



THE LEADER IN SECURITY OPERATIONS

# MDR

## BUYER'S GUIDE



How to Select a Managed Detection and Response Solution for Your Organization



# TABLE OF CONTENTS

## 01

EXECUTIVE  
SUMMARY

4

## 02

CREATING A STRONGER  
SECURITY POSTURE WITH MDR

6

## 03

THE ADVANTAGES OF  
MDR SOLUTIONS

8

## 04

KEY MDR FEATURES  
AND CAPABILITIES

10

## 05

TOP CRITERIA FOR  
EVALUATING MDR VENDORS

13

## 06

FINAL  
THOUGHTS

17



# 01



## EXECUTIVE SUMMARY





# EXECUTIVE SUMMARY

In the era of digital transformation, many organizations find it a never-ending struggle to defend against rampant cybercrime. Organizations are starting to realize they can't stop data breaches by adding more tools. Because adding tools also adds more consoles and more alerts, both of which add complexity without actually improving security.

At the same time, the expanding attack surface makes the IT environment increasingly vulnerable. Identifying and managing vulnerabilities has become exponentially more complex with more devices joining the corporate network, a mobile workforce connecting to the network from anywhere, and applications moving to the cloud.

In combination with limited in-house resources, the ongoing cybersecurity skills gap, rapid growth in the number and sophistication of threats, and an unstable geo-political environment, has overwhelmed many security teams who are typically understaffed, and unable to keep up.

In this new normal, a data breach or network intrusion is all but inevitable. And the result is not only loss of productivity and revenue, but also potential liability, regulatory noncompliance, and enormous reputational damage.

Managed Detection and Response (MDR) solutions can help address these challenges not only through traditional threat detection, response, and remediation capabilities, but also by providing ongoing security program improvements and supporting an organization's security posture improvement over time.

Use this guide to assess vendors' offerings and identify questions you should be asking as you evaluate potential MDR providers.

***In this new reality, a data breach or network intrusion is all but inevitable. And the result is not only loss of productivity and revenue, but also potential liability, regulatory noncompliance, and enormous reputational damage.***



02

**CREATING A STRONGER  
SECURITY POSTURE WITH  
MANAGED DETECTION  
AND RESPONSE**



# CREATING A STRONGER SECURITY POSTURE WITH MDR

As the threat landscape evolves and expands, so must your defense strategy. But trying to stay ahead of the curve has become increasingly difficult.

Alert triage can simply overwhelm security teams, particularly those that are understaffed. Research shows teams only respond to approximately half the alerts they see on a daily basis. And with fewer than 40% of organizations seeing less than 5,000 alerts a day (while the number of organizations receiving more than 100,000 alerts a day has grown from 11% to 16% over the course of three years)<sup>1</sup>, too often the doors are wide open for attackers.

These inadequate defenses come with a significant price tag that affects both the top and bottom lines. The costs of data breaches continue to escalate — currently reaching \$164 per record, or an average of \$4.35 million per breach in 2022.<sup>2</sup>

**CALCULATE THE COST OF A BREACH FOR YOUR ORGANIZATION**

To combat the significant growth in attacks, managed detection and response (MDR) is an increasingly popular solution since it delivers real-time, 24x7 monitoring, detection and response using a holistic, turnkey approach. A cost-effective alternative to building an in-house security operations center (SOC), MDR protects against advanced threats and enables organizations of all sizes to follow cybersecurity best practices even within resource constraints.

## 67%

The percentage of IT teams that ignore lower priority alerts.

— 2021 State of SecOps, Forrester

## \$4.35M

The average cost of a data breach.

— 2022 Cost of a Data Breach Report 2022, IBM and Ponemon Institute

## 277 DAYS

The average time it takes an organization to identify and contain a breach.

— 2022 Cost of a Data Breach Report 2022, IBM and Ponemon Institute

## QUICK REFERENCE

### Endpoint Security Solutions

Next-generation endpoint security solutions focus on advanced threats, including continuous monitoring and response. These solutions can include Endpoint Detection and Response (EDR) Endpoint Protection Platforms (EPP) and Next-Generation Antivirus (NGAV).

