happen. To do this, the analysts use a suite of cutting-edge software — known as Endpoint Detection and Response (EDR) — to monitor a company's systems and identify suspicious activity. (We'll talk more about the technology later.)

A typical MDR analyst sees more cyberattacks than a single business ever will due to the number of clients they monitor. This gives them more experience and expertise in handling these threats.

Using their skills for both investigating and understanding tech, these analysts carefully monitor and correlate the activities of all devices connected to the network, investigate any suspicious activity, and use shared information about threats to take decisive action that will protect your business from attacks.

This allows MDR providers to deliver continuous oversight of a company's assets, offering not only reactive response to threats, but proactive identification and alerting of potential threats before they become a problem.

7 Things Businesses Should Know About MDR Services

Choosing the right MDR service is much like choosing the right business partner. You need to find a vendor that's right for your business, from communication styles to industry expertise to operational maturity.

We've broken down the seven most important areas businesses should consider when choosing an MDR service provider.

1

Broad Expertise

An MDR analyst team should have a mix of skills in finding threats (threat detection), handling incidents (incident response), and investigating the traces left by cyberattacks (forensic analysis). A diverse team with skills across a range of security disciplines can offer a more comprehensive approach to defending your digital assets. The team should support your security program every step of the way, from setting up a solid strategy to make your defenses stronger, to managing threat detection and response, and even being ready to handle a security incident if one occurs.

2

Robust Response

Many MDR services simply inform customers of the problem, but actually stop short of responding to an incident and taking the necessary action to resolve it. Unfortunately, most small businesses don't have the resources or know-how to respond quickly on their own. It's important that your MDR service doesn't just spot attacks, but also steps in to stop them. At the same time, it's crucial to work with your provider and align on the specific type of response needed for the different technologies that may be in use at your company.

3

24/7/365 Availability

The availability and responsiveness of the analyst team is another factor key to MDR efficacy. Since cyberthreats can occur at any time, an analyst team that is available 24/7/365 is essential for coverage. Ask specific questions regarding their Service Level Agreements (SLAs) to better understand their coverage and how quickly the team identifies and responds to incidents. You should ask the provider to explain precisely what guarantees it offers for continuous monitoring and their protocol for immediate support. Discuss how analysts manage to respond to threats promptly, asking for clear response timeframes that are documented within their SLAs.

4

Operational Maturity

The moments after a cyber incident occurs can often feel chaotic. Teams that have a clear process for spotting, sorting, looking into, fixing, and bouncing back from incidents are usually more trustworthy and reliable. There are established methodologies for responding to incidents, like the Cyber Kill Chain or the MITRE ATT&CK framework, that help categorize and stop cyberattacks on your business. Ask if they use one of these recognized frameworks or another, and why.

5

Collaboration and Cooperation

Communication skills play a pivotal role in an MDR service. Should your business be the victim of a cyberattack, your team will need to work closely with the MDR experts you've hired. Ensure communication and collaboration styles match up between your team and theirs. Ideally, the MDR provider should understand your industry specifics, infrastructure, and the critical nature of your data and applications. It's also important to find an MDR team willing to work with other vendors or third-party partners, such as cyber insurance vendors or outside legal teams, which may be necessary to resolve any incidents.

6

Commitments in Case of Incidents

Typical MDR SLAs offer very limited recourse in case you get breached despite their claims of securing your business against threats. Some of the highest quality providers offer warranties or other representations to provide support in case of an incident. Providers that align their interest with their customers' are generally committed to a higher quality of service since they will suffer financial loss if they fail. Inquire about the limitations of those warranties so you understand exactly what is being guaranteed and what recourse may be available in the event of a breach.

7

EDR Technology

MDR security experts use technology called Endpoint Detection and Response (EDR) to monitor your company's systems and identify suspicious activity. MDR's effectiveness is largely dependent on the quality of the EDR used by analysts. There can be a significant difference in an EDR's performance from vendor to vendor, so you should focus on an MDR provider that uses best-in-class EDR. We'll cover the nuances of EDR software in the next section.

Recommendations Based on Real-World Claims

You should always speak with your authorized cyber insurance representative about whether an investment in your business' cybersecurity preparedness, such as the purchase of an MDR solution, may qualify you for more affordable cyber insurance coverage.

Additionally, in recent years, a handful of cyber insurance providers (like At-Bay) have begun offering MDR as a separate service. By being part of a family of companies that includes a cyber insurance provider, this subset of MDR vendors have access to real-world claims and incident data, giving them a better understanding of risk and allowing them to make better recommendations or provide solutions to improve overall security.

