eSENTIRE®

Five Essential Questions to Ask Your MSSP/MDR Vendor

How to find an MDR provider who actually enhances your portfolio and helps you succeed

Introduction

To fill in the gaps in security portfolios and to gain a superior competitive position, many Managed Service Providers (MSPs) are partnering with Managed Detection and Response (MDR) providers.

Adding MDR capabilities presents MSPs with the opportunity to expand their lineup of modern cybersecurity services without needing to incur the added operational complexities of building or extending security operations centers (SOCs) and without cannibalizing existing security offerings.

Buyer beware!

However, not all MDR providers are created equal. Some undoubtedly have a mature partner program and can quickly become a cornerstone of an MSP's growth strategy. Other MDR providers view their channel program as an afterthought that is far down the priority ladder.

Choosing the right MDR provider allows an MSP to unlock valuable new revenue streams, attract new customers and increase retention. Choosing the wrong provider results in an MSP investing time and effort for little or no benefit and plenty of headaches.

The right MDR provider identifies and—crucially—contains breaches as they happen on your customers' behalf; the wrong provider overwhelms your customers with alerts and forces them to interpret the data and attempt to contain threats on their own.

How can you spot the difference and make the right decision?

Finding an MDR provider who actually enhances your MSP portfolio and delivers to expectations often comes down to knowing what questions to ask.

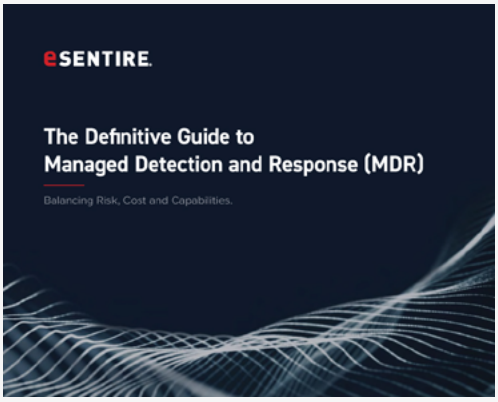
Understanding MDR

Managed Detection and Response means different things to different people, which creates real confusion when you're trying to find the right MDR partner.

Read The Definitive Guide to MDR to learn about:

- The current marketplace definition of MDR
- Technical criteria and detailed questions to evaluate MDR providers
- The strengths and weaknesses for each of the seven categories of MDR

This instructive eBook will help you make more informed cybersecurity choices that align with your business objectives, in-house security resources and risk tolerance levels.



The Five Essential Questions to Ask of MDR Providers

#1 - How much of the threat surface do you cover?

Detecting a known or new threat—and being able to respond effectively—requires coverage of the entire threat surface. Today, that means security solutions must address:

- **Endpoints:** to protect against malware, fileless attacks, zero-day attacks and advanced persistent threats, to recognize suspicious or abnormal activity and to prevent lateral movement
- **Network:** to protect against brute force attacks, service exploits attempts, active intrusions, drive-by attacks, malicious connections and executables, port scans, DoS/DDoS attacks and web application attacks
- **Cloud:** to extend MDR capabilities into the Infrastructure- and Software-as-a-Service (IaaS and SaaS) domains
- **Logs:** to correlate multiple events into a single incident, to map threats to affected resources, to perform ad hoc queries on stored data for forensics and to accelerate investigations and decrease response times
- **Insider Threats:** to protect against advanced persistent threats and malicious insiders

Of course, prospective MDR providers will simply say, "Yes!" when you ask them if they cover they whole threat surface, so be sure to ask for details and make them list—*and actually explain*—their coverage.





	ENDPOINTS	NETWORK	CLOUD	LOGS	INSIDER THREATS
COVERAGE	East/West (internal, lateral)	North/South (ingress/egress)	IaaS and Saas environments	Contextual awareness	Behavioral
FORENSIC CAPTURE	Endpoint telemetry	Packet capture and traffic metadata	Cloud provider logs and real-time telemetry	Multi-month archival	NetFlow, endpoint, DNS, logs

Collectively, these solutions cover the entire threat surface and equip security analysts with critical forensic data to aid in thorough investigation and rapid containment.

#2 - How do you ingest and process data?

