eSENTIRE®

The Definitive Guide to Managed Detection and Response (MDR)

Balancing Risk, Cost and Capabilities.

Table of Contents

Introduction

FROM CONCEPT TO CRIMINALITY

A first-mover advantage in chess is inherently enjoyed by the player who opens the game, taking the upper hand with an offensive strategy, while forcing the opponent to adopt a defensive strategy. Much like chess, the history of cybersecurity follows similar gameplay.

In 1971, a computer researcher named Bob Thomas created a program named Creeper, which moved between mainframe computers connected to the ARPANET and outputted the message, "I'm the creeper: catch me if you can."

Intrigued by this idea, Ray Tomlinson (who invented email the same year) modified Creeper to replicate itself, rather than move itself, thereby creating the first self-replicating worm. Subsequently, Tomlinson also created the first antivirus program, Reaper, to chase and delete Creeper. As they say, the rest is history.

Originally rooted in academia, cybersecurity soon took on a darker nature when criminals took an interest. In the late '80s, the Morris worm nearly wiped out the early internet; in doing so, it had the effect of spurring recognition of the potential weaponization and monetization of cyberpower.[1]

Fast forward to today: global cybersecurity spending will exceed $200 billion in 2019, and cybercrime is expected to cost $6 trillion annually by 2021.

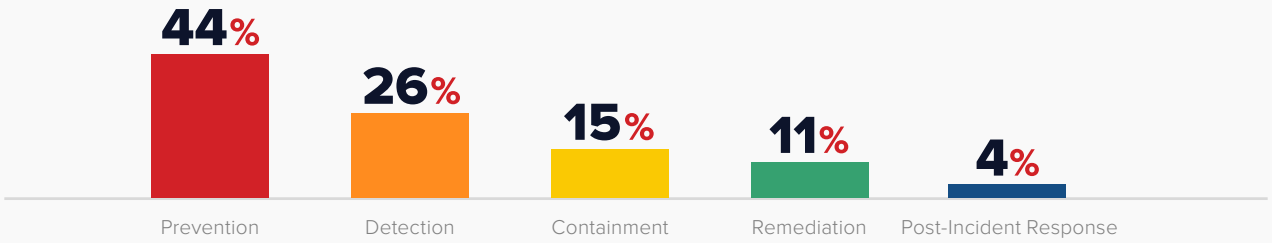
From the Morris worm of 1988 to the thousands of new exploits that now emerge on a daily basis each year, cyberattackers have demonstrated over the past three decades precision, skill and creativity in exploiting new technologies and applications. With the first-mover advantage of time and calculated execution, cyberattackers enjoy continued success despite enormous investments in cyberdefenses.

[1]Named after its creator, Robert Tappan Morris, the Morris worm also resulted in the first felony conviction in the United States under the 1986 Computer Fraud and Abuse Act

Introduction

Attackers enjoy a first-mover advantage, whether they bide their time or strike quickly. Despite large defensive investments, particularly in prevention, breaches remain hidden longer and take longer to contain than ever before, leading to significant real-world consequences for organizations.

DEFENSIVE INVESTMENT[2]



ATTACKER SPEED[3]

1-5 HOURS: 15%

5-10 HOURS: 20%

10-15 HOURS: 19%

>15 HOURS: 46%

CONSEQUENCES[5]

Abnormal Client Churn:

2018: **3.4%**

2019: **3.9%**

Average Cost of Breach: **$3.92M**

Per Employee (SMBs): **$3,533**

Cost Per Record: **$150**

DEFENSIVE SPEED[4]

Mean Time to Identify a Breach (Days):

2017: **191**

2018: **197**

2019: **206**

Days to Contain a Breach:

2017: **66**

2018: **69**

2019: **73**

[2]Ponemon (March 2018): Third Annual Study on the Cyber Resilient Organization
[3]2018 Nuix Black Report
[4,5]Ponemon: 2019 Cost of a Data Breach Study

The Advent of Managed Detection and Response (MDR)

Under-resourced, overextended and facing complications due to distributed people, process and technology, cybersecurity teams often struggle with threat prevention, detection, response and recovery activities.

Historically, prevention commanded the largest allocation of budget and resources. However, as threat actors developed more sophisticated attacks capable of bypassing preventative measures, the need for equal investment in detection and response capabilities became clear.

Released in 2016, the inaugural Gartner Market Guide for Managed Detection and Response Services[6] cited an emerging category of security service providers that "improves threat detection monitoring and incident response capabilities via a turnkey approach to detecting threats that have bypassed other controls."

Going back to as early as 2011, the concept of Managed Detection and Response (MDR) represents an acknowledgment that prevention will fail in some instances. Risk mitigation is dependent upon how fast an attack can be detected, and more importantly, contained and remediated before business is disrupted.

In this high stakes race against time, the threat detection and response challenge is exacerbated by digital transformation and mobility that have substantially expanded the attack surface. What was once a defined perimeter is now a borderless environment, which can span on-premises and cloud domains. With increased pressures from competitive markets, socioeconomic factors and regulatory consequences, security teams are looking for Security Operations Center (SOC) services to bolster internal capabilities with improved detection and response.

[6]Gartner Market Guide for Managed Detection and Response Services, Toby Bussa, Craig Lawson, Kelly Kavanagh, Sid Deshpande, Craig Lawson, Pete Shoard, 10 May 2016

From prevention to modern threat management; over time, the mitigated risk has outpaced the total cost of solution ownership/investment, resulting in greater customer value

PREVENTION TECHNOLOGY AND DEVICE MANAGEMENT

Early stages of security services centered around prevention and leveraged firewalls, antivirus and patching as proxies for risk management. As device numbers grew, organizations outsourced management of these devices, increasing scale but falling short in mitigating risk.

ALERT MANAGEMENT AND ALERT RESPONSE

As the attack surface spread and regulatory consequences grew in severity, focus shifted to correlating signals and generating alerts that could be actioned quickly while satisfying compliance. Unfortunately, the majority of alerts resulted in longer incident dwell times due to lack of personnel and the expertise to hunt, confirm and contain threats in a timely manner.

PROACTIVE AND PREDICTIVE RESPONSE

Ultimately, organizations recognized that achieving compliance alone does not equal effective cybersecurity. As a result, proactive and predictive threat management emerged. Both approaches leverage advanced technologies, including artificial intelligence, to illuminate the most elusive threats, to reduce false positives and to predict cyberattackers' next moves.

Integrated response was the crucial factor in minimizing the dwell time of threat actors, alleviating the burden of staffing and operationalizing around-the-clock SOC.

A CROWDED, COMPLEX MARKETSPACE

While MDR has been validated in necessity and efficacy, the marketplace for such services has become complex. Early-stage security organizations such as managed security service providers (MSSPs) and those providing managed Security Information and Event Management (SIEM) now recognize the opportunity and are pivoting messaging and services to align with MDR. This growing contingent creates confusion around what MDR is and should be.

The original 2016 version of the Gartner Market Guide for Managed Detection and Response Services cited 14 organizations as being representative vendors. Just three years later, the 2019 edition states that "Gartner estimates that there are now over 100 providers visible in this market claiming to offer MDR services." [7]

The lack of clear definition as to what constitutes MDR creates confusion about the attributes that organizations should use to qualify and validate MDR delivery from a potential provider. While no singular definition can yet be established, a number of clear categories that exist at the intersections of different levels of risk mitigation and cost have emerged.

This guide objectively defines the seven categories of MDR and explores their associated strengths and weaknesses. The goal is to help organizations make an informed choice that aligns with their business objectives, security resources and risk tolerance.

THE SEVEN CATEGORIES OF MDR:

- SOCaaS/Managed SIEM
- ED-little-r (Single Telemetry)
- MD-little-r (Multiple Telemetry)
- MD-little-r (Full Telemetry)
- ED-big-R (Single Telemetry)
- MD-big-R (Multiple Telemetry)
- MD-big-R (Full Telemetry)

[7]Gartner Market Guide for Managed Detection and Response Services, Toby Bussa, Kelly Kavanagh, Sid Deshpande, Craig Lawson, Pete Shoard, 15 July 2019

Criteria for Managed Detection and Response Providers

CURRENT MARKET DEFINITIONS

Many analyst firms have released reports or guides that include broad category definitions of MDR providers. Many of these publications also list and discuss provider attributes to assist organizations with choosing an appropriate solution. Most recently, the 2019 edition of Gartner's Market Guide for Managed Detection and Response Services categorized providers into four general styles, based upon "technology stacks:"

- Full stack from the provider
- Managed point solutions: Endpoint Detection and Response (EDR) and Network Detection and Response (NDR)
- Bring your own (BYO) technology stack
- Technologies for other environments and assets like cloud and devices: Infrastructure as a Service (IaaS), Security as a Service (SaaS), Operational Technology (OT) and Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices

While these categories begin to distinguish between different MDR service providers, they don't stipulate the attributes that determine a provider's ability to deliver on the very purpose of MDR (i.e., minimizing threat actor dwell time). But before we define technical criteria by which any MDR provider can be objectively and functionally assessed, let's briefly examine organizational factors that can be used to initially qualify potential MDR providers.

SPOTTING POTENTIAL RED FLAGS

With over 100 MDR providers now being tracked in the marketplace, backgrounds differ vastly from provider to provider. MSSPs have evolved their offerings, software providers have added a managed component, consultants have added technology stacks and other players were founded as pure-play MDR providers.

While background alone does not qualify or disqualify a provider's capabilities, it does supply important context and is suggestive of a provider's ability to meet an organization's individual security requirements.

SPOTTING POTENTIAL RED FLAGS

Outlined below are questions that should be asked of any potential MDR provider; the answers to which provide important information for subjectively assessing a provider's qualifications and suitability.

The answers to these questions will help you understand if MDR is a core competency of a particular provider or more of a trendy and opportunistic addition to a non-specialized portfolio.

COMPANY PROFILE

- What was the company's original mission?
- How has the company evolved over time?
- What is the company's core competency?
- Is the company a market leader or a follower?
- What is the leadership team's background?
- What markets does the company serve?

FINANCIAL STRENGTH

- Is the company public or private?
- Who are the company's backers/investors, and what are their track records?
- Is the company profitable?
- What is the company's commitment to—and investment in—research and development?
- How much of the company's revenue is attributable to MDR?
- For how long will the company remain financially viable without additional investment?

INNOVATION

- Does the company hold granted patents and intellectual property?
- What is the company's history of service and product releases?
- Does the service and product release history indicate reactive response to cyberlandscape developments or proactive anticipation of emerging shifts?
- What are the backgrounds, specializations and skillsets of the company's development and engineering team? (LinkedIn is a useful resource in this regard.)
- For what percentage of the total employee base do development and engineering account?

PEOPLE AND SERVICE DELIVERY

- From where does the company provide the service?
- Does the company have different levels of analysts?
- Does the company have specific response personnel?
- Does the company have dedicated threat intelligence analysts and researchers?
- For what positions has the company hired in the past?
- For what positions is the company currently hiring?
- Where are the new positions based?

DEMONSTRATION OF DELIVERY AND REVIEWS

- What do employees say about the company? (Glassdoor is a useful resource in this regard.)
- What do peer review sites such as Gartner Peer Insights, SpiceWorks, G2, etc. reveal about the company?
- What do searches on subreddits reveal for experiences working with or at the company?
- Does the company have case studies?
- Is the company clear about what they do and how they will deliver?
- Does the company have customer references and statements attesting to delivery?
- What are the company's client satisfaction scores, NPS and retention rates?

TECHNICAL CRITERIA: VISIBILITY, FIDELITY, DETECTION, RESPONSE

Beyond subjective organizational factors, it is important to define objective technical criteria against which any MDR provider can be measured.

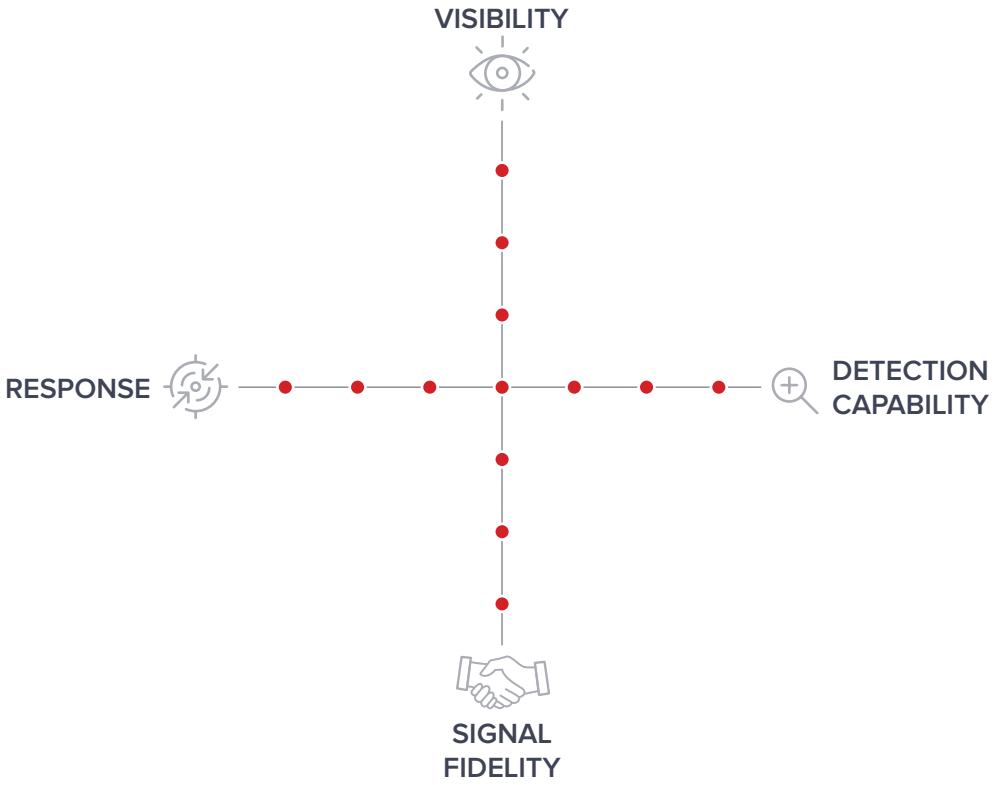
To create a framework for assessing and comparing MDR providers, we will use four criteria:

- Visibility
- Detection Capabilities
- Signal Fidelity
- Response

These criteria correspond to the primary purpose of MDR: minimizing threat actor dwell time.