How MDR and EDR Work Together

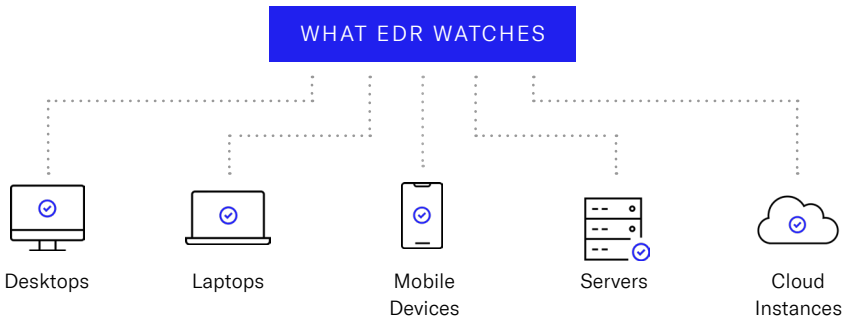
Endpoint Detection and Response (EDR) is software that continuously monitors and collects data from endpoints throughout your environment, such as desktops, laptops, tablets and mobile phones, servers or other devices that rely on an internet connection.

> EDR solutions can be used off-the-shelf, but having an expert fine-tune the system to best fit your business needs will **increase its effectiveness**.

Unlike legacy antivirus software that spots already-known threats, EDR software uses machine learning to catch new or changing attacks.

This means EDR can notice and stop threats that traditional antivirus might miss, keeping businesses safer in the face of changing and maturing threats.

EDR solutions can be used off-the-shelf, but having an expert fine-tune and monitor the system to best fit your business needs will increase its effectiveness. MDR can not only streamline your cybersecurity strategy, but it can also configure EDR technology correctly so you're getting the most from it.



EDR systems can mistakenly flag safe activities as threats, which requires someone with special skills to investigate. In addition, while EDR systems are particularly effective in catching attacks early to stop them from spreading, being quick to react is crucial and your IT team may not have the time to stop what it's doing and check alerts constantly.

This is where MDR services can become an invaluable asset: Relying on an MDR service can remove a significant burden from your own IT personnel, allowing you to focus on your core business operations with the assurance that experts are safeguarding your business.

SUMMARY

The Benefits of EDRs for Business Owners

- **Modernized Security**: An EDR continuously monitors endpoints to identify threat patterns or anomalies. When EDR software senses something might be wrong, it quickly lets analysts know, and sometimes even steps in to fix the problem on its own. This quick action can turn what could have been a huge security disaster into just a small hiccup, allowing you to continue with business as usual.
- **Efficient Incident Response**: When an attack does occur, EDR systems retain historical data of the breach so forensic investigators can quickly understand what happened.
- **Time and Money Savings**: EDR reduces the time and resources required to manage endpoints, investigate incidents, and recover from attacks. Plus, it can minimize the chances of downtime when recovering from a possible incident. However, EDR technologies need someone to manage them and respond to alerts. For this reason, MDR services are a good solution for teams that do not have enough resources to dedicate.

EDR Essentials

As you search for an MDR service provider, it's important to understand how EDRs work so you can ask which products the MDR team uses and their capabilities.

Here is a basic overview of key EDR functionality:

Continuous Monitoring and Data Gathering	EDR tools constantly monitor endpoint activity, gathering and storing large amounts of data. The data can then be analyzed to identify patterns that could indicate a security threat.
Threat Detection	EDR uses behavioral analysis and machine learning to identify unusual behavior or malicious activities that deviate from established "normal" patterns. This allows EDR to detect new or evolved threats that wouldn't be caught by antivirus.
Incident Response and Remediation	Upon detection of a potential threat, EDR systems can respond immediately so you don't have to. The response can range from automated actions like isolating a compromised endpoint to alerting security personnel, mitigating the potential damage.
Threat Hunting and Investigation	EDR tools provide the necessary data and visibility to understand how a specific threat entered and proliferated within the network, helping patch vulnerabilities more effectively.

Now that you have a broad understanding of how EDR works, we'll share how you can choose the right EDR for your business in the next section.

Choosing the Right EDR for Your Business

Running EDR software on your own can get complicated quickly, which is why many businesses choose an MDR service. MDR can streamline your cybersecurity strategy, providing not only the software and tools, but also the specialists needed to monitor, detect, and respond to threats.

However, here are some guidelines for you to consider:

Prioritize the Right Features

Price is an important factor when choosing an EDR, but even more important is whether it provides you with the security you need.

It can be tempting to pick the cheapest EDR to stay within your company's budget, but if it's not providing you with proper security, it may end up costing you down the line.

Not all EDR software is created equal. Be aware of low-cost options available that may not be equipped with the proper technology or rebranded legacy anti-virus software labeled as "EDR" that are not technically capable of providing protection you need.

Best-in-class EDR systems show a significant difference in performance and protection compared to others.

