BitLyft
Cybersecurity

THE COMPLETE MDR BUYER'S GUIDE

COMPREHENSIVE GUIDE

Learn what to expect with Managed Detection and Response (MDR) services

TABLE OF CONTENTS

INTRODUCTION

Recent, widely-publicized cyber attacks have made it clear to businesses and organizations across all industries that no one is immune to attack. All businesses and organizations store and use data that could be considered valuable. If your organization is connected to the internet, you are at risk. These revelations put business owners in the difficult position of ingesting a large amount of information about the complex subject of cybersecurity to catch up and find protection. Furthermore, as threat actors devise more covert and sophisticated threats, older security measures quickly become outdated, forcing high-risk organizations to find new solutions. While these natural advances of technology and the growing attack surface present a variety of challenges for businesses and other organizations, many other incidents have occurred that create a perfect storm for effective cybercrime.

A massive increase in remote work driven by pandemic restrictions, the rapid growth of the IoT, and the increased use of online communications and activities provide threat actors with a vast array of potentially vulnerable endpoints to exploit. Businesses, schools, government agencies, and other organizations searching for a comprehensive solution are faced with the staggering costs of setting up an in-house security operations center (SOC) and the stark reality that cybersecurity professionals are in short supply. For many, a complete solution with effective software and skilled professionals will come in the form of Managed Detection and Response (MDR).

Supplied by a third-party provider, MDR is a group of services that offers organizations the protection of an off-site SOC combined with a comprehensive security stack that allows organizations to rapidly detect, analyze, investigate, and actively respond to cybersecurity threats. A high-quality MDR solution addresses many of the pain points business leaders face when searching for a complete cybersecurity package or updating a company's existing protection.

MDR addresses current cybersecurity needs and eliminates certain issues with other solutions in these ways:

- MDR is a turnkey experience with a predefined security stack
- 24/7 assistance is provided by experienced cybersecurity professionals in an off-site SOC
- Services are tailored to your organization and installed by the provider
- The services address the four points of cybersecurity (detection, analysis, investigation, and response) required to manage a threat
- A variety of tools and services are combined to provide an ongoing and effective solution for existing and evolving threats

Many organizations are already investigating MDR as a potential cybersecurity solution. However, finding the right provider and getting the services that will work for your company can be more of a challenge than anticipated. Cybersecurity offerings come in many forms and are often categorized differently by different providers. Without careful investigation, you could get services that are entirely different from what you thought you were paying for. Our MDR buyers guide is designed to help you understand the essential parts of MDR, how MDR compares to other solutions, a comparison of some top MDR providers, and what the MDR experience actually looks like from a customer's point of view.

ESSENTIAL PARTS OF MDR

Gartner defines Managed Detection and Response as "services that provide customers with remotely delivered modern security operations center (MSOC) functions. These functions allow organizations to rapidly detect, analyze, investigate and actively respond through threat mitigation and containment. MDR service providers offer a turnkey experience, using a predefined technology stack (covering areas such as endpoint, network, and cloud services) to collect relevant logs, data, and contextual information. This telemetry is analyzed within the provider's platform using a range of techniques. This process allows for investigation by experts skilled in threat hunting and incident management, who deliver actionable outcomes."

Let's see if we can condense that down to a single sentence. MDR services provide remotely delivered modern security operations center functions provided as a turnkey experience using a predefined technology stack to collect relevant information that is analyzed and categorized in a way that allows for investigation by experts.

It's quite a mouthful, isn't it? Even though we've stripped Gartner's definition down to the bare-bones information, it's easy to see how providers could interpret this definition to mean different things. However, when you study the definition carefully and break down the parts, you'll find that there are specific elements that services must include to be classified as MDR. These are the essential elements of MDR described by Gartner.

Remote SOC

Remote services are provided, installed, and implemented to your organization by a third-party provider. Ongoing assistance from experts is supplied in the form of threat hunting and incident management,

