BUYER'S GUIDE

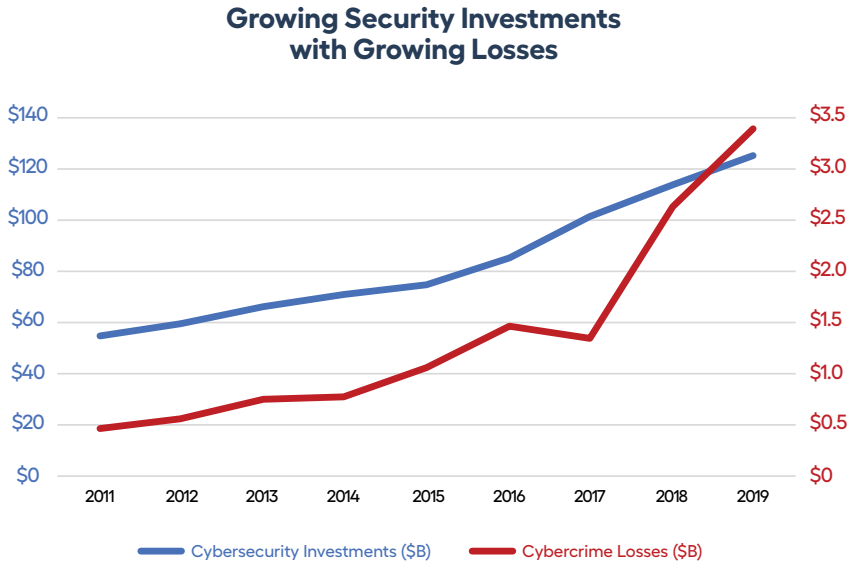
# How to Choose an Effective Managed Detection and Response (MDR) Provider

## Make Outcome-based Security First on Your List

ALERT LOGIC™

Successful breaches, and their resulting damage and repercussions, continue to rise. At the same time, technology and cybersecurity are also evolving, and the threat landscape keeps expanding with new tools and techniques as attackers adapt. Effective detection and response are crucial because no organization will ever be 100% protected against all cyber attacks, no matter how much they invest in security.

Cybersecurity providers offer a variety of point solutions to address specific security concerns. However, the complexity, cost, and staffing necessary to manage it all effectively mean that no matter how good the tools are, this approach typically falls short. Cyber attacks use automation, social engineering, and multi-faceted tactics to bypass security tools and avoid detection, requiring constant vigilance by experts who understand the threats and know what to look for.




Sourced from FBI IC3 Annual Reports

To address these challenges, the security landscape has shifted from a purely tools-based approach to also provide the services necessary to use these tools effectively. The need for more effective protection has driven the rise of managed detection and response (MDR) – a combination of platforms, services, and expertise designed to help quickly identify attacks and take the appropriate action to prevent or mitigate damage. The primary goal of MDR is to reduce the likelihood or impact of successful attacks.

***By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment capabilities."*** [1]

There are many providers attempting to address this market by offering MDR services, but not all MDR is created equally. This MDR buyer's guide will help you and your organization understand what to look for when comparing managed detection and response providers and partner. By examining the functions and capabilities MDR must deliver, this buyer's guide will equip you with the questions to ask before making a go-forward decision.

[1] *Gartner, "Market Guide for Managed Detection and Response Services," Toby Bussa, et al., 26 August 2020*

## 1. Will Successful Attacks Be Reduced?

The first, and most important, aspect to consider when evaluating MDR solutions is how well – or whether – it can reduce the likelihood of a successful attack against your environment. When an attack does occur, you need the technology and expertise to recognize and mitigate the threat to prevent or minimize the potential damage.

The MDR solution must proactively analyze your environment and the threat landscape. Vulnerability scans and configuration audits help to identify and address gaps in your security, while active threat research and intelligence keep you informed of emerging attacks, and how to best recognize and respond to them. MDR needs to enable you to quickly identify suspicious or malicious activity in your environment, so you can take immediate action to limit the access of vulnerable or compromised assets by restricting network access or reducing user roles and privileges.

## 2. Is There Comprehensive Visibility?

It's a simple fact that you cannot effectively protect things you cannot see. If you are unaware of devices connected to your network, or cloud apps being used to store data, you can't ensure they are patched, updated, and protected against unauthorized access or exploits.

Your MDR provider needs to have comprehensive visibility across your complete environment—as well as platforms that you may add to your environment in the future. Visibility of your on-premise network, remote endpoints and mobile devices, and the major cloud providers – AWS (Amazon Web Services), Azure, and GCP (Google Cloud Platform) – is crucial for effective MDR.