Using radar diagrams, these criteria are combined into an informative summary that captures the capabilities of each MDR segment.

This radar chart combines the four technical criteria.



VISIBILITY

From applications to infrastructure, organizations are operating on-premises, in the cloud or in both. What was once a clearly defined defensive perimeter is now a shifting blend of mobile users and cloud workloads. As a result, visibility into the digital network is more critical than ever before.

There are many ways visibility can be obtained. MDR providers typically rely on telemetry from:

- Endpoints: process and event data
- Networks: NetFlow, metadata records, full packet captures (e.g., PCAP)
- Log Data: login events, detection events, etc.
- Cloud: data outside of logs, endpoints and vulnerability data, for instance from cloud access security brokers (CASB) or cloud workload records
- Vulnerability Data: exposed common vulnerabilities and exposures, ports, etc.

In the context of the cyber kill chain[8], each telemetry source has core competencies, visibility and efficacy across the attack surface.

Visibility	LOG	NETWORK	ENDPOINT	Cloud (Outside of Log)	Vulnerability
Core competency	Breadth	Things in motion	Process visibility	Variable	Vulnerability visibility
External Recon	✓ (Depends on configuration)	✓ ○○○○		✓ (Depends on configuration)	✓ ●●●●●
Weaponization					
Delivery	✓ (Depends on configuration)	✓ ●●●○○	✓ ●●●●●	✓ (Depends on configuration)	
Exploitation	✓ (Depends on configuration)	✓ ●●●○○	✓ ●●●●●	✓ (Depends on configuration)	
Installation	✓ (Depends on configuration)		✓ ●●●●●	✓ (Depends on configuration)	
Internal Recon	✓ (Depends on configuration)			✓ (Depends on configuration)	✓ ●●●●●
Command and Control	✓ (Depends on configuration)	✓ ●●●●●		✓ (Depends on configuration)	
Data Collection	✓ (Depends on configuration)			✓ (Depends on configuration)	
Exfiltration	✓ (Depends on configuration)	✓ ●●●○○		✓ (Depends on configuration)	

[8]The kill chain was originally used as a military concept related to the structure of an attack; breaking or disrupting an opponent's kill chain is a method of defense. Recently, the concept has been applied to cybersecurity.

VISIBILITY

At a superficial glance, it appears that log and cloud data provide the greatest coverage; however, as we will see when we explore signal fidelity, this appearance is deceiving.

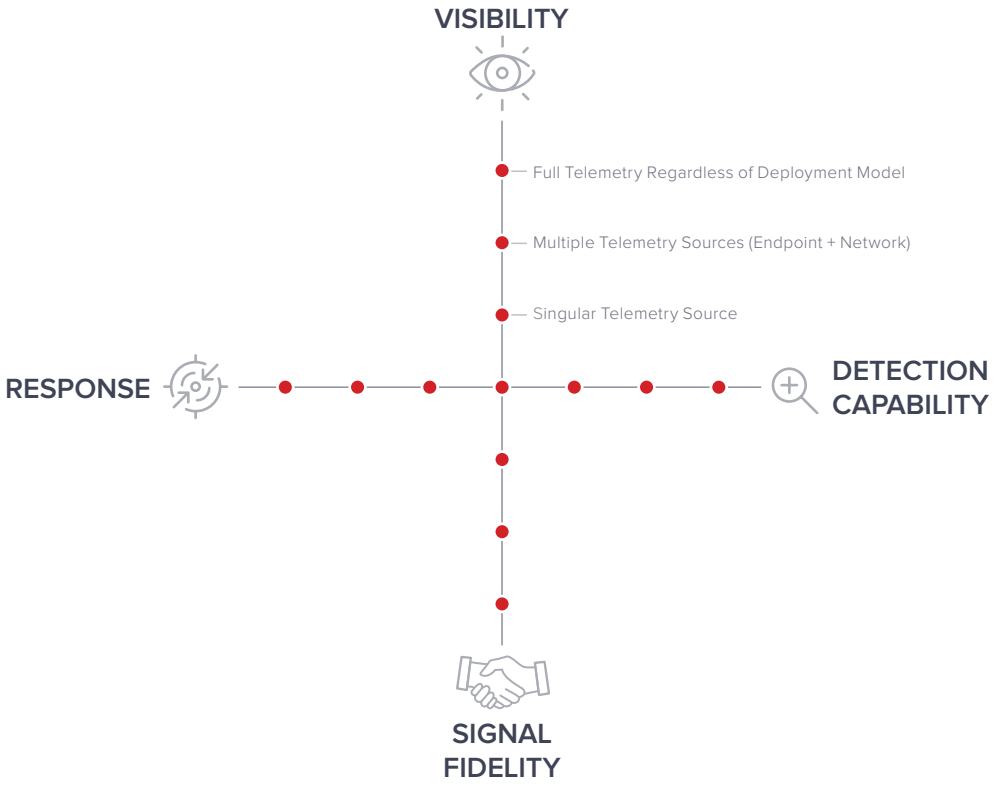
Moreover, since attack surfaces vary widely, it's important for organizations to keenly consider their particular attack surface when evaluating potential MDR providers' capabilities with respect to visibility.

For example, distributed environments require visibility into cloud, Internet of Things (IoT) devices, industrial IoT (IIoT) devices and industry-specific services (e.g., eDiscovery, patient records, trading terminals, etc.). And, all of these environments and devices are potential attack vectors from which signals must be drawn. In addition, visibility into the full attack surface is required is to reduce dwell times by monitoring all the places a threat actor might be hiding as blind spots serve as beachheads for attacks.

In addition, organizations should take into account their own or their service providers' ability to correlate data with telemetry that is out of the service scope. Admittedly, this consideration is typically a balancing act between in-house resources and cost; however, correlation and corroboration will nonetheless be required at some point for forensic investigation, confirmation of attacker presence, reduction of false positives and root cause discovery.

In reference to the radar chart, we can now populate the first axis, Visibility. While many variations can exist, to keep things simple the range of options are condensed into three points that capture the majority of MDR providers.

These three points capture the capabilities of the majority of MDR providers.



SINGLE TELEMETRY: Typically endpoint or log only (logs are limited if the source doesn't alert, no news is potentially a false indicator)

MULTIPLE TELEMETRY: Typically endpoint and log or network, but missing visibility to some degree across the entirety of the network

FULL TELEMETRY: Visibility across endpoint, log, network, cloud, vulnerability regardless of deployment model

VISIBILITY

QUESTIONS AND CONSIDERATIONS:

When examining the visibility capabilities of potential MDR vendors, organizations should ask:

- What does our environment look like today, and what will it look like in the future?
- What technologies will give us appropriate visibility in the context of our unique threat landscape?
- What additional resources (e.g., people, process, technology) do we require to take action on informed decisions?
- Does the data integrate with our systems, thereby making it possible or easier for investigation and forensic investigation?
- What industry-specific tools do we use that we must secure?
- Do the technologies also give us the ability to swiftly contain and respond to threats?
- What are the potential implications for regulatory requirements?
- Does the level of visibility help us meet our acceptable risk tolerance and support our business objectives?

SIGNAL FIDELITY

When law enforcement investigates a crime different evidence provides different information that leads to various degrees of confidence to reach a conclusion, such as:

- DNA provides an in-depth level of evidence that cannot reasonably be refuted
- Eyewitness testimony is much less reliable
- Video surveillance is somewhere in the middle: useful in some circumstances but not without blind spots

The deeper the level of evidence—the fidelity—the more empowered analysts are to detect, hunt and confirm threat actor presence.

Visibility and fidelity are closely, but typically inversely, related. Log data provides broad-level visibility but is limited in depth, whereas full packet captures from the network provide deep fidelity but are limited in breadth of scope. Importantly, each has strengths and weaknesses when applied to the investigative process.

Building upon the previous chart, we see that the depth to which different telemetry sources provide information varies.

Visibility	LOG	NETWORK	ENDPOINT	Cloud (Outside of Log)	Vulnerability
Overall depth of visibility	Low	High	High	High	Low
Core competency	Breadth	Things in motion	Process visibility	Variable	Vulnerability visibility
External Recon	✓ (Depends on configuration)	✓ ●○○○○		✓ (Depends on configuration)	✓ ●●●●●
Weaponization					
Delivery	✓ (Depends on configuration)	✓ ●●●○○	✓ ●●●●●	✓ (Depends on configuration)	
Exploitation	✓ (Depends on configuration)	✓ ●●●○○	✓ ●●●●●	✓ (Depends on configuration)	
Installation	✓ (Depends on configuration)		✓ ●●●●●	✓ (Depends on configuration)	
Internal Recon	✓ (Depends on configuration)			✓ (Depends on configuration)	✓ ●●●●●
Command and Control	✓ (Depends on configuration)	✓ ●●●●●		✓ (Depends on configuration)	
Data Collection	✓ (Depends on configuration)			✓ (Depends on configuration)	
Exfiltration	✓ (Depends on configuration)	✓ ●●●○○		✓ (Depends on configuration)	

SIGNAL FIDELITY

When analyzing potential MDR providers, organizations should concurrently consider both the visibility they provide and the depth of that visibility. For instance, stepping once again through different telemetry sources:

- Network: NetFlow or PCAP? Or both?
- Log: What APIs are available?
- Cloud: What data is being pulled besides logs? How is the data obtained (e.g., asset and service discovery, access management, data exfiltration, policy violations, etc.)?
- Vulnerability: What are the scope and limitations across cloud, mobile, IT, IoT, IIoT?
- Endpoint: What level of data is being pulled? Is it down to the process and binary level?

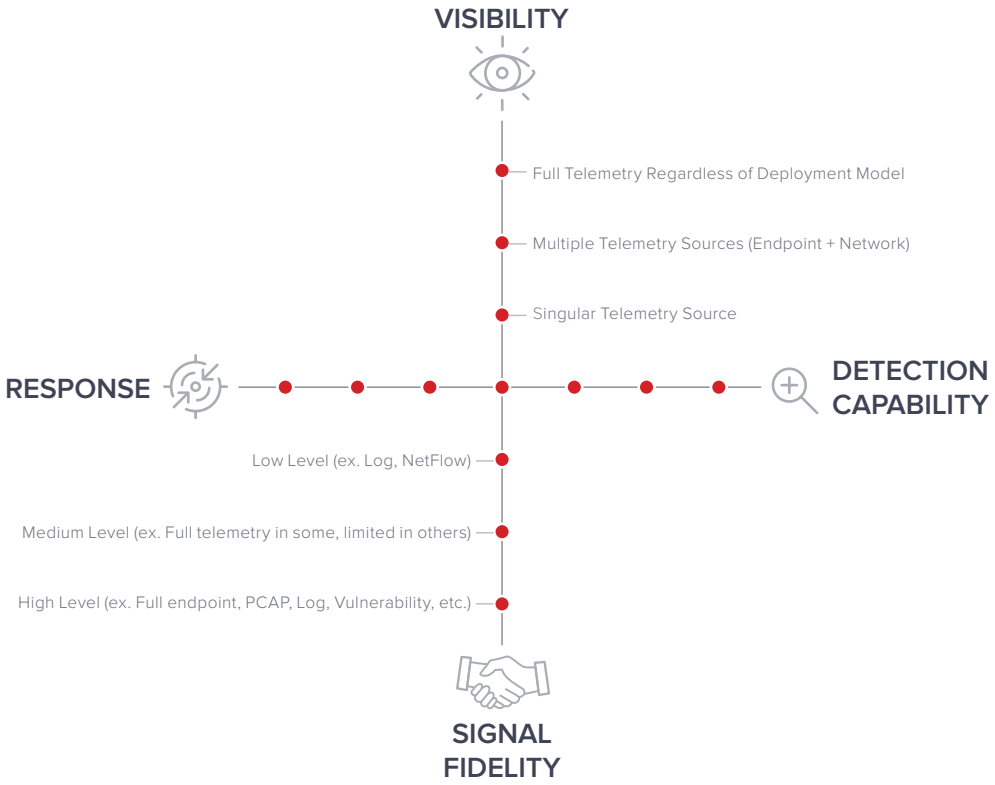
In reference to the radar chart, we now have the second axis. To keep things simplified, three points represent the majority of MDR providers that can be plotted:

LOW LEVEL: Collection of high level data only, including NetFlow or logs

MEDIUM LEVEL: Deep information from some sources (e.g., process and binary level from endpoint) but limited information from others (e.g., NetFlow only from network or logs)

HIGH LEVEL: Collection of full visibility depth including NetFlow, PCAP, full endpoint, vulnerability, log, etc.

These three points capture the capabilities of the majority of MDR provider.



QUESTIONS AND CONSIDERATIONS:

When examining the signal fidelity capabilities of potential MDR vendors, organizations should ask:

- Given our contextual threat landscape, what level of data is required to complete a thorough investigation of potential threats?
- Does the provider have the appropriate technologies and resources to ingest the data, normalize it and correlate to arrive at informed decisions quickly?
- Do we have the resources in place to make sense of the data from the provider and to action accordingly?