Detection

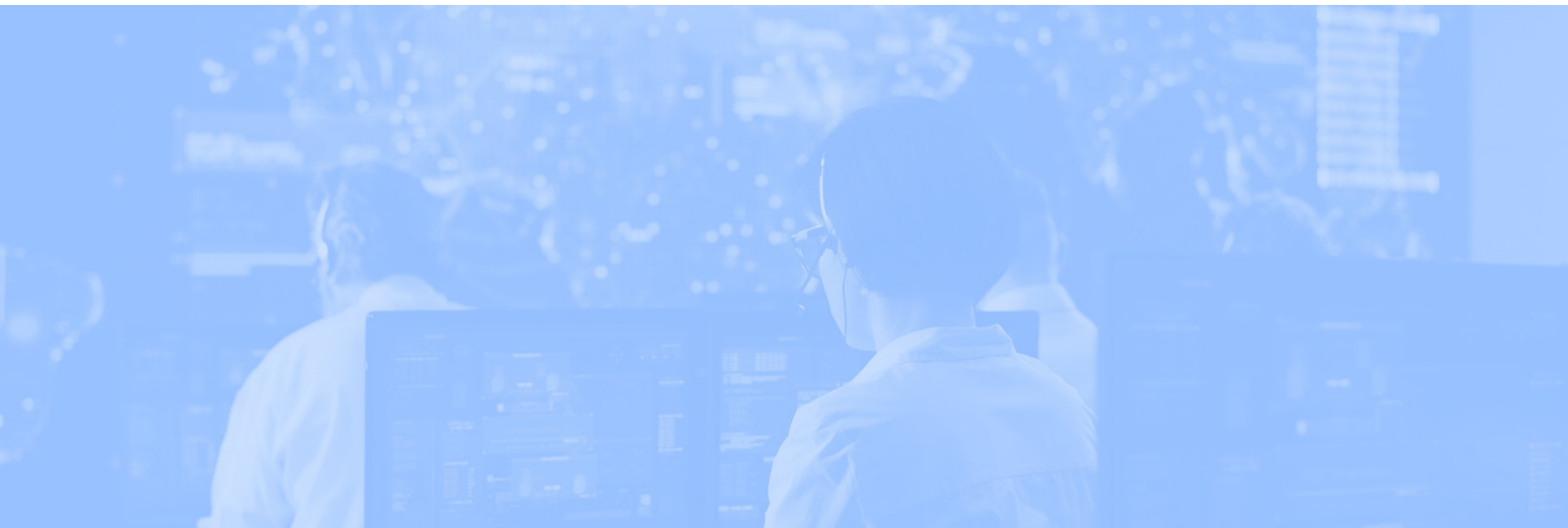
Security tools provide complete network visibility and log collection that allow automated threat detection when abnormal behavior occurs.

Analysis

Automated actions and human analysis are combined for further response and investigation into threats.

Investigation

As the threat is being contained, an investigation is launched to determine the depth of the breach and potential vulnerabilities.



Response

A combination of automation and human response is used to ensure the threat is contained and mitigated to avoid further damage.

Turnkey Experience

Software and other tools that make up your customized security stack are installed and deployed by your provider.

Technology

Specific technologies and tools are utilized within your network to take essential steps for threat detection and mitigation.

HOW MDR WORKS

Although several of the features required for Managed Detection and Response services are clear, there are many ways each portion can be interpreted. This is why it's important to understand how the tools and methods supplied by your MDR provider accomplish specific tasks to detect and eliminate sophisticated modern threats. Your MDR solution should contain these components to accomplish the essential tasks of MDR.

- Log management with SIEM
- Endpoint detection and response
- AI for proactive threat protection
- User entity behavior analytics (UEBA)
- SOAR to decrease response time
- Network monitoring for complete visibility
- Expert level analysts that act as an extension of your team

If you're looking for a deeper look into the essentials of MDR, check out our full description of the essential elements of MDR.

COMPARING MDR TO EDR TO XDR

If you're one of the many organizations planning to invest in cybersecurity, you've probably realized that Managed Detection and Response isn't the only confusing acronym to untangle. There are a variety of cybersecurity services available for organizations with different levels of security and different needs. With the evolving threat landscape and remote worktop of mind for most businesses, endpoint security and automated functions are some of the most sought-after features in any cybersecurity solution. Top cybersecurity offerings designed to tackle such modern threats include MDR, EDR, and XDR. Yet, these solutions don't all have the same capabilities. Before you choose which one is right for your organization, take the time to compare the three solutions.

Endpoint Detection and Response (EDR)

EDR is a cybersecurity solution that uses data analytics to identify potential endpoint threats before they occur, block malicious activity, and offer remediation suggestions. This type of protection has become crucial with the growth of Industry 4.0 and the wide implementation of remotely connected devices. Any device connected with your computer network can provide an entry for threat actors. These endpoints are considered particularly vulnerable since they often have minimal security. Endpoint detection provides a way to see the activity on your endpoints and identify suspicious behavior. Most importantly, the threat can be contained before going any further into the network.

EDR solutions must provide these capabilities.