### Network Monitoring and Detection

A hardware or software appliance that provides real-time monitoring of network traffic and generates automatic alerts upon detection of indicators of compromise (IOCs).

### Incident Response

An organized, systematic approach to addressing the impacts of a security incident or data breach with the goal of limiting the damage to the infrastructure and the business.

### Managed Detection and Response (MDR)

A comprehensive solution for continuous monitoring, threat detection, and incident response provided by a third-party vendor.

### Managed Service Provider (MSP)

An IT vendor that provides a service, software, or technology, such as remotely managing IT infrastructure, on a subscription basis.

### Managed Security Services Provider (MSSP)

An MSP that provides 24x7 management, monitoring, and maintenance of security services, such as intrusion detection and endpoint protection, at a fixed subscription cost.

### SIEM (Security Information and Event Management)

An integrated system that combines security information management and security event management to collect and correlate security events and alerts.

### Extended Detection and Response (XDR)

Extended Detection and Response (XDR) consolidates the data and tools necessary to provide enhanced visibility, analysis, and response for all system risks associated with users, endpoints, networks, and other telemetry sources. It helps unify workload and endpoint security processes through improved visibility, automation, and streamlined threat detection.

### SOC (Security Operations Center)

A centralized approach that combines security technology, people, and processes to manage threats — from prevention and detection to investigation and response.

### Threat Intelligence

Evidence-based data about current and potential threats, including context, indicators of compromise, mechanisms, and actionable information.

### Cloud Detection and Response (CDR)

Software solutions that are designed to monitor cloud resources for utilization and threat activity. Ideal CDR solutions should monitor a combination of IaaS, SaaS, and PaaS cloud architectures.



# 03

## **THE ADVANTAGES OF MDR SOLUTIONS**



# THE ADVANTAGES OF MDR SOLUTIONS

Gartner forecasts that 60 percent of all organizations will use MDR by 2025<sup>3</sup>. The market is growing in response to the need organizations have to now manage threats around the clock. MDR enables companies to expand capabilities beyond in-house resources.

## THE ADVANTAGES OF MDR SERVICES INCLUDE:

### 01

#### Greater Expertise

MDR vendors employ seasoned cybersecurity specialists who have needed expertise and a wide range of skills, serve as dedicated teams, and understand their clients' particular business needs.

### 03

#### Better Technology

MDR providers use advanced technology and a comprehensive suite of tools.

### 02

#### An Integrated Approach

A framework that integrates threat detection and vulnerability assessment enables you to more efficiently manage risks from both known and unknown threats.

### 04

#### Cost Savings

The technology and 24x7 staffing of a SOC are cost-prohibitive for many organizations, while an MDR solution acts as a force multiplier that is easier on a budget.



*Gartner forecasts that 60 percent of all organizations will use MDR by 2025<sup>3</sup>.*

## MDR VS. MSSP VS. mEDR

The introduction of managed detection and response (MDR) was designed to take a different approach from traditional managed security services. Managed security service providers (MSSPs) initially acted as extensions of legacy Managed Service Providers (MSPs) and therefore are designed to focus primarily on functions such as remotely managing security devices (like firewalls, for example), managing vulnerabilities, and monitoring network traffic. Since the focus of these services are primarily based on the tools and technology they manage, their capabilities are typically limited to known threats and include limited mitigation strategies.

Modern MDR also differs greatly from managed endpoint detection and response (mEDR) services because mEDR services are focused on the tools they manage and don't provide visibility into the network or cloud. Additionally, managed EDR services are limited in scope, as they are devoted solely to the EDR tool and therefore provide less relief to the already overworked and understaffed IT teams. When considering a managed EDR provider you should ask yourself a simple question: am I looking for a service dedicated to managing my EDR, or am I looking for a service dedicated to managing my security operations? If you are looking for a service entirely devoted to your endpoint detection and response architecture, then a managed EDR service may be right for you.