DETECTION CAPABILITIES

Hunting, machine learning, automation, customized threat intelligence, behavioral, known, unknowns, zero-days … thanks to the ingenuity of security researchers and the persistence of attackers, the list of detection capabilities and related threats is endless.

Ultimately, the detection capabilities axis is the hardest to discern between fact and fiction when assessing MDR providers. Examining both the traditional MSSP and the emergent MDR marketplaces reveals an abundance of buzzwords pertaining to the latest technologies and newest threats.

Without a proof of concept over an extended period, organizations vetting potential vendors must ask the right questions and should seek demonstrable proof of delivery.

To continue building the radar framework, a simplified spectrum of detection capabilities, starting from very basic detection and extending to advanced functionality that can detect even unknown threats, must be created.

Whether to detect insiders or malicious actors living off the land, signatures and indicators of compromise (IOCs) have become table stakes. It's the capability to find signals within the noise that separates advanced detection capabilities.

Some providers tout machine learning or automation to enhance the perception of their detection capabilities.

While important in the detection process, these technologies are tools to achieve scale, rather than techniques that provide additional detection capabilities per se. Consider the analogy of trying to drive a nail into an object: a hammer is just as effective as a nail gun, but they differ considerably in scale.

As workloads continue to grow, scale must be achieved, but not without sacrificing quality. Organizations must be careful to appropriately balance machine learning and human intuition.

Algorithms are very efficient at processing large amounts of data, but are no match for the insights of a security researcher; at the same time, researchers rely on advanced tools to help them separate signal from noise.

For MDR providers, scaling with growing volume—without producing false positives or false negatives—is key.[9] Aggregating across hundreds or thousands of clients and multiple technologies, the volume of signals can soar, eclipsing millions—and even billions—per day. Consequently, MDR providers must be able to ingest signals and apply detection and investigative techniques at scale without sacrificing service degradation, which would lead to longer threat actor dwell times.

[9]In the 2019 Ponemon SIEM Productivity Study, organizations on average reported wasting 441 hours a week investigating erroneous alerts from their self-managed SIEM alone

DETECTION CAPABILITIES

The following are criteria and a sampling of questions that should be taken into account when examining potential MDR vendors.

- Known Threat Detection (signatures, IoCs, etc.):
  - From where are the known threats sourced?
  - What rulesets are being used?
  - How is the list of known threats integrated into the detection process?
  - How often is the list of known threats being updated?
- Commodity Threat Intelligence:
  - From where is the threat intelligence sourced?
  - Is the threat intelligence validated?
  - How is the threat intelligence integrated into the detection process?
- Customized Threat Intelligence:
  - How is the vendor collecting and synthesizing this intelligence?
  - How quickly is the intelligence operationalized?
  - How does the intelligence contribute to the detection process?
  - How does the intelligence pertain to your unique threat landscape?
- Active Threat Hunting:
  - What is the provider's definition of active threat hunting?
  - Is the process documented?
  - Are there levels of the threat hunting process?
  - What starts the threat hunting process?
- Proactive Threat Hunting:
  - What is the provider's definition of proactive threat hunting?
  - How often does proactive threat hunting take place?
  - Is the proactive threat hunting driven by hypotheses, known IoCs, analytics, etc.?
  - What data is being correlated?
- Machine Learning:
  - What is the reliance on machine learning?
  - Where does it sit in the process chain?
  - Can the provider demonstrate the machine learning capabilities?
  - What level of information is examined by the machine learning?
  - How does the provider protect against false negatives?
  - What is the delineation between machine learning and human decision?
- Behavioral:
  - What particular threats does the provider's behavioral capabilities look for?
  - Can the provider demonstrate the behavioral capabilities?
  - What level of information does the behavioral capabilities look at?
  - How does the provider protect against false positives?
  - What is the relationship between machine learning and behavioral capabilities?
  - How does the provider correlate the data?

DETECTION CAPABILITIES

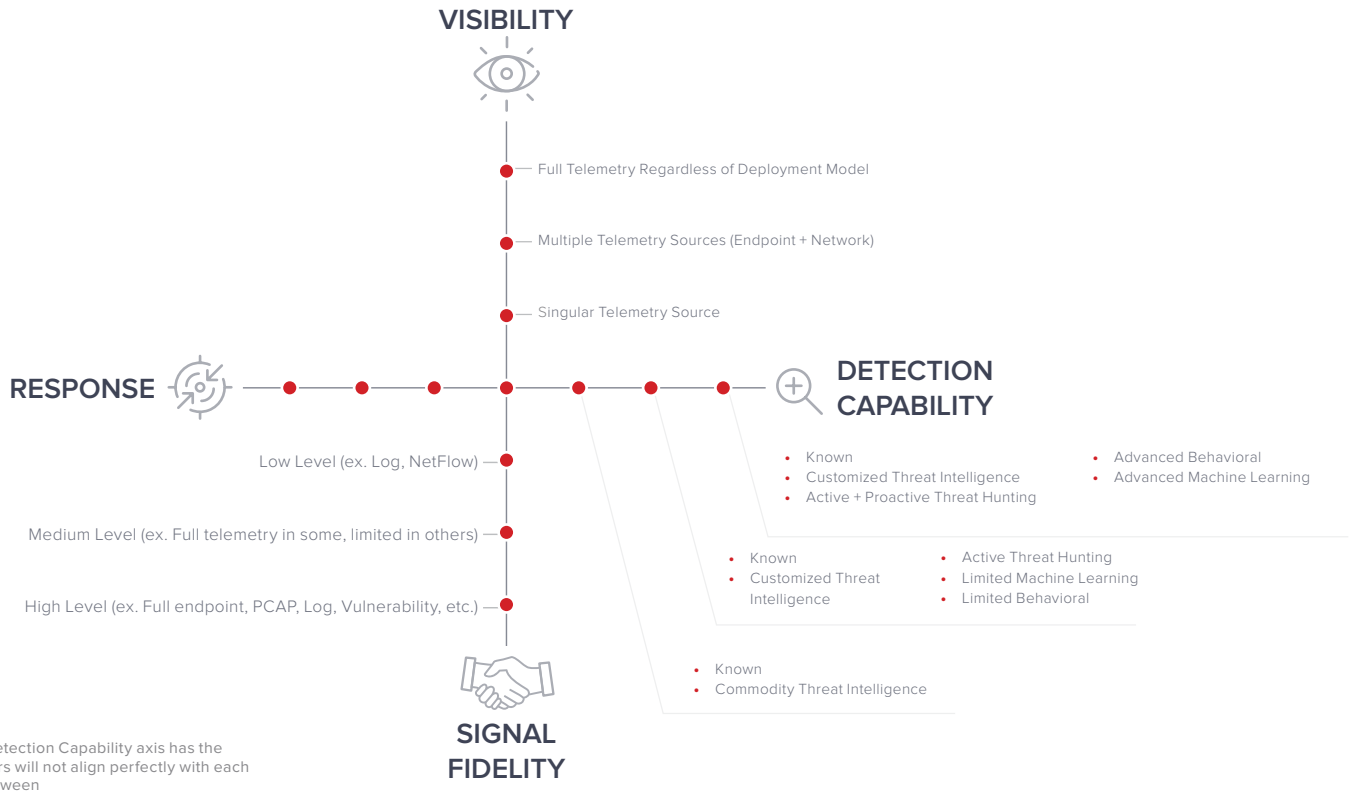
To populate the Detection axis of the radar chart, we will use three points to capture the general capabilities of MDR providers:[10]

LOW: Provides basic levels of detection capabilities using known threat indicators and commodity threat intelligence from subscribed feeds; these types of providers are usually new to the market or are MSSPs that are new to offering MDR.

MEDIUM: Detection capabilities extend into the unknown to a limited degree; machine learning and behavioral detection capabilities are limited but demonstrable for certain scenarios; customized threat intelligence is leveraged to a limited degree; additionally, active threat hunting is documented and exercised to speed time to detection and threat confirmation.

ADVANCED: Detection capabilities cover the entire spectrum of known and unknowns; advanced machine learning and behavioral capabilities extend well beyond known threat detection; integrated hunting teams are both active and proactive in nature, rapidly speeding time to detection using integrated threat intelligence, which is quickly operationalized into detection capabilities.

While the Detection capability axis has the greatest ambiguity, it can still be readily applied to assess the detection qualifications of prospective MDR providers.



[10]Of the four axes in the radar chart, the Detection Capability axis has the greatest ambiguity. As such, MDR providers will not align perfectly with each point but will instead lie somewhere in between

DETECTION CAPABILITIES

QUESTIONS AND CONSIDERATIONS:

When evaluating detection capabilities, organizations should ask:

- What is our unique threat landscape?
- What types of threats present the greatest risk? And does the MDR provider account for these?
- How will known threats be detected and mitigated?
- How will unknown and insider threats be detected and mitigated?
- How do integrated technologies and processes accelerate the time to detect threats?
- What is the provider's standard onboarding and tuning period? Will there be a delay while normalization occurs, leaving us at risk?
- What are the provider's SLAs?
- How will the provider confirm a threat, post-detection?
- What is our tolerance for false positives?
- Have the provider's detection capabilities been validated against real-world scenarios?
- Can the provider show examples, case studies and references?
- What is the delineation of responsibility in the threat hunting and detection process?
- What resources are needed to complement the provider's detection capabilities?
- How will we receive alerts and relevant data about detected threats?

RESPONSE

Put simply, detection is futile without timely response.

The 2019 Ponemon Cost of a Data Breach Study[11] highlights the relationship between containment time frame and total breach cost: each day between breach and containment is calculated to cost an organization, on average, $15,433 USD. The calculated cost of the average 2019 breach, which was reported to last 279 days, is $4.56 million USD.

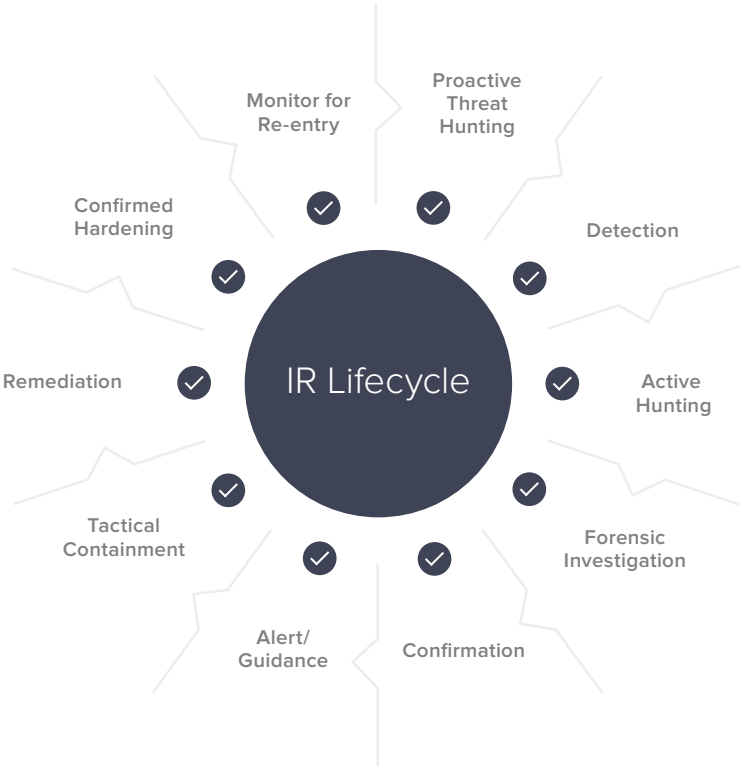
Obviously, there is enormous value in achieving rapid containment.

While the consequences of a data breach are irrefutable, the definition of the "Response" in MDR remains—perhaps ironically—unclear. To understand why, one must recognize that the very evolution of MDR was predicated on two fundamental principles:

1. Detecting what prevention misses
2. Minimizing threat actor dwell time

Unfortunately, "response" is an ambiguous word in the MDR marketspace. Used loosely, it can mean anything from non-vetted alert forwarding to full Incident Response Lifecycle (IR Lifecycle) coverage, which is an enormous range.

To define the criteria by which the response capabilities of all MDR vendors can be objectively assessed, begin by looking at the components within the Incident Response Lifecycle which correlate to threat actor dwell time.