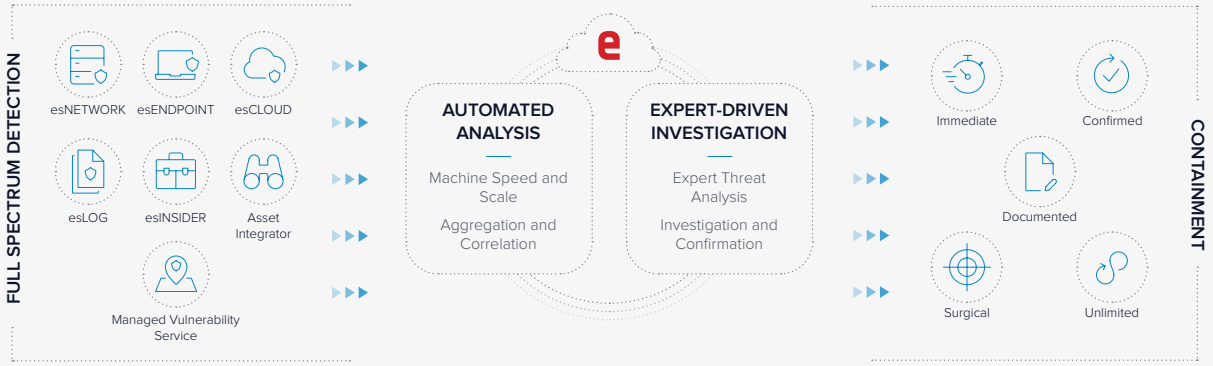
Mitigating risk requires augmented security resources and a swift response. With MDR, the best combination is a cloud-based, machine learning-led platform plus security experts who sift through the noise of thousands of alerts a day to hunt the real threats and disrupt them at wire-speed before they disrupt your customer's business.

When evaluating potential MDR providers be sure to ask exactly how they ingest and process data from their customer base. What processes and technologies are in place? How are they continually improving their capabilities? What metrics monitor operational effectiveness?

Plenty of MSSPs and IT solution providers can deploy and manage security technology (including firewall, IPS/IDS, dual-factor authentication solutions, endpoint protection, and so on)—but modern cybersecurity that can tackle modern, evolving threats is less about operating security technology and more about processing vast sums of data.

Recall the table from the previous page: full spectrum coverage creates a constant stream of forensic data and telemetry from an expansive threat surface. In practice, a mid-market company can easily generate 10,000 alerts per day. Most companies can process—at most—500 to 1,000 alerts per day, but bear in mind that processing "only" 500 alerts per day requires an analyst processing a little faster than one alert per minute for eight hours straight. Most IT teams are neither built nor staffed to perform this function. What about evenings? And weekends? Criminals don't adhere to the boundaries of the traditional workday. Your customers' cybersecurity defenses shouldn't either.

SIEM vendors suggest that seeing thousands of alerts on a single pane of glass is the solution, but this approach does nothing to address the true foundational challenge: how can your customers process a never-ending—and ever-growing—stream of security alerts with a zero-trust approach in mind? There's no point in outsourcing the problem of running the technology if the solution provider can't deal with the Big Data problem of processing the alerts.



Modern cybersecurity requires the ability to efficiently ingest and process enormous volumes of threat signals; the vast majority of MSSPs, private SOCs and self-proclaimed MDR providers simply aren't equipped to do so.

#3 - How do you respond to threats?

A key differentiator among MDR providers is how they define the term “response.” Unfortunately, for most, it essentially means they are processing alerts and only sending “true” or “valid” alerts to your customers. This puts the burden on your customers to then conduct threat hunting, diagnose potential malware and understand how to remediate.

Minimizing threat actor dwell time is of paramount importance, because skilled attackers can cause damage and exfiltrate sensitive data in short order. Consider that:

- Most criminals need only 15-25 hours to breach perimeter defenses, identify valuable data and extract it
- Modern ransomware can spread to a new device every six seconds

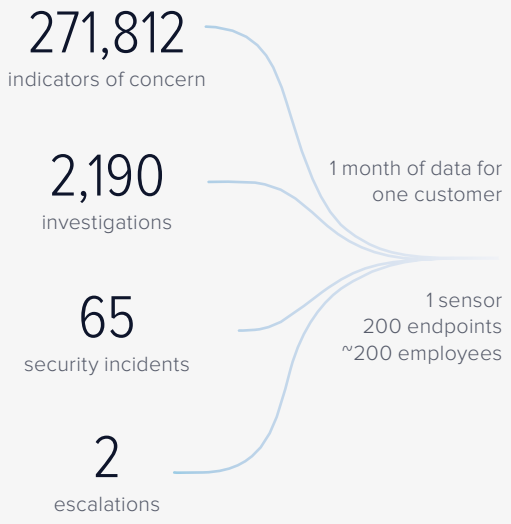
Effective response boils down to:

- Correctly identifying events which require a response, while eliminating false positives and false negatives
- Containing and remediating the threat, quickly and completely

An “MDR” provider who simply flips alerts over to either the MSP or the customer isn’t providing a real response; neither is an “MDR” provider who correctly flags an incident, but then expects the MSP or the customer to handle the actual response component.