- Detection of security incidents
- Containment of the incident at the endpoint
- Investigation of security incidents
- Remediation guidance for repairs and vulnerability assessment

While these capabilities offer significant benefits for detecting and mitigating endpoint threats, it's crucial to recognize that EDR is only a solution for endpoint security. It is designed to work in conjunction with other security tools and professionals.

Extended Detection and Response (XDR)

Understanding the details of XDR is slightly more difficult since it's still in the early stages of development and may be described differently by various types of vendors. While XDR uses some of the same techniques as EDR, it extends beyond EDR to include both endpoint and network activity. XDR solutions collect data to help identify and isolate threats across networks, cloud infrastructure, SaaS components, endpoints, and other network components. There are some idealized descriptions of XDR that suggest it is all-encompassing protection. However, the most accurate definition of XDR is an all-in-one platform to provide these tools.

- EDR
- Cloud access security brokers
- Secure web gateways
- Network firewalls
- Network intrusion prevention systems
- Unified threat management
- Identity and access management

It's important to note that XDR isn't a specific tool with defined parameters. It's more like a variety of tools bundled by a service provider. Like EDR, XDR is a tool designed to be installed and used by security experts for complete protection.

Managed Detection and Response (MDR)

As you're becoming more familiar with the components of Managed Detection and Response, you may recognize the biggest difference offered by this solution. While EDR and XDR are both tools used by professionals, MDR is an ongoing set of services that includes interaction with cybersecurity professionals.

Tools in your MDR solution may include:

- EDR
- SIEM
- Network traffic analysis
- User and entity behavior analytics
- Asset discovery
- Vulnerability management
- Intrusion detection
- Cloud vulnerability

Beyond the tools that make up your MDR solution, MDR offers the benefits of a remote SOC, providing you with around-the-clock access to cybersecurity experts. These experts act as an extension of your team and provide routine communication about your current cybersecurity posture as well as support when alerts and active threats are in progress. This is why MDR is the most comprehensive service available through a third-party provider.

For a more in-depth comparison, read our post, EDR VS MDR VS XDR: How They Differ and Which One Is Right for You.

COMPARING TOP MDR PROVIDERS

MDR provided by established cybersecurity professionals typically includes the essential elements as well as a trusted security stack. However, different vendors use a variety of tools and methods to achieve similar results. When you've chosen MDR for your cybersecurity solution, it's best to compare reputable providers before making a final decision. Some important elements that vary from one MDR provider to the next include communication style, security software, automation capabilities, involvement in incident response, and services offered by cybersecurity professionals. Our comparison of three top MDR providers can help you understand the differences between similar MDR services and which vendor might be the right choice for your organization.

Rapid7

Managed services by Rapid7 include vulnerability management, application security, and managed detection and response. This includes around-the-clock monitoring and attacker intelligence based on millions of endpoints. Rapid7 MDR promises to accomplish these results:

- Detection of threats within the first 60 days
- Tailored service based on your environment and security goals
- Finds known and unknown attackers with multi-layered detection methodologies across the SOC triad.

Rapid7 uses several tools and methods to detect incoming security threats, which include proprietary threat intelligence, behavioral analytics. NTA, and human threat hunts. Through these methods, Rapid7 MDR achieves real-time incident detection and validation, proactive threat hunting, and behavioral-based detection for your unique network.

Arctic Wolf

MDR from Arctic Wolf eliminates alert fatigue and false positives to promote a faster response with detection and response capabilities tailored to your organization. Arctic Wolf MDR promises to accomplish these results.

- Quickly identify and categorize risks
- Understanding of your current digital risk posture for identification of security gaps
- Find vulnerabilities and start prioritizing security improvements

Arctic Wolf MDR begins with broad visibility through software that integrates with your existing technology stack. This includes 24/7 monitoring for threats and risks. When threats are identified, data analysts take over to investigate suspicious activity.

BitLyft

BitLyft utilizes a variety of tools to supercharge security analysts with advanced detection and automated threat remediation. MDR from BitLyft provides greater visibility for threat detection and provides lightning-fast response time tuned to your environment. BitLyft AIR offers these results:

- Heavily enriched insights into threats, vulnerabilities, and user behavior
- 24/7 professional support with an expert security team
- Reduced dwell time with automated responses implemented for your network
- Integrated threat intelligence for proactive protection

At BitLyft, we use a variety of tools and methods to offer comprehensive security against known and unknown threats. BitLyft MDR begins with complete visibility into your network provided by Securonix SIEM. Analysts use software and data collected from your network to establish normal behavior and recognize threats. Built-in compliance, automated responses, and future threat protection through herd immunity are additional benefits of BitLyft Air.