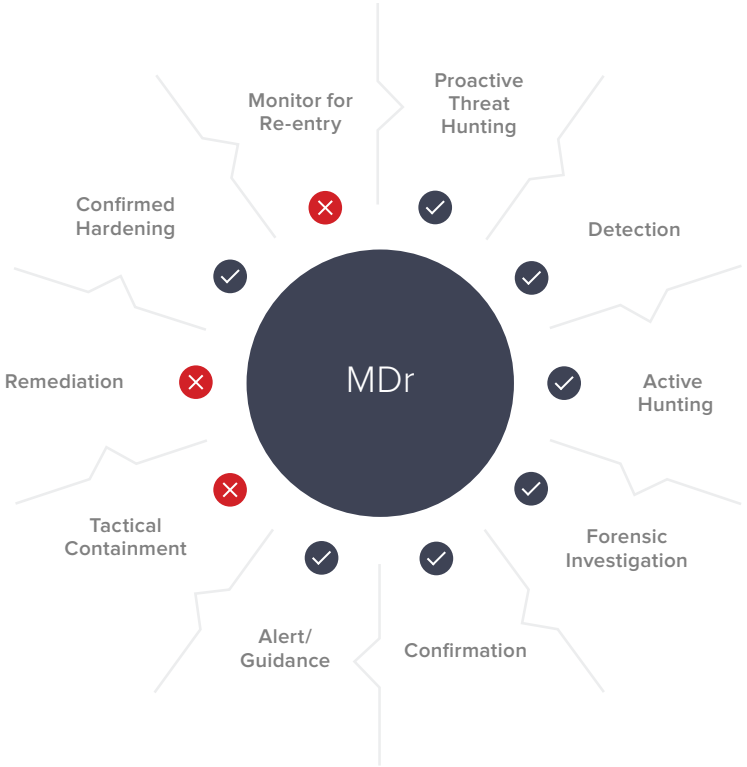


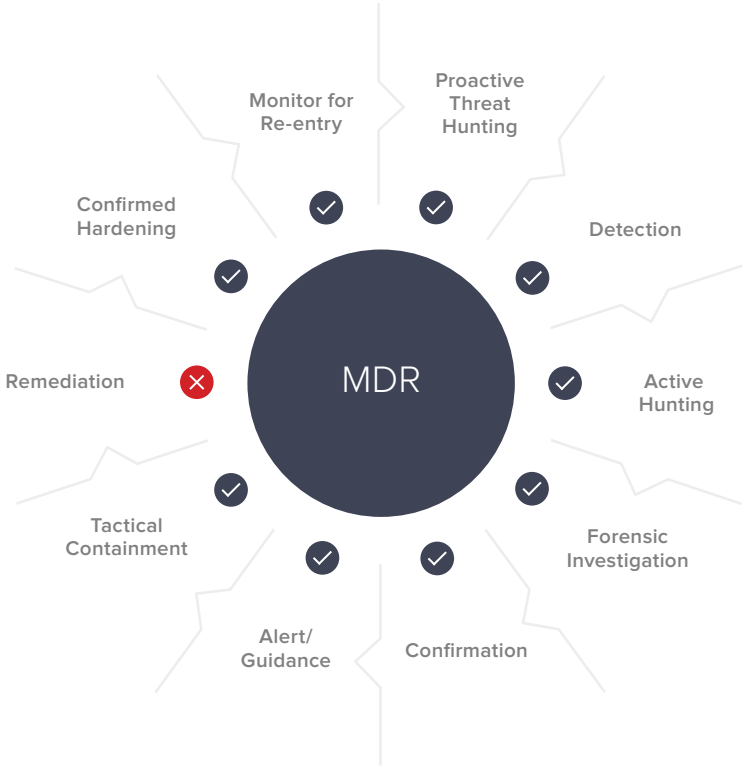
Each component requires people, process and technology. However, the delineation of those three pieces is where MDR vendors differ drastically. Broadly, we can distinguish between two categories of MDR providers:

- MD-big-R (MDR)
- MD-little-r (MDr)

Fundamentally, the difference between MDR and MDr is who holds direct responsibility for containment and remediation support. To be clear: neither approach is inherently right or wrong. Organizations must decide based upon the provider SLAs for alert and guidance if they have the appropriate internal resources to contain and remediate the threat before an adversary's objectives are obtained.

The fundamental difference between MDr and MDR is who holds direct responsibility for containment and remediation support.





Additionally, some technologies have built-in containment capabilities that allow a provider to perform automated or managed remote containment on a client's behalf. When considering MDR vendors, technologies used for visibility must be considered if it is the MDR provider who is performing containment, rather than an in-house security team.

RESPONSE

We can now update the kill chain diagram to include containment capacity.

For consideration: a holistic view of visibility, depth and containment capability.

Visibility	LOG	NETWORK	ENDPOINT	Cloud (Outside of Log)	Vulnerability
Overall depth of visibility	Low ●○○○○	High ●●●●●	High ●●●●●	High ●●●●●	Low ●○○○○
Containment capability	✗ No	✓ Yes	✓ Yes	✓ Yes	✗ No
Core competency	Breadth	Things in motion	Process visibility	Variable	Vulnerability visibility
External Recon	✓ (Depends on configuration)	✓ ●○○○○		✓ (Depends on configuration)	✓ ●●●●●
Weaponization					
Delivery	✓ (Depends on configuration)	✓ ●●●○○	✓ ●●●●●	✓ (Depends on configuration)	
Exploitation	✓ (Depends on configuration)	✓ ●●●○○	✓ ●●●●●	✓ (Depends on configuration)	
Installation	✓ (Depends on configuration)		✓ ●●●●●	✓ (Depends on configuration)	
Internal Recon	✓ (Depends on configuration)			✓ (Depends on configuration)	✓ ●●●●●
Command and Control	✓ (Depends on configuration)	✓ ●●●●●		✓ (Depends on configuration)	
Data Collection	✓ (Depends on configuration)			✓ (Depends on configuration)	
Exfiltration	✓ (Depends on configuration)	✓ ●●●○○		✓ (Depends on configuration)	

RESPONSE

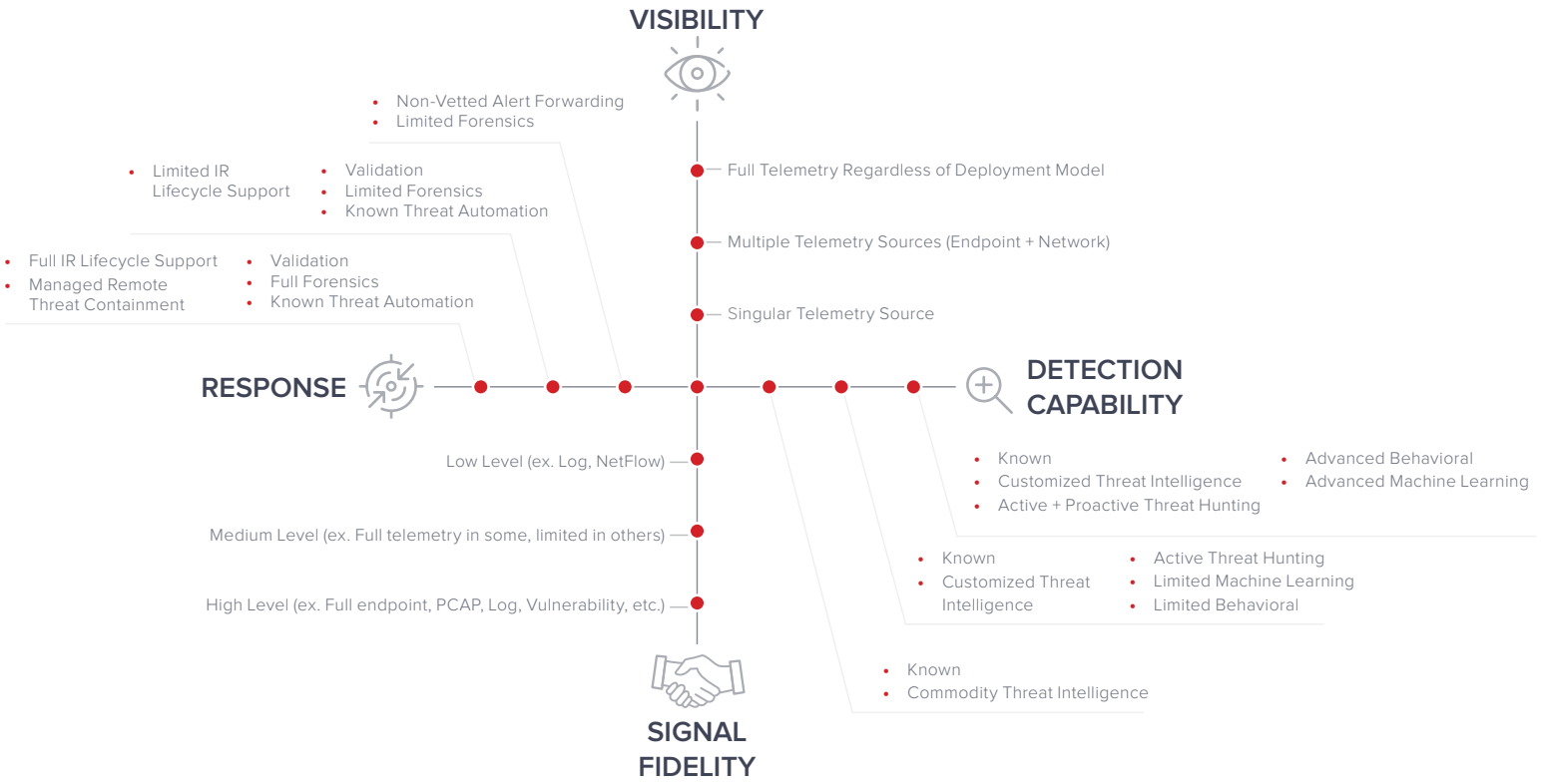
Returning to the radar chart framework, the fourth axis can now be populated. As was the case with the Detection Capability axis, a broad spectrum of capabilities have been concentrated into three points for Response:

TIER 1:
Non-Vetted Alert Forwarding
Limited Forensics

TIER 2:
Threat Validation
Limited Forensics
Known Threat Automation
Limited IR Lifecycle Support

TIER 3:
Threat Validation
Full Forensics
Known Threat Automation
Managed Remote Tactical Containment
Full IR Lifecycle Support

The complete framework by which organizations can objectively evaluate potential MDR providers.



RESPONSE

QUESTIONS AND CONSIDERATIONS:

When evaluating response, organizations should ask:

- What existing internal resources do we have to quickly contain and remediate threats?
- What response timeframe aligns to our acceptable risk tolerance?
- With what parts of the IR Lifecycle do we require assistance?
- Do we trust an outsourced provider to contain on our behalf?
- How will threats be confirmed—and false positives eliminated?
- What are the provider's response SLAs?
- Does the provider work under an incident response retainer model? If so, then what is the delineation between their IR and MDR services?
- What is the general delineation of responsibilities between client and provider?
- Do we, or does the provider, have the appropriate technologies to facilitate rapid containment?
- How will data be received and visualized for active investigation?
- What reporting is available for incidents?
- What runbooks does the vendor have to flag compliance, regulatory, privacy and law enforcement notification?

[11]2019 Ponemon Cost of a Data Breach Study

OTHER CRITERIA TO CONSIDER

The four-axis radar chart provides a framework comparing MDR providers; however, there are additional criteria for consideration that correlate to time to detect, time to respond and subsequent risk mitigation. To ensure a potential MDR vendor is aligned to organizational requirements, the following additional criteria should be validated or considered in the selection process.

TIME OF COVERAGE

Many service providers include 24x7 monitoring as standard in their service delivery model. However, as the MDR market has evolved, so too has customization. Select providers offer 9x5, 12-hour shifts, nights and weekends and other versions of customized coverage. These options are usually intended for organizations that have SOC coverage in place already, but are limited in the hours of coverage due to resource constraints. Organizations are encouraged to carefully read contracts and SLAs to ensure coverage complements existing resources.

SERVICE TIERING

Another component of customization is division of responsibilities among tiering. Threat hunting, IR Lifecycle coverage, forensic investigation and so on are all time- and cost-consuming measures from an MDR provider's perspective. As a result, tiering options have emerged to offer greater choice among required capabilities. Organizations are encouraged to ensure service tiers align to applicable risk acceptance and internal capabilities.

INCIDENT RESPONSE RETAINERS

Many MDR providers offer incident response retainers to accelerate the IR process in the event of an incident. Contractually agreed upon for a standard set of hours and rate, the IR retainer can be enacted when remediation is out of standard delivery scope. Organizations are encouraged to look at SLAs from the following aspects:

- Time from incident detection to boots on the ground (virtual or physical)
- Coverage on weekends, nights, holidays
- Cost when the event exceeds retainer hours
- Quantity of incident responders
- Quality of incident responders

MANAGEMENT

Most MDR providers will manage the devices and technologies included in their service portfolio. However, and as Gartner has acknowledged, a new category provider has emerged, referred to as BYO. This approach provides tremendous flexibility for organizations that already have significant technology investments.

Consequently, to make informed decisions, organizations are encouraged to analyze the ongoing internal resources required to manage devices. Additionally, organizations are also encouraged to consider the loss of situational awareness and detection efficacy if the provider does not retain control to tune the technology to ensure operation in the manner for which it is intended.

[11]2019 Ponemon Cost of a Data Breach Study

PORTAL

Data visualizations are standard with all MDR providers. However, the information within and the timelines of data differ dramatically. From post-incident investigation details to real-time insight into SOC analyst views, data and the value that it provides to organizations must be taken into consideration.

Portals are now available on mobile platforms with integrated response capabilities, which can be enacted with the click of a button. As organizations examine MDR providers, the desired insight and response capabilities (if applicable) should be considered in direct relation to the delineation of responsibilities from provider to client. If the MDR provider does not provide incident life cycle coverage, then organizations are encouraged to choose a provider with deep level visibility and integrated response capabilities to minimize the threat actor dwell time.

PREVENTION

In the case of MDR providers, prevention can be included under an Endpoint Protection Platform (EPP). Many MDR single telemetry providers that are EDR-based include EPP along with endpoint technology. This feature can be a value-add as it provides additional information to SOC analysts in the event of an incident. Additionally, management of the EPP removes operational overhead and consolidates EPP and EDR into a single agent.

SERVICE-LEVEL AGREEMENTS

SLA, SLO, best effort … MDR providers build standards into contracts that outline what they are contractually obligated to abide by or must make best effort to adhere to. In many cases, these SLAs and SLOs align to response times once an incident is detected. Organizations are encouraged to pay particular attention to these timeframes as they have substantial implications for threat actor dwell time, which could mean the difference in breach occurrence.

COMPLIANCE

Virtually all organizations operate under one or many regulatory measures. As compliance is usually a byproduct of sound security, many MDR providers check the box on multiple components. Organizations are encouraged to ask potential MDR candidates for compliance alignment to ensure the service provider meets regulatory standards under audit.

REPORTING

Building on compliance, reporting is a critical component for submission to regulatory bodies. Additionally, reporting provides technical- and executive-level insight into security posture status, improvement and overall value of the MDR provider. Organizations are encouraged to vet an MDR provider's reports to ensure they meet both internal and regulatory requirements.