An MDR provider gives you contextual understanding of your environment and digs deeper into the nuanced details that make your environment vulnerable to threats. And unlike MSSPs or EDR providers, managed detection and response is a holistic approach that helps you monitor and understand your overall security posture while also improving compliance and reducing your risks.







# 04

## **KEY MDR FEATURES AND CAPABILITIES**



# KEY MDR FEATURES AND CAPABILITIES

*Specific capabilities range from vendor to vendor. However, look for these five key features when exploring the market:*



## 24x7, Real-Time Threat Detection

Cybercriminals don't keep office hours. A security incident can unfold at any time. You need a 24x7 team of security analysts and engineers who monitor and triage alerts across the entirety of your IT environment, and actively respond to indicators of compromise when they occur. You can't afford to wait for a report to be delivered to you hours or days later.



## Threat Intelligence Integration

To reduce the risk of advanced threats, you need the latest threat intelligence from multiple sources. MDR solutions that integrate threat intelligence, as well as behavioral analytics, are much better positioned to analyze data in the right context to detect advanced, unknown threats.



## Advanced Analytics

Leveraging machine learning, threat intelligence, and big data, advanced analytics is a critical MDR component that enables real-time threat detection. Top providers invest heavily in analytics platforms and other tools to analyze data in context, as well as correlate events across the entire environment.



## Incident Response

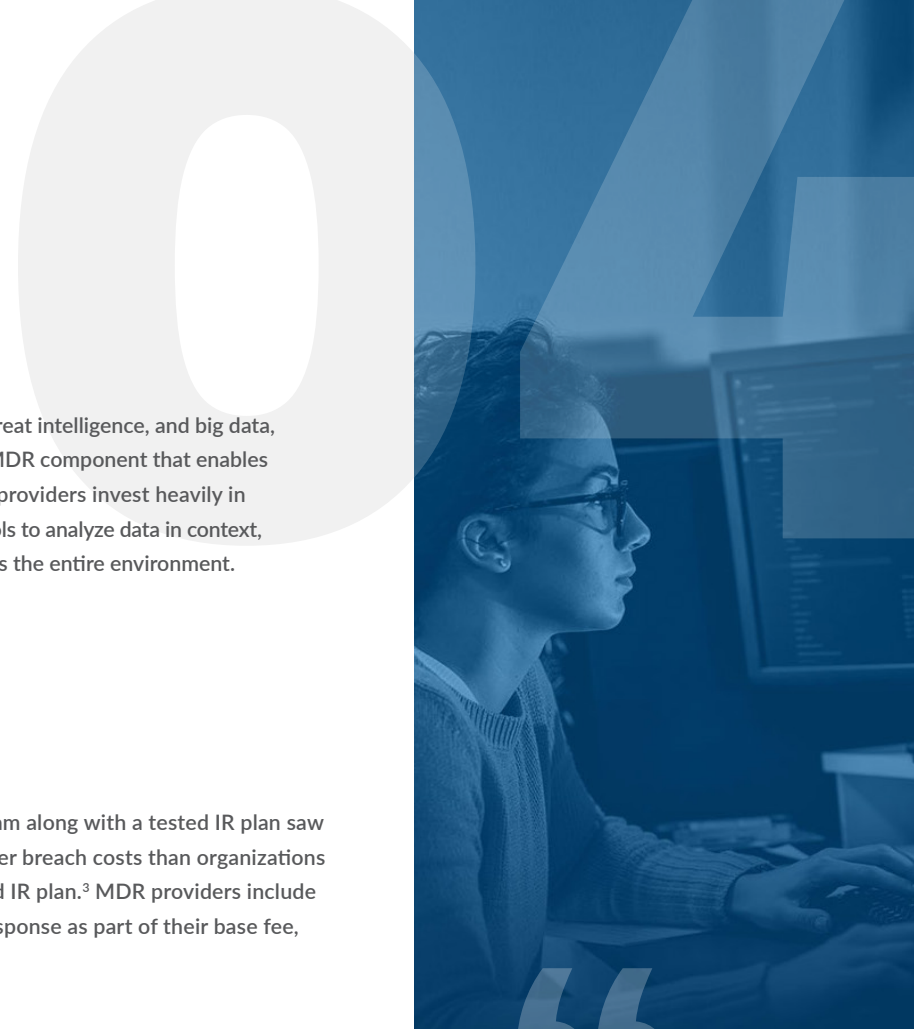
Organizations utilizing an IR team along with a tested IR plan saw an average of \$2.66 million lower breach costs than organizations without an IR team and a tested IR plan.<sup>3</sup> MDR providers include different degrees of incident response as part of their base fee, along with crisis support.