To learn more about these highly rated MDR providers, read our in-depth comparison.

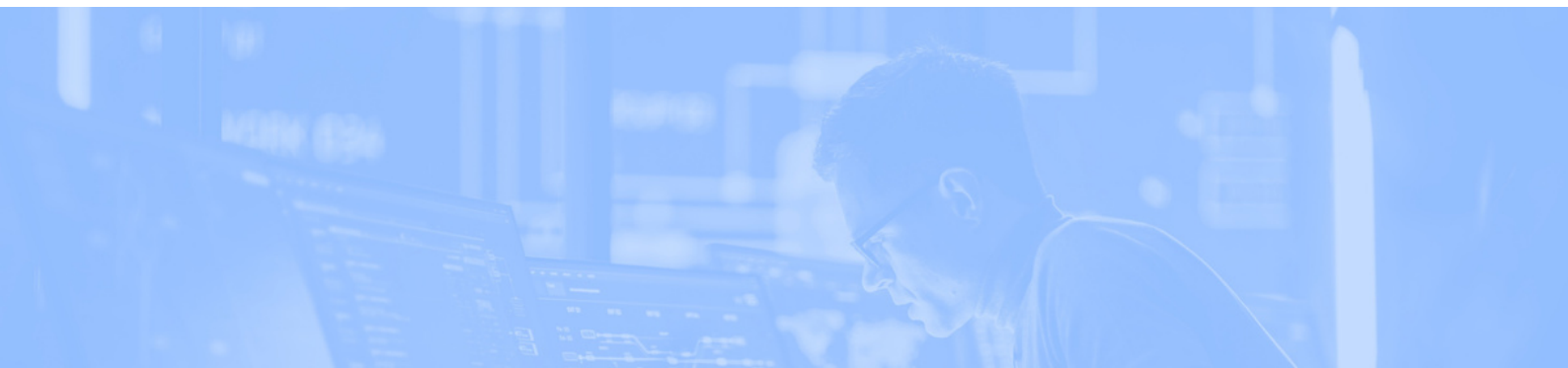
WHAT SHOULD YOUR UNIQUE MDR SOLUTION INCLUDE?

We've covered the essential elements of MDR. Yet, defining MDR doesn't take into consideration how businesses and organizations differ from one another or your current security posture. The ability to customize services to your unique network is a key benefit of MDR. It allows you to determine whether you need services to close gaps or a complete solution. Before hiring a vendor, you should know exactly why you're investing in MDR and what you expect from the services provided.

Common Reasons to Adopt MDR

Taking the time to recognize your expectations and how MDR services will improve your security posture will help you choose the right vendor and get the most out of your services. These are the most common reasons organizations seek MDR services.

- Limited staffing options due to an ongoing talent shortage in the cybersecurity field
- Avoid alert fatigue that arises from false positives
- Eliminate repetitive tasks with automation and assistance from cybersecurity professionals
- Sophisticated tools and professional threat hunting that provide proactive threat detection instead of simply responding to attacks
- 24/7 protection to close gaps left by your existing security solution



Tools and Methods to Meet Your Unique Needs

An effective MDR offers a variety of advanced tools and services to provide your business or organization with a comprehensive cloud-based security solution that offers continuous support from cybersecurity professionals. The tools, software, and communication should complement your existing security posture in a way that makes tasks easier and security more effective. When searching for an MDR provider, it's important to consider how the vendor's services meet your organizational needs. MDR services should include these capabilities.

Threat Intelligence

Through log collection and data analysis, MDR provides ongoing intelligence about potential threats with SIEM, EDR, network firewalls, threat hunting, vulnerability management, incident response, and UEBA. Bitlyft also utilizes crowdsourced intelligence to offer herd immunity.

24/7 Coverage

With the combined use of software and human expertise, MDR provides 24/7 threat monitoring, detection, and response.

Incident Investigation

With the use of automated responses to alerts and the professional knowledge of highly trained security specialists, a thorough investigation is conducted for every incident and new information is added to the threat intelligence cycle.

Threat Containment

Sophisticated attacks are often designed to be discreet to help threat actors carry out their objective while posing as normal network activity. MDR tools and functions isolate these attacks to a single device or area of operations to contain threats without taking business systems offline.

Threat Monitoring

Continuous monitoring of your network with software, data analysis, and UEBA allows your organization to recognize and halt threats before attacks occur.

Remote Response Services

24/7 response from experienced cybersecurity professionals comes in many forms. Take time to ask security vendors exactly what services they provide.