SERVICE REVIEWS

While not standard across all MDR vendors, monthly, quarterly or yearly service reviews are becoming increasingly common. Cadenced reviews are intended to provide an overview of what has happened during a specific time period and the strength of the organization's cybersecurity from a technical- and executive-level perspective. Organizations are encouraged to look at service reviews from the perspective of value-add from information that is not available via portal or reporting. Presentations should be easy to follow and consumable for both technical and non-technical audiences.

[11]2019 Ponemon Cost of a Data Breach Study

CONTRACTUAL OBLIGATIONS

Organizations are encouraged to carefully dissect a provider's Managed Services Agreement (MSA) in detail. While provider and client must protect vested interests, contracts—and, in particular, the details within them—are key components to understanding the division of responsibilities and the subsequent risk to which an organization could be subjected per the agreement terms. The following are example MSA components that clients should ensure are included and aligned to organizational risk tolerance:

- Authorized persons
- Handling of personal and highly-sensitive information
  - Standard of care
  - Breach of personal information by provider
  - Return or destruction of personal information
- Authorized persons (third-party access)
  - Standard of care
  - Restrictions or disclosure to third-party
  - Breach involving third party
- Compliance with law enforcement
  - Demonstration and documentation of adherence
- Compliance with IT management standards
  - Demonstration and documentation of adherence
- Minimum security safeguards
- Oversight of authorized employees
- Network infrastructure and security diagrams
- Security breach procedures or cooperation in the event of a security breach
- Expense of remediation for a security breach
- Disclosure of breach to third-parties
- Customer audits of facilities and practices
  - Customer questionnaire
- Indemnification which allocates the risk of loss between the parties
  - Cyber insurance inclusion and what is covered and required to demonstrate payout

CYBER INSURANCE

Building on cyber insurance within contractual obligations, organizations are encouraged to review the details and terms of their provider's cyber insurance if they are, in fact, included as part of a provider's indemnification clause.

In a recent Ponemon study,[12] organizations reported that only 16 percent of potential losses to information assets were covered, while 60 percent of potential losses related to property, plant and equipment (PP&E) were covered.

Organizations must recognize the value of information assets versus PP&E. Consequently, organizations must understand if there are restrictions on the types of incidents covered:

- External attacks by cybercriminals
- Malicious or criminal insiders
- Third parties
- System of business process failures
- Human error, mistakes or negligence

[11]2019 Ponemon Cost of a Data Breach Study

OTHER CRITERIA TO CONSIDER

In addition, organizations must understand what is covered under their provider's cyber insurance that could require acquisition of additional cyber insurance to cover resultant gaps.

For instance:

- Forensics and investigative costs
- Replacement of lost or damaged equipment
- Notification costs to data breach victims
- Credit monitoring and identity protection services for victims
- Employee productivity losses
- Communication costs to regulators
- Regulatory penalties and fines
- Legal defense costs
- Third-party reliability
- Revenue losses
- Brand damage

[12]Ponemon Report: 2019 Intangible Assets Financial Statement Impact Comparison Report

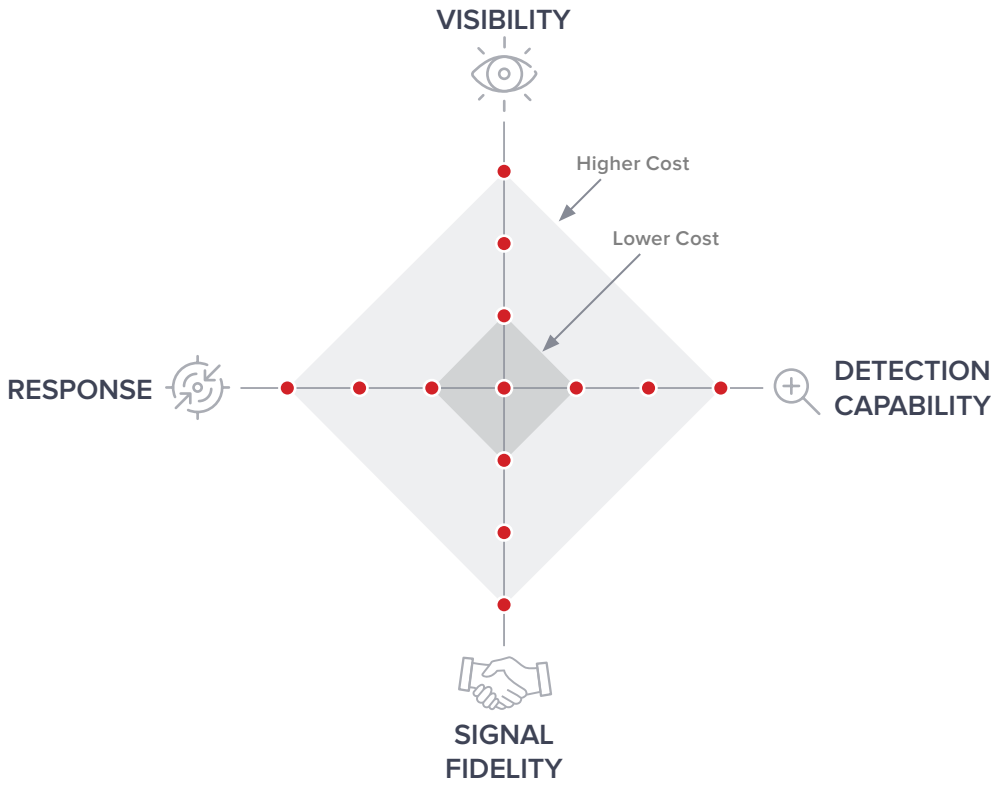
TAKEAWAYS

No MDR provider currently covers the entire spectrum of the four-axis framework, which is intended to set the bar for all MDR providers with continuous adaptation to the threat landscape. The most important thing to remember when looking at MDR providers is to make a selection appropriate in the context of internal capabilities to strike the correct balance between budget and risk acceptance.

At a macro level, MDR providers can be categorized across SOCaaS, MDr and MDR. Subsets of MDr and MDR include single telemetry, multiple telemetry and full telemetry.

It is also important to understand the interconnection between the four axes. For example, limitations in visibility directly impact signal fidelity; consequently, limitations in visibility and fidelity strongly correlate to detection capabilities and, ultimately, integrated response. As mentioned previously, no MDR vendor aligns perfectly to the three points on each axis. Many shades of grey exist, creating a spectrum and interrelated dependencies.

While full visibility, fidelity, detection capabilities and response appear to be the ideal choice as coverage extends outward in the radar chart, cost of the service subsequently increases. This capability and cost relationship typically determines limitations in the coverage organizations can achieve.



TECHNICAL CRITERIA SUMMARY

The seven types of MDR providers can be reasonably evaluated against each of our criteria; the following charts summarize their capabilities across visibility, signal fidelity, detection and response capabilities. Organizations are encouraged to assess internal capabilities, budget and risk tolerance levels when selecting an MDR vendor to ensure proper alignment.

Summarized view of the capabilities of the seven different types of MDR providers across our four technical criteria.

VISIBILITY

	SOCaaS/ Managed SIEM	EDr (Single Telemetry)	MDr (Multiple Telemetry)	MDr (Full Telemetry)	EDR (Single Telemetry)	MDR (Multiple Telemetry)	MDR (Full Telemetry)
Full Telemetry Regardless of Deployment Model				✓			✓
Multiple Telemetry Sources (Endpoint + Network)			✓			✓	
Singular Telemetry Source	✓	✓			✓		

SIGNAL FIDELITY

	SOCaaS/ Managed SIEM	EDr (Single Telemetry)	MDr (Multiple Telemetry)	MDr (Full Telemetry)	EDR (Single Telemetry)	MDR (Multiple Telemetry)	MDR (Full Telemetry)
Low Level (ex. Log, NetFlow)	✓	✓			✓		
Medium Level (ex. Full Telemetry in one or some, limited in others)			✓			✓	
High Level (ex. Full endpoint, PCAP, Log, Vulnerability, etc.)				✓			✓

TECHNICAL CRITERIA SUMMARY

DETECTION CAPABILITY

	SOCaaS/ Managed SIEM	EDr (Single Telemetry)	MDr (Multiple Telemetry)	MDr (Full Telemetry)	EDR (Single Telemetry)	MDR (Multiple Telemetry)	MDR (Full Telemetry)
Known Threats	✓	✓	✓	✓	✓	✓	✓
Commodity Threat Intelligence	✓	✓	✓	✓	✓	✓	✓
Customized Threat Intelligence		Varies	Varies	Varies	Varies	Varies	Varies
Limited Machine Learning	✓	✓	✓		✓	✓	
Limited Behavioural	✓	✓	✓		✓	✓	
Advanced Machine Learning		Varies	Varies	✓	Varies	Varies	✓
Advanced Behavioral		Varies	Varies	✓	Varies	Varies	✓
Active Threat Hunting	Typically No	Varies	Varies	Varies	✓	✓	✓
Proactive Threat Hunting	Typically No	Typically No	Typically No	Typically No	✓	✓	✓

RESPONSE

	SOCaaS/ Managed SIEM	EDr (Single Telemetry)	MDr (Multiple Telemetry)	MDr (Full Telemetry)	EDR (Single Telemetry)	MDR (Multiple Telemetry)	MDR (Full Telemetry)
Non-vetted Alert Forwarding	✓			✓			
Validation	✓	Limited	Stronger	Strongest	Limited	Stronger	Strongest
Known Threat Automation	Possibly	Possibly	Possibly	Possibly	✓	✓	✓
Limited IR Lifecycle Support		✓	✓	✓			
Full IR Lifecycle Support					✓	✓	✓
Full Forensic Capabilities				✓			✓
Endpoint Managed Remote Tactical Containment					✓	Likely	✓
Network Managed Remote Tactical Containment						Possibly	✓

The Seven Categories of MDR

1. SOCaaS/MANAGED SIEM

PROFILE

Security Operations Center as a Service (SOCaaS), also referred to as Managed SIEM, is a category of MDR provider commonly exemplified by MSSPs that are evolving services from alert-driven to more comprehensive coverage across the IR Lifecycle. Capitalizing on the breadth of log visibility, SOCaaS/Managed SIEM providers offer a cost effective option to organizations that are looking to outsource expertise but have limited budgets.

COVERAGE

- Breadth across network signals and technologies (including cloud providers with available APIs)

STRENGTHS

- Use of best-in-class SIEM technology
- Can offer ability to bring your own SIEM
- APIs for log visibility across a wide breadth of signal sources
- Can offer automated known threat response via APIs
- Proven development and use of runbooks
- Established SOCs with global coverage
- Established investigation processes
- Detailed portals and visualizations
- Meets broad level of regulatory requirements
- Lower-cost provider

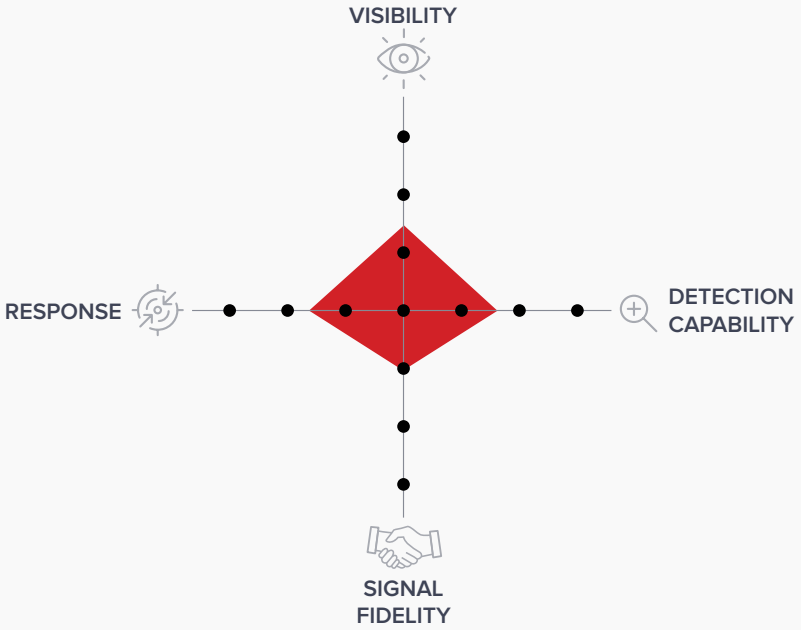
WEAKNESSES

- Newer entrants to MDR market; relatively inexperienced
- Require high client-side resources to complete investigation, correlation and confirmation of threat presence
- Limited visibility beyond logs
- Limited signal fidelity
- Limited forensic and correlation capabilities
- Typically limited threat hunting coverage
- Higher incidence of false positives
- Limited maturity in advanced detection responsibilities
- Limited IR Lifecycle coverage
- Limited scope can lead to longer threat actor dwell time

1. SOCaaS/MANAGED SIEM

24x7 Monitoring	✓
End-to-End Management	Varies—carefully dissect delineation of responsibilities in SIEM management
Endpoint Visibility	✗
Network Visibility (PCAP)	✗
Log Visibility (on-premises and cloud)	✓
Additional Cloud Visibility (beyond log, endpoint and vulnerability)	✗
Vulnerability Management	✗
Automated Known Threat Response	Possibly—depends on APIs
Proactive Threat Hunting	✗
Active Threat Hunting	Possibly—but typically not
Forensic Investigation	Limited
False Positive Reduction	Limited
Managed Remote Host Tactical Threat Containment	Client responsibility
Managed Remote Network Tactical Threat Containment	Client responsibility
Managed Remote Cloud-Based Threat Containment	Client responsibility
Unlimited Remediation Support	Typically requires IR retainer

SOCaaS/Managed SIEM providers offer a cost-effective, but limited-capability, option to organizations that are looking to outsource expertise but have limited budgets.