MSPs need real MDR partners who will identify events and proceed to contain and remediate them quickly. Of course, being able to do so is very much dependent upon how well-equipped the MDR provider is to ingest and process data, to conduct the necessary investigations and to leap into action.

Asking *“How do you respond to threats?”* before you sign any agreements has the potential to prevent some unwelcome surprises.



eSentire equips world-class SOC analysts with advanced technologies to enable rapid, effective response to cybersecurity threats.

#4 - How do you overcome the cybersecurity skills gap?

Essentially, MDR is a combination of advanced threat detection technologies, extensive processes to monitor and react to the signals generated and recognized by those technologies and—most importantly—expert analysts who decide if and when a response is needed for real attacks against customers.

Many MSSPs and companies who try to build a private Security Operations Center (SOC) capability find out the hard way that operating and scaling an effective SOC requires overcoming a major hurdle: the global cybersecurity skills shortage—estimated by (ISC)[2] to have surpassed four million professionals.

To put this in perspective, staffing a SOC to achieve 24x7x365 coverage requires a minimum of 12 people once you factor in PTO, sick leave and employee churn. And that's simply providing a minimum of one analyst at all times. You can assume roughly 10,000 alerts per day per customer, so you need to ask yourself, "How are they processing all of that data?"

Operating a SOC in this environment and over the long term demands a mature approach to talent recruitment and retention, including:

- **Establishing a talent pipeline** to maintain access to cybersecurity professionals despite the global shortage
- **Taking care of your SOC analysts** to prevent the burnout which is the number one problem cited in surveys of cybersecurity professionals
- **Establishing quality assurance processes** to help analysts grow while also ensuring customers receive the best possible service
- **Investing in tools and technologies** to continually improve operational effectiveness, efficiency and human-machine collaboration in the face of ever-increasing threat signals
- **Providing continuous education and certification support** to help SOC analysts level-up with new skills and credentials
- **Providing career advancement opportunities** whether someone is interested in deep technical growth, a managerial path or exploring other roles within the organization

In normal operating circumstances, these programs ensure your MDR partner can out-recruit and outperform MSSPs and private SOCs. In trying circumstances—including natural disasters and unforeseen events—the operational foundation laid by these programs become vital to maintaining MDR service continuity.

Read this blog to learn more about how eSentire developed and operates effective, resilient and world-class SOCs.

#5 - How good is your partner program?

MSPs and MDR providers partner for mutual benefit—and both parties benefit more when they work together.

With many MDR providers, their partner program is nothing more than a landing page and ungated access to a handful of marketing assets.

Real partner programs—those designed to maximize an MSP's success—consist of much more. When considering different MDR providers, be sure to ask about:

- **A dedicated portal** to serve as a single place to access marketing support, sales resources, deal registration, deal tracking and other partner enablement services
- **A partner enablement team**, complete with contact information, so that there's always someone to turn to for assistance and coordination
- **Partner onboarding** to help you hit the ground running to generate immediate returns
- **Marketing support** to drive lead generation and accelerate deal closings with co-marketing programs, content and advice
- **Revenue incentives and other programs** to help you boost revenue without added OpEx
- **Joint selling** so you can turn prospects into customers with the assistance of your MDR domain experts
- **Deal protection and tracking** from registering opportunities and synchronizing with your MDR partner
- **Partner-exclusive programs and services** to augment your existing security offerings

And finally, the proof—as they say—is in the pudding.

Many MDR providers excel at signing up new customers and MSP partners, but their retention rates tell a story of neglect and a failure to deliver when it matters.

Your prospective MDR partner should be transparent about their customer and partner retention rates, as these figures reveal whether or not the MDR provider lives up to their commitments.

eSentire isn't an MSP that just bolted on MDR. We're the category creator with the depth, breadth and customer trust that comes from nearly 20 years of proven success.

Awarded 5-Star Rating in the 2020 CRN® Partner Program Guide

Boasting a world-class Net Promoter Score of 72

Customer retention is 97%

About eSentire:

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 $6 trillion AUM, 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**.