Aside from visibility of every platform and asset, it is also essential to have continuous visibility because cyber attacks do not follow "business hours." The MDR provider should have skilled professionals keeping an eye on the environment around the clock. Does the MDR provider offer 24/7 monitoring? Does the provider have multiple / redundant SOCs (security operations centers) for constant vigilance and response?

## 3. How are Research and Threat Intelligence Incorporated?

The threat landscape changes quickly, and attackers are constantly developing new exploits and techniques. It is imperative to have continuous research performed by experienced analysts to augment your security tools and technologies. Understanding the scope and impact of a threat also enables proper prioritization of risk from those threats, based on analysis of current instances of similar attacks in the wild.

When evaluating MDR, ask if the provider conducts its own vulnerability and threat research, and whether it incorporates internal and/or third-party threat intelligence feeds in its analysis of threats. How does the MDR provider get value from the output of threat research, and what is the approach to ensuring threat intelligence is current?

## 4. Are Responses Relevant and Reliable?

Cybersecurity tools are crucial for analyzing activity at scale and filtering through the noise to identify events that require attention. However, tools alone are not enough. Detection must be combined with human intelligence from cybersecurity professionals for credible validation before taking action to respond.

Your environment is complex and dynamic, and the threat landscape is constantly shifting. Tools alone can result in false positives or misguided prioritization of potential threats. MDR needs to include human intelligence to understand the broader context and impact and provide the necessary analysis to determine the appropriate response.

*"Response is a defining element of MDR services."* [2]

The prioritization of, and response to, threats must be unique to your environment. A given attack or exploit may theoretically be "critical," but the potential impact to your network and data must be viewed from the perspective of mitigating factors that reduce or eliminate the threat from the value or impact of the potentially affected systems. How you respond to a given threat may be different from other organizations.

Your MDR solution should offer custom responses specific to your environment, assets, and exposure to risk. The MDR provider needs to enrich security notifications with additional data and context before taking any active steps to mitigate a threat.

Ask the MDR providers you're evaluating: Do you have expert cybersecurity professionals with the right skills and experience to reliably respond to security incidents? Are humans involved in the analysis of security events to reduce false positives? Do security experts play a part in threat prioritization? Is incident response customized for my unique environment and situation?

## 5. Is the Solution Automated and Scalable?

According to NIST, there were over 17,000 common vulnerabilities and exposures (CVEs) reported in 2019. That is an average of 50 new vulnerabilities daily. AV-Test registers more than 350,000 new malicious programs and potentially unwanted applications every day.

MDR must have automated, continuous information gathering to be able to catalog and analyze the overwhelming volume of new threats. It must also include analytics to provide high-quality indications of attack to eliminate dwell time and inform effective response efforts.

Does the MDR provider have cloud-native tools? Is threat detection automated to keep pace with the volume of security events? Can the detection and analysis scale to meet demand?

[2] *Gartner, "Midsize Enterprises Should Embrace MDR Providers," James Browning, Toby Bussa, 27 February 2020*

### 6. What Types of Dashboards and Reporting are Available?

Your MDR solution must, first and foremost, reduce the likelihood or impact of successful attacks. Ultimately though, you also need to effectively report on the state of your cybersecurity posture and demonstrate compliance with industry and regulatory frameworks.

Effective MDR must include reporting that is credible and useful. It must provide the details and information you need for requirements like compliance, governance, and risk reporting – coordinating and correlating information from different systems across your environment, so it can be clearly presented and understood.

Ask the MDR provider: Do you provide dashboards and reporting for a simple, at-a-glance view of your current security posture? Are there separate dashboards for key metrics? Can you drill down in the dashboards and reports to get more context and detail? Are the reports easily accessible and consumable?

## Technology + Experts = Outcomes

As you evaluate MDR solutions and providers, keep in mind that MDR should be easy to deploy and integrate network, log, and endpoint-based detection technologies with continuous threat intelligence and active threat hunting. The MDR provider should offer 24/7 monitoring and support and have dedicated security experts with the capabilities and credentials to deliver the level of protection you require, now and in the future.

Cybersecurity is complex and challenging, but with the right technology and expertise, it is a challenge that can be effectively managed. A true MDR partner will keep constant vigilance on your environment, so you can focus on business outcomes and not security concerns.

To learn more about Alert Logic MDR, visit **alertlogic.com/MDR**