1. SOCaaS/MANAGED SIEM

QUESTIONS AND CONSIDERATIONS:

- Does log data alone provide appropriate visibility across current and future network infrastructure? What else is required to manage and provision to complete the missing visibility?
- Does log data provide the appropriate depth of data that covers the contextual threat landscape?
- Does the MDR provider have integrated automated response for known threats available via APIs?
- How can data be ingested into existing technologies and processes to facilitate additional client-side investigation?
- Does the provider have adequate detection capabilities that enable detection of known and unknown threats?
- How will threat hunting be conducted? Are additional internal resources required to conduct forensic investigation and confirm threat presence in a timely manner?
- What existing internal resources are required to quickly contain a confirmed threat—including people, process and technology?
- Does the provider manage the platform end-to-end or are there requirements from a client perspective?
- What resources are required to cover components of the IR Lifecycle not covered by the provider?
- What are the provider's SLAs for alerts and remediation? Do they meet our requirements?
- Does the provider have adequate visualizations and reporting to support our internal teams and to meet our regulatory requirements?

2. ED-LITTLE-r (Single Telemetry)

PROFILE

Endpoint Detection Response (EDR) and MDR are used interchangeably by many Managed Endpoint Detection and Response providers. EDR—or in this case ED-little-r (EDr)—is a subset of the MDR market providing expertise focused solely on endpoint.

Providers in this space typically emerged as software vendors that have since added SOCs with deep-level expertise specific to managing and monitoring proprietary technology. As a category, EDr providers offer advanced detection capabilities for endpoint threats; however, the majority of the IR Lifecycle—including containment—is the client's responsibility.

EDr vendors are a viable option for organizations looking for endpoint monitoring and detection and that have in-house resources to correlate data from other signal sources to confirm, triage and contain threats in a timely manner.

COVERAGE

- Process visibility
- East/West (internal/lateral)

STRENGTHS

- Use of best-in-class endpoint technology
- Can offer bring your own endpoint technology model (i.e., BYO)
- Can include endpoint prevention under singular agent, eliminating redundancy
- High level of expertise contextual to endpoint
- Advanced endpoint threat detection capabilities
- Deep-level fidelity into endpoint (e.g., process, binary, etc.)
- Limited false positives
- Integrated remediation recommendations
- Deep-level portal visibility into endpoint
- Can include integrated response capabilities, which can be enacted from the client side within provider's portal
- Lower cost

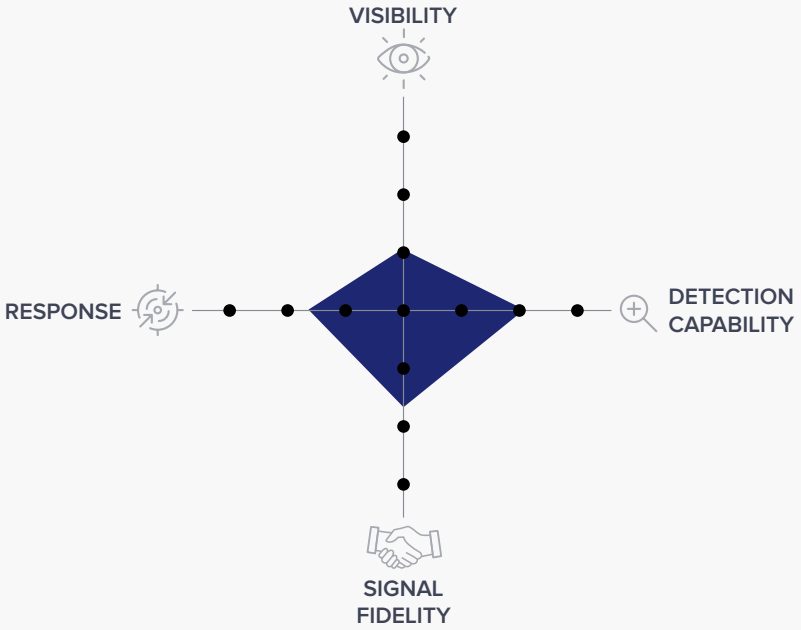
WEAKNESSES

- Commonly represents newer, inexperienced entrants to MDR market
- Unproven SOCs
- Reliance on single security signal
- High client-side resources required to complete investigation, correlation and confirmation of threat presence
- No visibility beyond endpoint
- No signal fidelity outside of endpoint
- Hunting capabilities limited to endpoint only
- Response support limited to endpoint only
- Requires client-side response team for stages outside of IR Lifecycle coverage
- Limited scope can lead to longer threat actor dwell time

2. ED-LITTLE-r (Single Telemetry)

24x7 Monitoring	✓
End-to-End Management	✓
Endpoint Visibility	✓
Network Visibility (PCAP)	✗
Log Visibility (on-premises and cloud)	✗
Additional Cloud Visibility (beyond log, endpoint and vulnerability)	✗
Vulnerability Management	Varies, but limited to endpoint only
Automated Known Threat Response	Typically yes—carefully review contracts and SLAs
Proactive Threat Hunting	Varies—carefully review contracts
Active Threat Hunting	✓
Forensic Investigation	Limited to endpoint telemetry
False Positive Reduction	Limited to endpoint telemetry
Managed Remote Host Tactical Threat Containment	Client responsibility
Managed Remote Network Tactical Threat Containment	Client responsibility
Managed Remote Cloud-Based Threat Containment	Client responsibility
Unlimited Remediation Support	Typically requires IR retainer

EDr vendors are a viable option for organizations that have in-house resources to correlate data from other signal sources to confirm, triage and contain threats in a timely manner.



2. ED-LITTLE-r (Single Telemetry)

QUESTIONS AND CONSIDERATIONS:

- Does endpoint data alone provide appropriate visibility across current and future network infrastructure? What else is required to manage and provision to complete missing visibility?
- Does the endpoint data captured provide the appropriate depth of data to cover our contextual threat landscape?
- Does the provider have integrated automated response for known threats available via APIs?
- How will our team correlate endpoint data with data from technologies across the network? Do we have adequate internal resources to do so?
- How can data be ingested into existing technologies and processes to facilitate additional investigation?
- Does the provider have adequate detection capabilities to enable detection of known and unknown threats?
- Do we have the internal resources required to hunt, to correlate data from the provider with existing data from other technologies, to conduct forensic investigation and to confirm threat presence in a timely manner?
- What existing internal resources do we have to quickly contain a confirmed threat, including people, process and technology?
- Do we have the appropriate resources to cover components of the IR Lifecycle not covered by the provider?
- What are the provider's SLAs for alerts and remediation? Do they meet our requirements?
- Does the provider have adequate visualizations and reporting to support our internal teams and to meet regulatory requirements?

3. MD-LITTLE-r (Multiple Telemetry)

PROFILE

MDr (Multiple Telemetry), or MDr-MT, represents the majority of the MDR market today. Vendors in this space leverage multiple telemetry sources but fall short of full stack visibility across on-premises and cloud environments. Typical combinations seen in the MDr-MT space are:

- Endpoint and log (most common)
- Endpoint and network
- Network and log

Vulnerability visibility and integration into detection and response processes vary from provider to provider, as does cloud visibility beyond cloud-based endpoints and logs. Vendors in the space typically utilize machine learning and behavioral analysis software to process large amounts of data to look for unknown threats.

Coverage of the IR Lifecycle is limited and incident response retainers are typically available for clients in the event of an incident that cannot be handled in-house. MDr-MT is a viable option for organizations that are trying to balance restricted budgets with wider network visibility and that have existing in-house response capabilities.

COVERAGE

Varies, but typically two of the following options (note that cloud visibility outside of endpoints, logs and vulnerability varies by provider):

- Endpoint: process visibility, East/West (internal lateral)
- Network: things in motion, ingress/egress
- Log: breadth across network signals and technologies

STRENGTHS

- Higher level threat expertise than SOCaaS and EDr models
- Historically proven vendors in the MDR marketspace
- Use of best-in-class technologies, typically SIEM plus EDR
- Higher level of visibility compared to SOCaaS and Edr models
- Able to correlate multiple signals to arrive at more informed decisions
- More advanced threat detection capabilities that SOCaaS or EDr models
- Has some degree of integrated machine learning and behavioral processes
- Deep-level fidelity into endpoint
- Improved ability to limit false positives
- Integrated remediation recommendations
- Deep-level portal visibility
- Typically supports multiple regulatory measures

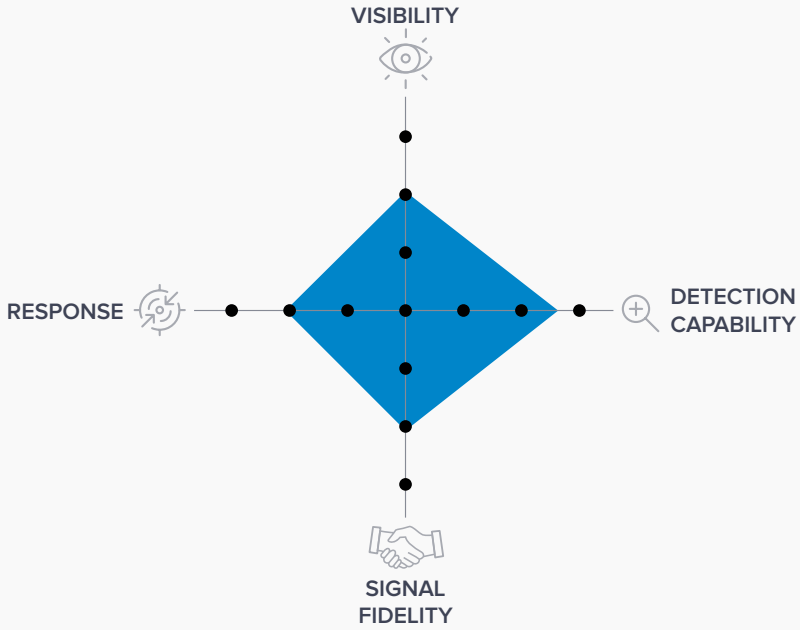
WEAKNESSES

- Higher level service cost compared to EDr and SOCaaS
- Client-side resources required to complete investigation, correlation and confirmation of threat presence
- Client-side resources required for containment and response
- Limited visibility in comparison to MDr (Full Telemetry)
- Limited signal fidelity in certain network components
- Limited inclusion of active and proactive threat hunting
- Limited IR Lifecycle coverage
- Limited scope can lead to longer threat actor dwell time

3. MD-LITTLE-r (Multiple Telemetry)

24x7 Monitoring	✓
End-to-End Management	✓
Endpoint Visibility	Typically 2 of 3 visibility options
Network Visibility (PCAP)	Typically 2 of 3 visibility options
Log Visibility (on-premises and cloud)	Typically 2 of 3 visibility options
Additional Cloud Visibility (beyond log, endpoint and vulnerability)	Varies
Vulnerability Management	Varies—carefully review contracts
Automated Known Threat Response	Varies—carefully review contracts and SLAs
Proactive Threat Hunting	Varies—carefully review contracts
Active Threat Hunting	✓
Forensic Investigation	Limited to visibility
False Positive Reduction	Limited to visibility
Managed Remote Host Tactical Threat Containment	Client responsibility
Managed Remote Network Tactical Threat Containment	Client responsibility
Managed Remote Cloud-Based Threat Containment	Client responsibility
Unlimited Remediation Support	Typically requires IR retainer

MDr-MT is a viable option for organizations that are trying to balance restricted budgets with wider network visibility and that have existing in-house response capabilities.



3. MD-LITTLE-r (Multiple Telemetry)

QUESTIONS AND CONSIDERATIONS:

- Does included visibility appropriately account for our current and future network infrastructure? What else is required that will have to be managed and provisioned?
- Does the level of data captured provide the appropriate depth contextual to our threat landscape?
- Do we have adequate budget for the provider's services and in-house requirements without sacrificing our overall security posture in other critical areas?
- Does the provider have integrated automated response for known threats available via APIs?
- Does the provider have adequate detection capabilities to enable detection of known and unknown threats?
- Do we have the internal resources required to hunt, to correlate data from the provider with existing data from other technologies, to conduct forensic investigation and to confirm threat presence in a timely manner?
- What in-house resources are required to quickly contain a confirmed threat, including people, process and technology?
- Do we have the appropriate resources to cover components of the IR Lifecycle not covered by the provider?
- What are the provider's SLAs for alerts and remediation? Do they meet our requirements?
- Does the provider have adequate visualizations and reporting to support our internal teams and to meet regulatory requirements?

4. MD-LITTLE-r (Full Telemetry)

PROFILE

MDr (Full Telemetry), or MDr-FT, encompasses complete visibility across an organization's potential threat landscape. Whether on-premises, cloud or hybrid, MDr-FT providers have the capability to adapt visibility and detection wherever workloads reside.

Importantly, vendors in this space have complete visibility and typically deliver full fidelity including log, NetFlow, PCAP, endpoint, vulnerability and cloud data outside of logs.

MDr-FT providers are commonly established in the MDR market, with proven advanced detection capabilities supported by machine learning and behavioral processes. MDr-FT has the potential to deliver full coverage; however, the cost can escalate as visibility increases, putting more technologies in play and greater burden on SOC analysts.

MDr-FT is also limited in IR Lifecycle coverage, putting responsibility on the client for timely threat containment. This category is a viable option for organizations looking for complete threat coverage among on-premises and cloud workloads and that have in-house capabilities to complete the IR Lifecycle.