Ensure Your EDR Has These Core Functionalities

Every MDR should be using an EDR with these core functionalities (as explained in the previous section):

- Real-time monitoring
- Behavioral analytics for automatic threat detection
- Integration with threat intelligence
- Automated response actions
- Threat hunting capabilities

Technical and Organizational Considerations

Aside from examining the software capabilities, there are several indirect technical considerations to take into account when assessing an EDR used by a potential MDR vendor:

- **Scalability**: Can new security countermeasures be added without needing to re-engineer the solution?
- **Connected Insights**: Does the EDR learn from security event data to better its defenses and respond to attacks?
- **Integration Capabilities**: How well does the EDR software work with your current technology setup?
- **User-friendliness**: Although seasoned security experts are overseeing an MDR, the EDR system should also be user-friendly for your staff.
- **Maintenance and Updates**: How is the system maintained and updated over time, and will these updates disrupt your business operations in any way?
- **Resource Demands**: How much processing power and memory usage will it use, and how might it impact other applications and systems running in your environment?
- **Ease of Setup**: Does the EDR run on the cloud, which allows for instant operation and easy accessibility?
- **Reporting and Analytics**: Does the EDR offer comprehensive reporting options that provide insights into your security posture and allow your MDR team to make data-driven decisions for your business?

If considering all of these variables feels overwhelming, choosing an MDR service can make it easier.

In the next section, our team of security experts has compiled a comprehensive list of questions to help you evaluate MDR vendors.

MITRE Evaluation Scores

Given that EDR software can differ between providers, consider using independently-run evaluations to help inform your research. For example, the MITRE ATT&CK Evaluation, measures how well these products detect and respond to real-world threats and attacks. The scoring scale ranges from 0 to 100, with good scores topping 80. The best-in-class often finish with a 99 or 100.

Ask your MDR provider whether the EDR it uses has gone through a MITRE ATT&CK evaluation and what score it was awarded.

Special Considerations for Small Businesses

At-Bay's claims data shows the most common cyber threats to small and medium-sized businesses are ransomware and financial fraud. An MDR provider should know how an EDR reacts to these types of attacks in particular, as well as other types of attacks you may not be aware of.

The MDR Buyer's Checklist for Small Businesses

Choosing the right solution may seem daunting, but with this checklist, it can be straightforward. Below is a list of questions to ask an MDR provider, that can allow your organization to understand what EDR solution and MDR service will work best for you:

	QUESTION	WHAT TO LOOK FOR
☐	What is your onboarding process?	Choose a provider that has a relatively simple onboarding process and will guide you through each step on a timeline that works for you.
☐	What experience does your staff have?	The provider you choose should have the expertise to understand the specifics of your business and industry, and the diverse backgrounds to respond to potential threats. Some common analyst backgrounds include digital forensics, incident response, information security or law enforcement.
☐	What are the terms of the contract?	Your provider should be able to give you the specifics on how the contract is structured, including costs, duration, and termination clauses. Ask if it is aware of any potential benefits or discounts from cyber insurance providers.
☐	What services are provided in your MDR package and does it include 24/7/365 coverage?	Attacks can happen at any time, so you want someone watching and responding to potential issues 24/7/365. Make sure your MDR provider has around-the-clock coverage so that you can focus on running your business and living your life.

	QUESTION	WHAT TO LOOK FOR
☐	What insight into up-to-date, real-world cyber claims do you have?	Some MDR providers have access to practical claims and data from actual incidents. This insight into real risks allows them to offer more informed advice and deliver solutions that enhance overall security more effectively.
☐	What type of response actions do you take when you detect an issue?	When an incident occurs, it's important to have an MDR provider that will take action to remediate the issues with an immediate response. Some MDR providers limit their role to simply alerting you of issues, rather than actually handling them. The best providers will align with you on when their analysts will respond and when they will escalate to you.
☐	What type of support will you provide in helping me build a strong security program?	Your MDR provider should help you set up your entire security program to get the full benefits of the MDR service. This not only means ensuring your EDR is properly configured and fully deployed in your environment, but also supporting you in constructing your overall security program by identifying gaps that could leave you vulnerable.

MDR: A Powerhouse Security Asset For Your Small Business

Investing in the right MDR solution can drastically reduce your vulnerabilities and strengthen your cybersecurity posture to meet the needs of your business. While it does require time and resources, the potential return makes it an investment worth the effort. As the cyber landscape continues to evolve, this guide can be used to help you safeguard your business.

At-Bay's Stance™ MDR brings top-tier security within reach for small and mid-size businesses, proactively managing risks through threat prevention, detection, and response, leveraging both advanced software and a team of cybersecurity experts. Stance MDR can optimize protection and lower costs, making it a valuable offering for businesses looking to enhance their cybersecurity against ever-changing threats. It's a key part of InsurSec, which combines At-Bay's insurance expertise, world-class cybersecurity team, and a market-leading security software solution. With Stance MDR, At-Bay[1] can deliver enterprise-level security technology and expertise at a price growing businesses can afford.

[1] At-Bay Security, LLC is a wholly owned subsidiary of At-Bay, Inc., providing cybersecurity services including MDR and incident response. At-Bay Security, LLC does not provide insurance services.