## Visibility

MDR solutions are capable of incorporating telemetry from across the enterprise, unifying disparate solutions in a single platform, thereby creating a comprehensive, holistic view of an organization's IT environment.

CONTINUED ON NEXT PAGE



**“To effectively staff a SOC for 24x7 coverage, it would require a team of 10 and upwards of 30 or more for large enterprises.”**

— Security Magazine<sup>4</sup>



# KEY MDR FEATURES AND CAPABILITIES





# 05

## **TOP CRITERIA FOR EVALUATING MDR VENDORS**



# TOP CRITERIA FOR EVALUATING MDR VENDORS

## Technology Stack Capabilities

While some vendors employ EDR agents provided by an outside vendor, others offer a comprehensive, proprietary technology stack for a SIEM solution. Using network sensors deployed on customers' premises, the provider's stack should include tools such as network traffic analysis and endpoint activity monitoring. When researching MDR providers, ensure their technology stack fits within your IT and security technology, such as your point tools, and that you won't need to make an additional investment.

## Ability to Monitor Both On-Premises and Cloud Assets

You need visibility into, and protection for, your entire environment — both on-premises and in the cloud. Many providers, however, only specialize in one or the other. As the adoption of IaaS and SaaS grows, monitoring those environments becomes more critical.

Although public cloud providers offer various native security features, you can't rely on those capabilities to keep your cloud secure.

## Common Framework for Known and Unknown Threats

Many malware campaigns and other attacks exploit vulnerabilities that have had patches available for months — and sometimes years. These tactics are successful because it's common for organizations to lack strong policies for managing vulnerabilities.

Some vendors offer a common framework that helps you identify these known vulnerabilities and prioritize patching, while at the same time the MDR solution continuously monitors for new threats that emerge in the wild. The added benefit is that you only need to work with one vendor to ensure you're covered in both areas.

## Unlimited Log Ingestion

Unlike alternatives that charge based on event or log volume or license capabilities separately, foundational technologies such as endpoint agents, unlimited log retention and search, and external network scanning are included as part of the core MDR offering. The MDR approach is to provide coverage across your attack surface based on number of users, servers, and internet egress points — providing coverage that grows along with you as your organization grows.

## 3 IMPORTANT QUESTIONS TO ASK VENDORS: TOOLS & THREAT LANDSCAPE

### 01

Do you leverage threat intelligence and known vulnerabilities from your customer base to proactively protect your other customers? How?

### 02

What is your pricing for log ingestion?  
What is your log retention policy?

### 03

Do you require customers to use certain tools or technologies or can you work with my existing stack?



# TOP CRITERIA FOR EVALUATING MDR VENDORS

## 24x7 Eyes-on-Glass Monitoring

Threats can hit your organization at any time, and 24x7 live monitoring is a critical factor that determines your ability to detect and respond to a security incident quickly and effectively. A vendor who doesn't have 24x7 staffing to provide eyes-on-glass monitoring leaves you with blind spots and a limited ability to detect malicious activity.

## Real-Time Alerts, Time to Remediation, and Time to Respond

Reducing your time to respond and your time to remediation is critical during a security incident. Weigh the response capabilities of prospective MDR providers: Do they effectively monitor, triage, and investigate alerts in real time? Do they use a mix of human and artificial intelligence to shorten the time between detection and response?