COVERAGE

- Endpoint: process visibility, East/West (internal lateral)
- Network: things in motion, ingress/egress
- Log: breadth across network signals and technologies
- Vulnerability
- Cloud (beyond logs)

STRENGTHS

- High level of expertise across multiple telemetry
- Typically a highly proven MDR vendor
- Use of best-in-class technologies
- Complete visibility across attack surface
- Able to correlate multiple signals
- Integrated advanced threat detection capabilities
- Integrated machine learning and behavioral processes
- Deep-level fidelity
- Limited false positives
- Integrated remediation recommendations
- Deep-level portal visibility
- Supports multiple regulatory measures

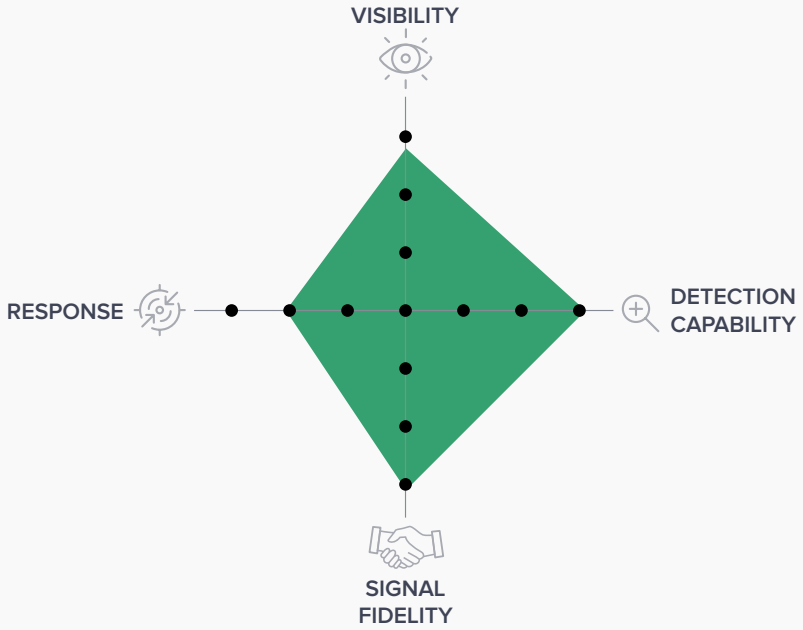
WEAKNESSES

- High client-side resources required for containment and response
- Higher service cost compared to SOCaaS, EDr and MDr-MT models
- Limited IR Lifecycle coverage
- Possibility of longer threat actor dwell time due to client-side requirements

4. MD-LITTLE-r (Full Telemetry)

24x7 Monitoring	✓
End-to-End Management	✓
Endpoint Visibility	✓
Network Visibility (PCAP)	✓
Log Visibility (on-premises and cloud)	✓
Additional Cloud Visibility (beyond log, endpoint and vulnerability)	✓
Vulnerability Management	✓
Automated Known Threat Response	Varies—carefully review contracts and SLAs
Proactive Threat Hunting	✓
Active Threat Hunting	✓
Forensic Investigation	✓
False Positive Reduction	✓
Managed Remote Host Tactical Threat Containment	Client responsibility
Managed Remote Network Tactical Threat Containment	Client responsibility
Managed Remote Cloud-Based Threat Containment	Client responsibility
Unlimited Remediation Support	Typically requires IR retainer

MDr-FT is a viable option for organizations looking for complete threat coverage across all environments and that have in-house capabilities to complete the IR Lifecycle.



4. MD-LITTLE-r (Full Telemetry)

QUESTIONS AND CONSIDERATIONS:

- Do we have adequate budget for the provider's services and in-house requirements without sacrificing our overall security posture in other critical areas?
- Does the provider have integrated automated response for known threats available via APIs?
- Does the provider have adequate detection capabilities to enable detection of known and unknown threats?
- Do we have the internal resources required to hunt, to correlate data from the provider with existing data from other technologies, to conduct forensic investigation and to confirm threat presence in a timely manner?
- What in-house resources are required to quickly contain a confirmed threat, including people, process and technology?
- Do we have the appropriate resources to cover components of the IR Lifecycle not covered by the provider?
- What are the provider's SLAs for alerts and remediation? Do they meet our requirements?
- Does the provider have adequate visualizations and reporting to support our internal teams and to meet regulatory requirements?

5. ED-BIG-R (Single Telemetry)

PROFILE

Similar to EDr, outlined previously, ED-big-R (EDR) is an evolution of a subset of the MDR vendor landscape. Virtually all EDR vendors own, manage, monitor and respond to their own proprietary end-point software. Deep machine learning and behavioral processes are highly integrated, thereby facilitating threat hunting and rapid response to elusive endpoint threats.

Management, monitoring, hunting and containment capabilities were developed secondary as value-adds for clients who lack adequate in-house resources.

Many EDR vendors provide an EPP in addition to EDR, alleviating the need for multiple agents. Additionally, next-generation antivirus data empowers threat hunters with data that can expedite investigation and response by providing important additional context.

EDR vendors are a viable option for organizations that lack the resources specifically to monitor, investigate and respond to endpoint threats, but have in-house resources to correlate endpoint data from the MDR vendor with network, log, cloud and vulnerability telemetry to detect and respond to threats out of provider scope.

COVERAGE

- Process visibility
- East/West (internal/lateral)

STRENGTHS

- Use of best-in-class endpoint technology
- Can include endpoint prevention under singular agent, eliminating sprawl/redundancy
- Offers value-add for organizations that have already invested in endpoint software
- High level of expertise with endpoint threats
- Advanced endpoint threat detection capabilities
- Deep-level fidelity into endpoint
- Limited false positives
- Full IR Lifecycle coverage
- Deep-level portal visibility into endpoint threats
- Lower cost of service

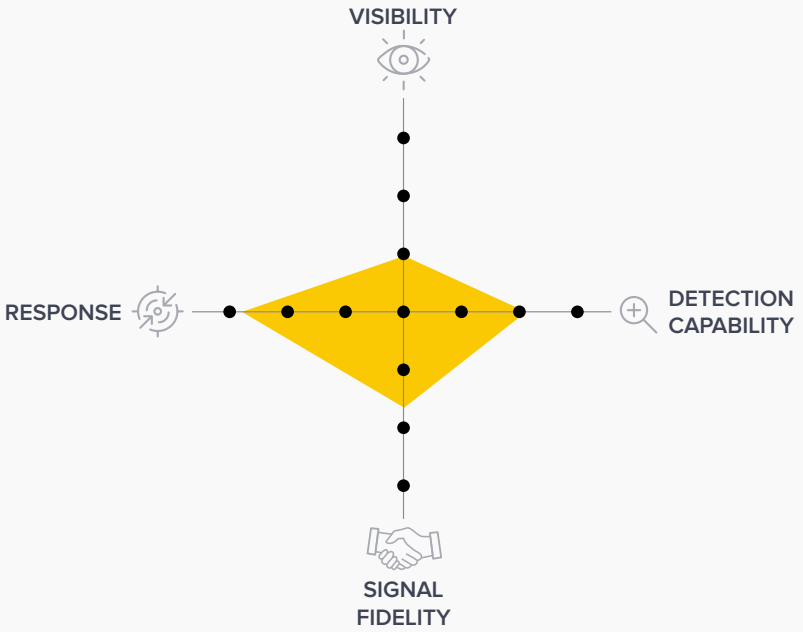
WEAKNESSES

- Newer entrants to MDR market; relatively inexperienced
- Reliance on single security signal
- Unproven SOCs
- Limited visibility beyond endpoint
- Limited signal fidelity outside of endpoint
- No hunting capabilities outside of endpoint telemetry
- Response support limited to endpoint only
- Requires client-side team to hunt, investigate, confirm and respond to threats outside of scope

5. ED-BIG-R (Single Telemetry)

24x7 Monitoring	✓
End-to-End Management	✓
Endpoint Visibility	✓
Network Visibility (PCAP)	✗
Log Visibility (on-premises and cloud)	✗
Additional Cloud Visibility (beyond log, endpoint and vulnerability)	✗
Vulnerability Management	Varies—and limited to endpoint only
Automated Known Threat Response	✓
Proactive Threat Hunting	✓
Active Threat Hunting	✓
Forensic Investigation	Limited to endpoint telemetry
False Positive Reduction	Limited to endpoint telemetry
Managed Remote Host Tactical Threat Containment	✓
Managed Remote Network Tactical Threat Containment	Client responsibility
Managed Remote Cloud-Based Threat Containment	✓ Endpoint only
Unlimited Remediation Support	✓

EDR vendors are a viable option for organizations that lack the resources specifically to monitor, investigate and respond to endpoint threats, but have in-house resources to correlate endpoint data from the MDR vendor with network, log, cloud and vulnerability telemetry to detect and respond to threats out of provider scope.



5. ED-BIG-R (Single Telemetry)

QUESTIONS AND CONSIDERATIONS:

- Does endpoint data alone provide appropriate visibility across our current and future network infrastructure? What else is required to manage and provision to complete missing visibility?
- Does endpoint data captured provide the appropriate depth of data to cover our contextual threat landscape?
- Does the provider have integrated automated response for known threats available via APIs?
- How will our team correlate endpoint data with data from technologies across the network? Do we have adequate internal resources to do so?
- How can data be ingested into existing technologies and processes to facilitate additional investigation?
- Does the provider have adequate detection capabilities to enable detection of known and unknown threats?
- Do we have the internal resources required to hunt, to correlate data from the provider with existing data from other technologies, to conduct forensic investigation and to confirm threat presence in a timely manner?
- What are the provider's SLAs? Do they meet our requirements?
- Does the provider have adequate visualizations and reporting to support our internal teams and to meet regulatory requirements?

6. MD-BIG-R (Multiple Telemetry)

PROFILE

MD-big-R (Multiple Telemetry), or MDR-MT, options are typically built around a log-based and EDR service stack. In some instances, MDR vendors will offer endpoint and network components without log visibility; however, this approach is rare.

In MDR-MT, it's increasingly common to see legacy MSSPs evolve their service offerings to include as their MDR service model an integrated response to EDR. Other services—such as vulnerability management or visibility into cloud services beyond log, endpoint and vulnerabilities—may also be included, but could come at incremental costs.

Fundamentally, the difference between MD-little-r (Multiple Telemetry) and MDR-MT is that the latter includes managed remote threat containment and full IR Lifecycle support.

The EDR component of these solutions typically represents the ability to contain on the client's behalf. However, organizations are encouraged to carefully read SLAs and/or incident response retainers, which can be misrepresented as big-R in this category. Buyers are also encouraged to investigate the level of integration between the services that comprise the Multiple Telemetry MDR solution, as some vendors silo particular services rather than including them within a single MDR platform. MDR (Multiple Telemetry) is a viable option for organizations with higher budgets, lower risk tolerance and limited in-house capabilities to respond to endpoint threats.

COVERAGE

Varies, but typically two of the following options (note that cloud visibility outside of endpoints, logs and vulnerability varies by provider):

- Endpoint: process visibility, East/West (internal lateral)
- Network: things in motion, ingress/egress
- Log: breadth across network signals and technologies

STRENGTHS

- Higher level expertise
- Commonly a proven vendor in the MDR marketspace
- Use of best-in-class technologies, typically SIEM plus EDR
- Greater level of visibility in comparison to EDR
- Able to correlate multiple signals
- Advanced threat detection capabilities
- Integrated machine learning and behavioral processes
- Deep-level fidelity into certain visibility, typically endpoint
- Improved ability to limit false positives
- Full IR Lifecycle support
- Typically has ability to contain threats at endpoint level
- Deep-level portal visibility
- Supports multiple regulatory measures

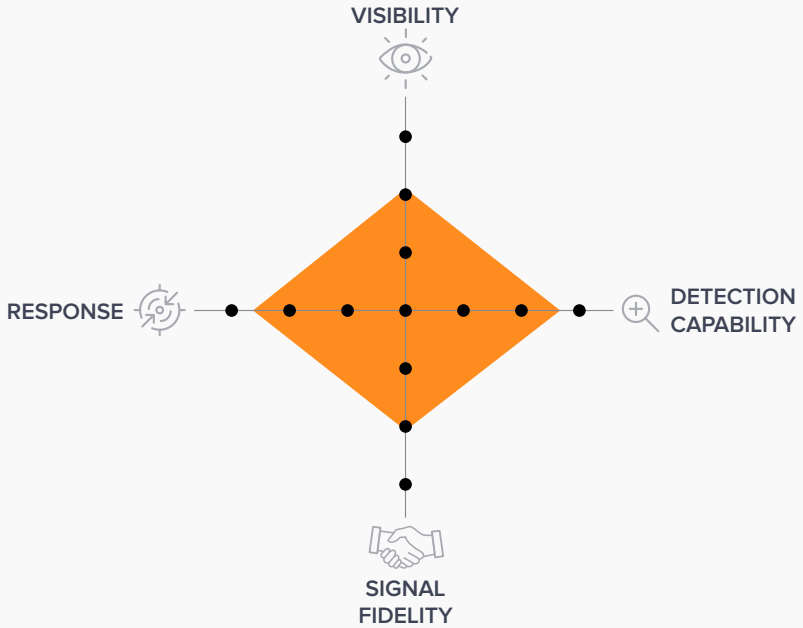
WEAKNESSES

- Higher-level service cost compared to EDR
- Limited visibility in comparison to MDR (Full Telemetry)
- Limited signal fidelity in certain network components
- Incomplete signals required for correlation and forensic investigation
- Hunting limited to in-scope visibility
- Requires client-side team to hunt, investigate, confirm and respond to threats outside of scope
- Limited response capabilities in comparison to MDR (Full Telemetry)

6. MD-BIG-R (Multiple Telemetry)

24x7 Monitoring	✓
End-to-End Management	✓
Endpoint Visibility	Typically 2 of 3 visibility options
Network Visibility (PCAP)	Typically 2 of 3 visibility options
Log Visibility (on-premises and cloud)	Typically 2 of 3 visibility options
Additional Cloud Visibility (beyond log, endpoint and vulnerability)	Varies
Vulnerability Management	Varies—and limited to endpoint only
Automated Known Threat Response	✓
Proactive Threat Hunting	✓
Active Threat Hunting	✓
Forensic Investigation	Limited to visibility
False Positive Reduction	Limited to visibility
Managed Remote Host Tactical Threat Containment	✓ Depends on visibility
Managed Remote Network Tactical Threat Containment	✓ Depends on visibility
Managed Remote Cloud-Based Threat Containment	✓ Depends on visibility
Unlimited Remediation Support	✓

MDR (Multiple Telemetry) is a viable option for organizations with higher budgets, lower risk tolerance and limited in-house capabilities to respond to endpoint threats.



