FORTRA™

BUYER'S GUIDE (ALERT LOGIC)

How to Choose the Right Managed Detection and Response Service Provider

Organizations around the world face a constant threat of compromise and disruption from security breaches. An ever-changing threat landscape is fueled by threat actors who develop new or adapt existing threats. Without an effective solution to strengthen your security posture, your organization is at increased risk.

There's a plethora of security service providers and tools that claim they can address your organization's specific security needs. Experience shows that an organization needs more than just the right tools in-house to achieve their desired security outcomes. With the complexity, costs, and staffing needed to ensure the tools are used correctly and having to manage all aspects of your security, this approach often falls short.

To address these challenges, many organizations are partnering with external security service providers who act as an extension of their internal team, providing comprehensive, cost-effective coverage on a 24/7 basis. One of the leading security solutions with proven value and improved security outcomes is managed detection and response (MDR).

> "By 2025, 60% of organizations will be actively using remote threat disruption and containment capabilities delivered directly by MDR providers, up from 30% today."
>
> *2023 Gartner® Market Guide for MDR*

A curated set of technologies, advanced analytics, and security operations experts integrated into a single managed service, MDR's primary goal is to reduce the likelihood and impact of successful cyberattacks. MDR solutions identify and rapidly respond to anomalies and potential breaches — this quick detection of incidents allows MDR to contain, investigate, and remediate issues, ultimately minimizing any potential damage.

As the popularity of MDR solutions increase, so, too, are the number of providers who say their service is MDR. In reality, all MDR solutions are not created equally. This MDR buyer's guide shines a light on what your organization should look for when comparing managed detection and response providers and partner. By examining critical MDR functions and capabilities, this buyer's guide will equip you with the questions to ask before making a go-forward decision.

Will Successful Attacks Be Reduced?

The first, and most important, aspect to consider when evaluating MDR solutions is how effective they are at reducing 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 potential damage.

To be effective, the MDR solution must proactively analyze your environment and threat landscape. Vulnerability scans and configuration audits help to identify and address gaps in your security, while active threat research and intelligence keeps you informed of emerging attacks, and how to best recognize and respond to them. An MDR solution needs to quickly identify suspicious or malicious activity in your environment, so immediate action can be taken.

Is There Comprehensive Visibility?

You cannot protect what you cannot see, that's a simple fact. 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.

An MDR provider needs to have comprehensive visibility across your resources and assets that currently reside within your environment as well as those which are added in the future; it's a continuous detection of change. Visibility must be inclusive of your networks, endpoints, and cloud workloads.

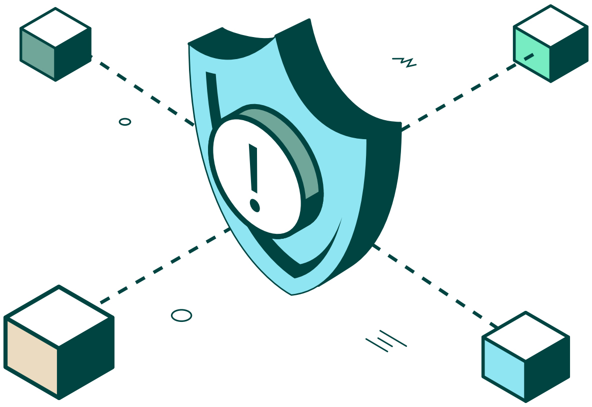
> "MDR services can vastly help organizations to improve their security postures, shield them from threats, and mitigate incidents that occur."
>
> *Bloor MDR Market Update 2023*

Visibility must be continuous as cyberattacks can happen anytime of day. An MDR service must have a team of experts both monitoring and ready to provide actionable insights 24/7. Ensure that the MDR provider has around-the-clock protection from an experienced security operations center (SOC) operating a comprehensive console that facilitates quickly identifying, detecting, and responding to threats.

How Do They Incorporate Research and Threat Intelligence?

The threat landscape changes rapidly as threat actors are constantly developing new exploits and techniques. Without a commitment to proactive threat intelligence performed by expert analysts, your secure posture will not be at the level to effectively protect your organization. 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 an MDR provider, determine if they conduct their own vulnerability and threat research, and whether this research incorporates internal and/or third-party threat intelligence feeds in its analysis. What approach do they take to ensure their threat intelligence is current?



Are Responses Relevant, Prioritized, and Actionable?

Cybersecurity tools are crucial for analyzing activity at scale and filtering through the noise to identify events that require attention. However, tools alone can't provide true security. An effective MDR solution combines tools with human intelligence from a team of experts who provide remediation guidance and insights to proactively protect against threats and improve your overall security posture.

Prioritizing and responding 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 service provider needs to enrich security notifications with additional data and context before taking any active steps to mitigate a threat.

> "Response is a defining element of MDR services." Gartner, Midsize Enterprises Should Embrace MDR Providers
>
> *Gartner, Midsize Enterprises Should Embrace MDR*

Ask the MDR providers you're evaluating if they have expert cybersecurity professionals with the right skills and experience to reliably respond to security incidents. Are people involved in security event analysis to reduce false positives? Is incident response customized for my unique environment and situation?

Is the Solution Automated and Scalable?

According to NIST, there were more than 25,000 identified common vulnerabilities and exposures (CVEs) in 2022. That is an average of 68 new vulnerabilities daily. AV-Test registers more than 450,000 new malicious programs and potentially unwanted applications every day.

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

Effective MDR is a balance between process automation and human interaction to address your evolving security requirements. Look for a provider that allows you to automate actions based on circumstances such as risk tolerance, skillset, and headcount. With both automated and human response, you'll experience improved security posture.

Make sure to ask if the MDR provider has 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? Can you automate at your own pace or is it a set schedule from the provider?

What Types of Dashboards and Reporting are Available?

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

Effective MDR must include credible, useful reporting. You'll need easy access to details and information for compliance, governance, and risk reporting that lets you coordinate and correlate information across your environment so it can be clearly presented and understood.

Find out if the potential MDR solution has dashboards and reporting in an easy-to-understand, at-a-glance view. Are there 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 + Expertise = 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 monitor your environment 24/7 and have dedicated security experts with the capabilities and credentials to deliver the level of protection you require, now and in the future.

Protecting your organization's IT estate is a challenge but with the right people, platform, and processes on your side, it's a challenge that can be effectively managed. The right MDR partner will help you achieve your desired security outcomes with around-the-clock, comprehensive coverage.

Learn more about Fortra's Alert Logic MDR at
alertlogic.com/managed-detection-and-response/

FORTRA™

Fortra.com

About Fortra
Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.