## Incident Response and Remediation Capabilities

Attackers can cause large amounts of damage in a short amount of time. Fast threat containment and remediation is crucial to minimizing the impact on your business. You need an MDR partner with an experienced incident response team who can take immediate steps to facilitate a speedy remediation.

## 6 IMPORTANT QUESTIONS TO ASK VENDORS: PROCESS

01

Will you need to change your infrastructure or deploy new technology? Do you need to adapt to the MDR vendor's technology stack?

02

Does the vendor monitor and provide security around your existing applications and those you plan to use in the future?

03

Which types of updates and reports do they provide and how frequently?

04

Which log sources does the vendor collect and retain?

05

Can you directly search your log information?

06

How do the vendor's security experts engage/communicate with your in-house team?



# TOP CRITERIA FOR EVALUATING MDR VENDORS

## Compliance Reporting and Custom Reports

Regulatory compliance is a major concern for select industries, and MDR solutions need to adapt to this new regulatory environment.

Choose an MDR partner who offers reporting on policies for your compliance regime (PCI, DSS, HIPAA) and areas such as data privacy and network mapping — you'll not only simplify compliance, but also reduce audit costs.

## Predictable Pricing

It's difficult to budget for security if your MDR provider charges based on log volume. Imagine the costs when an incident requires sifting through an enormous collection of activity data.

A fixed, recurring price that's based on your attack surface rather than log volume simplifies your pricing structure while helping with cost control.

## Consistent Relationships With Dedicated Advisers

If you have to work with a different analyst every time you have an issue or a question, your security contacts don't really have the complete understanding of your business and operations. Conversely, when a vendor provides a dedicated team of experts and a single point of contact, you can build a trust-based, consistent relationship.

A consistent team is the foundation for having the MDR solution as an extension of your internal team.

## 6 IMPORTANT QUESTIONS TO ASK VENDORS: SERVICE OFFERING

01

Does the vendor also offer risk management services on the same incident framework?

02

Are both cloud and on-premises infrastructure monitored for security threats? What cloud assets?

03

What is the vendor's pricing model? Is it a fixed subscription price or based on log volume?

04

Will you receive a dedicated point of contact/support? Are they available 24x7 or on a preset schedule?

05

Will you have direct access to your dedicated point of contact/support? What channels of communication are available to you: phone, gated chat, etc.?

06

How do the vendor's services scale/tailor to your needs?



# 06

## FINAL THOUGHTS





# FINAL THOUGHTS

Whether your organization still needs internal detection and response capabilities or just needs more flexible technology choices, a managed detection and response solution can help you keep up with the changing threat landscape. But not all MDR providers are the same. It's important to ensure their solution fits your organization's specific needs, existing security capabilities, budget, and maturity level.

However, a trusted MDR provider is not just about technology and expertise. Find a partner who will get to know your business deeply and will build a long-lasting relationship with your internal team. An effective approach to threat detection and response requires both trust and collaboration.

[REQUEST A DEMO](#)

#### Sources

- 1 [https://www.cisco.com/c/en\\_us/products/security/ciso-benchmark-report-2020.html](https://www.cisco.com/c/en_us/products/security/ciso-benchmark-report-2020.html)
- 2 <https://www.ibm.com/reports/data-breach>
- 3 <https://arcticwolf.com/resource/aw/analyst-Gartner-MDR-Guide-2023>
- 4 <https://www.securitymagazine.com/articles/87717-staffing-your-security-operations-center-to-run-like-a-well-oiled-machine>



**SOC2 TYPE II CERTIFIED**



ISO 27001  
CERTIFIED  
CYBERGUARD  
COMPLIANCE

**CONTACT US**

arcticwolf.com  
1-888-272-8429  
ask@arcticwolf.com



# ABOUT ARCTIC WOLF®

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, identity, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit [arcticwolf.com](https://arcticwolf.com).