6. MD-BIG-R (Multiple Telemetry)

QUESTIONS AND CONSIDERATIONS:

- Does included visibility appropriately account for our current and future network infrastructure? What else is required that will have to be managed and provisioned?
- Does the level of data captured provide the appropriate depth to cover our threat landscape?
- Do we have adequate budget for the provider's services and in-house requirements without sacrificing our overall security posture in other critical areas?
- Does the provider have integrated automated response for known threats available via APIs?
- Does the provider have adequate detection capabilities to enable detection of known and unknown threats?
- Do we have the internal resources required to hunt, to correlate data from the provider with existing data from other technologies, to conduct forensic investigation and to confirm threat presence in a timely manner?
- What are the provider's SLAs for response? Do they meet our requirements?
- Does the provider have adequate visualizations and reporting to support our internal teams and to meet regulatory requirements?

7. MD-big-R (Full Telemetry)

PROFILE

MD-big-R (Full Telemetry), or MDR-FT, represents the MDR industry's most complete offerings.

Full visibility across on-premises and cloud environments, coupled with integrated machine learning and behavioral analysis, feeds threat hunters with vital information and facilitates near real-time threat detection and containment. Additionally, SLAs strictly outline potential threat actor dwell time, limiting client-side requirements for IR Lifecycle coverage.

Accordingly, the cost to remove those requirements for in-house capabilities across people, process and technology is typically hefty.

Importantly, organizations looking to outsource to MDR-FT providers must have complete trust in the provider's capability to deliver on SLAs, or else the organization could be put at risk without adequate internal resources to address gaps. MDR-FT is a viable option for organizations that have substantial security budgets and are looking for complete threat and IR Lifecycle coverage among on-premises and cloud workloads.

COVERAGE

- Endpoint: process visibility, East/West (internal lateral)
- Network: things in motion, ingress/egress
- Log: breadth across network signals and technologies
- Vulnerability
- Cloud (beyond logs)

STRENGTHS

- High level of expertise across multiple telemetry
- Highly proven MDR vendor
- Use of best-in-class technologies
- Complete visibility across attack surface
- Ability to correlate multiple signals
- Integrated advanced threat detection capabilities
- Integrated machine learning and behavioral processes
- Deep-level fidelity
- Limited false positives
- Full IR Lifecycle support
- Integrated managed remote threat containment
- Deep-level portal visibility
- Supports multiple regulatory measures

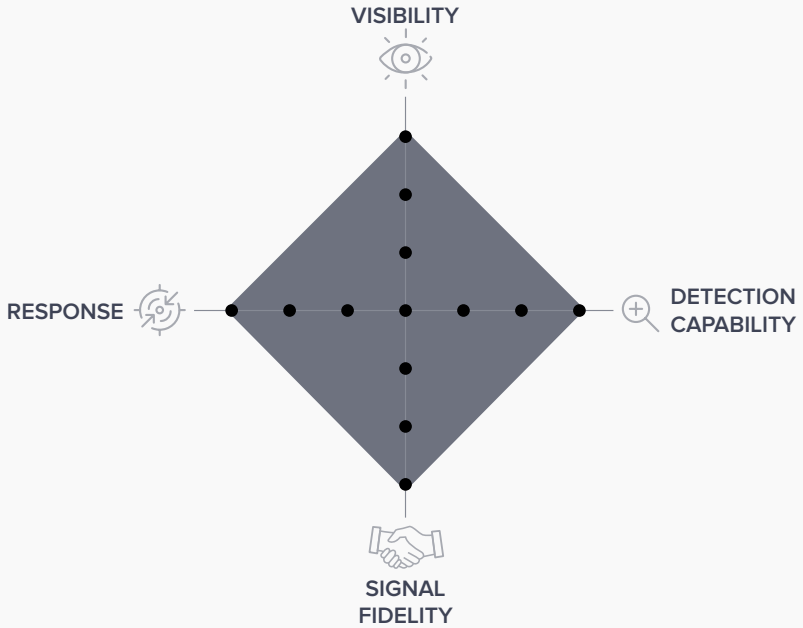
WEAKNESSES

- Higher service cost relative to SOCaaS, EDr and MDr-MT models

7. MD-big-R (Full Telemetry)

24x7 Monitoring	✓
End-to-End Management	✓
Endpoint Visibility	✓
Network Visibility (PCAP)	✓
Log Visibility (on-premises and cloud)	✓
Additional Cloud Visibility (beyond log, endpoint and vulnerability)	✓
Vulnerability Management	✓
Automated Known Threat Response	✓
Proactive Threat Hunting	✓
Active Threat Hunting	✓
Forensic Investigation	✓
False Positive Reduction	✓
Managed Remote Host Tactical Threat Containment	✓
Managed Remote Network Tactical Threat Containment	✓
Managed Remote Cloud-Based Threat Containment	✓
Unlimited Remediation Support	✓

MDR-FT is a viable option for organizations that have substantial security budgets and are looking for complete threat and IR Lifecycle coverage across any environment.



7. MD-big-R (Full Telemetry)

QUESTIONS AND CONSIDERATIONS:

- Do we have adequate budget for the provider's services and in-house requirements without sacrificing our overall security posture in other critical areas?
- Does the provider have integrated automated response for known threats available via APIs?
- Does the provider have adequate detection capabilities to enable detection of known and unknown threats?
- What are the provider's SLAs for response? Do they meet our requirements?
- Does the provider have adequate visualizations and reporting to support our internal teams and meet regulatory requirements?

Summary and Recommendations

As threat actors continue to evolve their techniques and activities in response to workload proliferation across digital landscapes, organizations will continue to be at risk. As a result, MDR vendors will quickly adapt coverage and capabilities in response in an effort to expedite detection and containment regardless of workload residency.

As more MDR vendors enter the market and align to the categories in this guide, personnel involved in risk management and security operations should take care in selecting an MDR provider that:

- Aligns to organizational risk tolerance levels
- Complements internal capabilities across people, process and technology
- Addresses visibility gaps in current and future network activity
- Addresses the organization's threat landscape
- Scales with organizational growth and digital expansion (e.g., cloud, IoT, IIoT, etc.)
- Advances detection of both known and unknown threats
- Accelerates the time frame from detection to containment and remediation
- Meets regulatory, third party and partnership requirements

Ultimately—and in pursuit of appropriate and informed decisions—we encourage organizations to analyze business objectives and to determine subsequent risk to those objectives, which could be due to prolonged threat actor dwell time. Following this methodology will guide organizations down the path to determine which category of MDR vendor effectively and efficiently provides appropriate business protection.

Glossary

dwell time

The amount of time threat actors go undetected in an environment

Endpoint Detection and Response (EDR)

Tools and actions focused on detecting, investigating and responding to suspicious activities (and traces of such) on hosts/endpoints; in this ebook, we distinguish between EDR and EDr based upon who holds direct responsibility for containment and remediation support:

- EDR: containment and support (i.e., response) is largely or entirely the responsibility of the vendor
- EDr: containment and support is largely or entirely the responsibility of the client

endpoint protection

An approach to protecting computer networks which are remotely bridged to client devices by focusing on the hosts and devices themselves, rather than the network; endpoint protection provides crucial defense against threats which can readily bypass traditional antivirus solutions

Endpoint Protection Platform (EPP)

A solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts

Traditional endpoint protection platforms (EPPs) were delivered via a client agent managed by an on-premises server; modern solutions utilize a cloud-native architecture, which shifts management, as well as some of the analysis and detection workload, to the cloud

Incident Response Lifecycle (IR Lifecycle)

An organized approach to addressing and managing the aftermath of a security breach or cyberattack, the goal of which is to standardize an effective process for limiting damage and reducing recovery time and costs

Managed Detection and Response (MDR)

A service which arose from the need for organizations, that often lack sufficient internal resources, to improve their ability to detect and respond to threats—MDR services typically add 24x7 threat monitoring, detection and response capabilities to security operations capabilities via an outcome-oriented approach; in this ebook, we distinguish between MDR and MDr based upon who holds direct responsibility for containment and remediation support:

- MDR: containment and support (i.e., response) is largely or entirely the responsibility of the vendor
- MDr: containment and support is largely or entirely the responsibility of the client

managed security service provider (MSSP)

A company that provides outsourced security services, typically including the remote monitoring or management of IT security functions delivered via shared services, from remote security operations centers

NetFlow

A network protocol, developed by Cisco and extended over the years, for collecting summarized IP traffic information usually for the purpose of monitoring network traffic by system administrators, for handling particular requests and situations

Glossary

Network Detection and Response (NDR)

Tools and actions focused on detecting, investigating and responding to suspicious activities (and traces of such) on computer networks

PCAP

An API for capturing network traffic; the name derives from an abbreviation of "packet capture"

Ponemon

(Dr. Larry Ponemon) The Chairman and Founder of the Ponemon Institute, a research "think tank" dedicated to advancing privacy, data protection and information security practices; publishes security reports that are often colloquially referred to as the "Ponemon Report'

runbook

A compilation of procedures and operations, typically carried out by system administrators, for handling particular requests and situations

Security Operations Center (SOC)

A centralized unit (which may or may not be located in a single "center") that deals with security issues on an organizational and technical level

Security Information and Event Management (SIEM)

An approach to security management that combines security information management (SIM) and security event management (SEM) functions into a single security management system

Security Operations Center as a Service (SOCaaS)

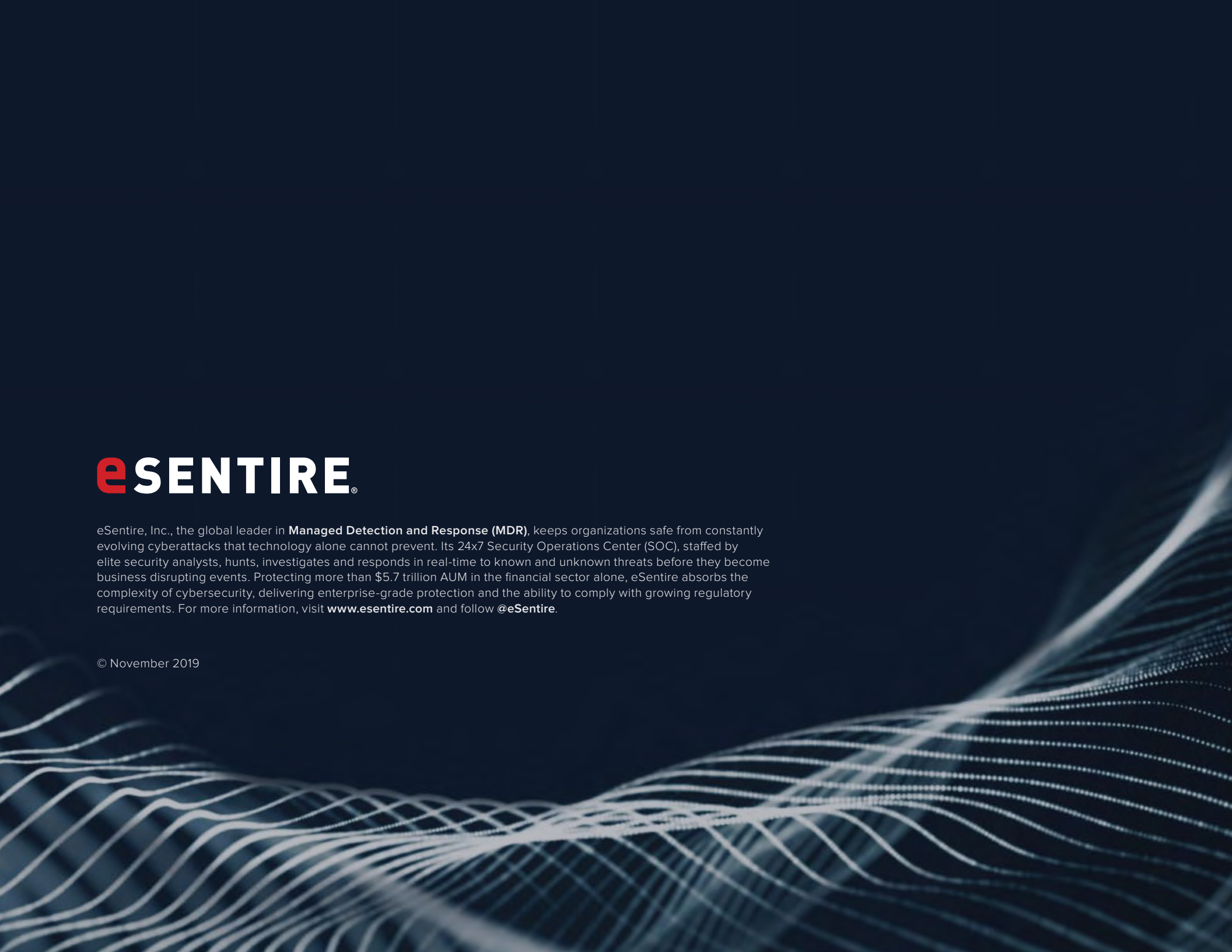
A service that provides real-time monitoring, detection and analysis of cybersecurity threats

telemetry

The collection of measurements or other data and their automatic transmission to receiving equipment for monitoring

threat actor

A person or entity responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity



eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire**.