Advanced Analytics

A variety of tools provide administrators and analysts with the data necessary to customize threat models based on your organization's specific needs and design automated responses to relevant threats.

Human Expertise

Ongoing assistance from your off-site SOC should include installation and implementation of cybersecurity software, updates, routine communication, emergency response, and timely answers to questions.

Incident Validation

The best MDR providers perform alert validation to minimize the number of false positives that reach your team. This means when threat alerts reach your team, they will include specific information about why the threat is likely valid.

For a deeper look into the tools and actions that make up a comprehensive MDR solution, read our complete guide to what your MDR solution should include.

MDR COMPONENT CHECKLIST

- ☑ Threat Intelligence
- ☑ 24/7 Coverage
- ☑ Incident Investigation
- ☑ Threat Containment
- ☑ Threat Monitoring
- ☑ Remote Response Services
- ☑ Advanced Analytics
- ☑ Human Expertise
- ☑ Incident Validation

A LOOK INTO THE MDR EXPERIENCE

As an MDR provider accustomed to the most effective cybersecurity tools and the most advanced methods of fighting cybercrime, it makes sense for us to share a lot of information about the tools of the trade. Still, for the average layperson simply hoping to find adequate protection within their budget, it can be hard to understand exactly how MDR works from the customer's point of view. This glimpse into the MDR experience can help you understand how MDR works to complement your current cybersecurity efforts and exactly how MDR services lift the burden from your team.

Your Responsibilities vs Those of Your MDR Provider

The best MDR providers offer services that act as a partnership to protect your business. It's crucial to determine what tasks you have the capacity to complete and the support that will be provided by your MDR vendor. When choosing a provider, ask about their level of involvement in these activities.

- Software optimization for proper log collection and effective automated threat responses
- Alert monitoring to weed out false positives, so alerts that reach your team are relevant
- The visibility that extends to cloud storage and other cloud environments
- Tools to provide compliance management and generate necessary reports

Top Questions to Ask your Prospective MDR Provider

Choosing an MDR provider is similar to inviting a new partner into your organization. To make the best match, it's important to make sure that the vendor's service is compatible with your company's workflow and addresses specific security pain points. Before making a final choice, get detailed answers to these top 10 questions to ask your MDR provider.

- Are you familiar with my industry?
- Will I need specialized software to work with you?
- What's your main form of contact?
- What does reporting look like?
- Is the security plan customizable?
- Is 24/7 support available?
- How do you handle proactive threat detection?
- Is there comprehensive visibility?
- Is the solution automated and scalable?
- Will successful attacks be reduced?

Your MDR experience will depend heavily on your understanding of your organizational needs and the communication style of your provider. By determining your expectations, you can get a clearer picture of the assistance you need from your provider. Learn more about the MDR experience and what you can expect in our article A Look Into the MDR Experience

This guide offers a glimpse into everything you need to know before choosing an MDR provider. Each section relates to an in-depth article that offers extensive information for additional research. For more information about MDR services and choosing a provider, contact the cybersecurity experts at Bitlyft.

WE'RE HERE TO HELP

When you're looking to protect an entire organization on a limited budget you can have trouble prioritizing spending. The one certainty is that you need people. Whether you're an established company, or just getting started, BitLyft has a solution to help you protect your organization from cyber attacks. Our team of cybersecurity professionals can fully augment, or come along your existing team to help you illuminate and eliminate cyber threats.

Schedule a meeting with our BitLyft Success Team to get started.

"In over a decade of helping businesses decide to build their own SOC or outsource to a SOCaaS provider, I have seen time and time again a much better ROI to subscribe to the right vendor than to build internally. Everyone's environment is different and the use cases can vary. However, there's never a bad reason to take a moment to review your current state and future needs with experts like those at BitLyft."

securonix

MIKE JOHNSON
CHANNEL SALES DIRECTOR
SECURONIX, INC.

THE BITLYFT APPROACH

Our approach to cybersecurity focus on providing our clients with a comprehensive platform that goes beyond MDR, SIEMaaS, and MSSP models. Our team of security experts coupled with our powerful BitLyft AIR platform illuminates and eliminates cyber threats in seconds before they have time to harm you or your customers.

AIR PLATFORM

Visibility
Security Information and Event Management (SIEM)

Expert People
Security Operations Center (SOC)

Speed & Efficiency
Security Orchestration Automation and Response (SOAR)

Intelligence & Accuracy
Central Threat Intelligence (CTI)

The BitLyft AIR platform merges the best of people and software to provide you unparalleled protection for your organization.

LEARN HOW

info@bitlyft.com | www.bitlyft.com | 517.220.0990