BUYER'S GUIDE

Managed Detection & Response (MDR)

SAEPIO.CO.UK

SAEPIO
INFORMATION SECURITY

Assured Service Provider

in association with
National Cyber Security Centre

TABLE OF

Contents

WHAT IS

MDR?

Managed Detection and Response (MDR) services are outsourced solutions that monitor, detect, and respond to unusual IT behaviours. They provide 24/7 threat detection, alerting, and incident response, leveraging expert analysts and advanced tools to protect your environment.

The MDR market is growing rapidly, with some reports projecting growth of up to $9.5 billion by 2028. Whilst the use case for these services is compelling this has created a crowded and complex marketplace for organisations to identify suitable partners or their requirements.

WHY DO YOU NEED AN

MDR Service?

The volume and sophistication of cyber-attacks continues to grow. It's not an if, it's when will you have an incident. Therefore, the ability to detect, contain and minimise the impact of adversaries is essential for the ongoing operation of business. MDR addresses the gap between growing cyber threats and limited internal resources. They provide organisations with access to highly skilled and experienced security analysts and coverage that would be costly and impractical to develop internally.

For example. 4.2 FTEs is typically considered to be the minimum head count for a 24x7 shift pattern. This figure is often unrealistic for IT Security teams in small and medium size organisations, and has other implications for broader business operating models. There are also obvious challenges to recruitment and retention of specialist teams.

MDR services are ideal for organisations that:

Lack 24/7 coverage or fast response times.

Struggle with alert fatigue and false positives.

Want centralised visibility across tools.

Need expert escalation support.

Have limited specialist security expertise and experience.

Have multifunctional IT/Security teams.

MDR providers offer access to a Security Operations Centre (SOC) focused on rapidly investigating and neutralising cyber threats across endpoints, networks, cloud, and more, enabling rapid threat hunting and response.

Choosing the right MDR provider is a critical decision. The ideal MDR provider should become a trusted partner, freeing your internal security team to focus on core business functions while providing 24/7 vigilance against cyber threats.

CHOOSING THE RIGHT

MDR Provider

In today's rapidly evolving technological world, choosing the right MDR partner can be a daunting task. This guide is designed to simplify your decision-making process by providing clear insights, essential considerations, and a structured approach to finding the perfect solution for your needs. Whether you're a first-time buyer or reviewing options, understanding the core aspects of Managed Detection and Response is crucial. We'll help you cut through the jargon and focus on what truly matters.

Key Questions to Ask

Before diving into specific solutions, it's vital to clearly define what you need and expect from your Managed Detection and Response Service. Consider the following questions:

- **Purpose:** Do you need 24/7 coverage, advanced skills, or operational resilience?
- **Access & Customisation:** Do you want hands-on use of tools or tailored detection rules or response actions?
- **Budget:** Are you looking for entry-level, mid-range, or premium solutions?
- **Current Setup:** Are you focussed purely on SLAs and outcomes; or do you want to leverage, and drive value from existing technology solutions?
- **Coverage:** Is your environment standardised or complex/diverse?
- **Communication:** How, and with whom do you want to communicate?
- **Scalability:** Do you anticipate your needs changing in the next 1-3 years? Is scalability and/or flexibility important?
- **Response:** What level of action should the provider take during incidents?
- **Must-Haves:** Are there any non-negotiable features?

KEY

Considerations

4

When it comes to MDR, not all providers are created equal. While many MDR services sound similar, the underlying technologies, detection capabilities and operational models can differ significantly, and choosing the wrong provider can lead to blind spots or alert fatigue. Here's what you should be considering:

Technology Stack

- **EDR-Based MDR:** Strong endpoint visibility; limited elsewhere.
- **SIEM-Based MDR:** Broad log ingestion; can be noisy without tuning and lead to slower response times.
- **XDR-Based MDR:** Correlates across endpoints, cloud, email, identity, and network, providing better fidelity, but some are closed systems with integration limitations.

Operational Model

- **True 24/7 Coverage:** Is a true "follow-the-sun" model with a global footprint of Security Operations Centres important; or are remote shift patterns and/or automated responses sufficient.
- **Architecture Alignment:** Ensure compatibility with your cloud and on-prem environment.
- **Integration:** Open XDRs offer flexibility; closed systems may limit tool choice. Its important to understand how MDRs integrate with your current tools/investments, or whether you would need to rip-and-replace aspects of your existing security stack.
- **Telemetry Coverage:** Effective MDR tools need to span the organisation; across endpoints, cloud, identity, email, and network.
- **Customisation:** Ability to define playbooks and tune detections is essential to ensure the MDR is aligned to your infrastructure and reduce noise and false positives.
- **SLAs:** it's important to understand what the guaranteed time for alert, triage, escalation and mitigation is, as these SLAs vary with each provider.

- **Incident Response Retainers:** When scoping for budget for an MDR tool, an incident response retainer should always be included in the cost, to ensure that in the case of an incident, you have support across your entire estate.
- **Shared Responsibility:** Ensure you understand who handles containment, isolation, and root cause analysis. Some MDR providers focus on only alerting, while others will take actions that you have pre-approved.
- **Transparency:** Avoid "black box" providers. Look for shared visibility, ticketing, and investigation logs.

COMPARISON

Criteria

5

To objectively compare different MDR options, use consistent metrics to evaluate providers:

- **Commercials:** What are the pricing metrics? How predictable are the costs? What is they annual purchase cost?
- **Total Cost of Ownership:** What other costs exist? E.g., cloud compute/storage, Integrations, long-term retention.
- **Performance:** How do they perform compared to their SLAs?
- **Customer Service:** How is your contract managed, what communication methods are available, and how do these integrate with existing processes.
- **User Feedback:** What do existing customers say about them?
- **Resilience:** How does the organisation ensure operational continuity and global coverage?
- **Compliance:** Do they have certifications like ISO27001, SOC2? Do you have any data residency requirements they have to meet?

NEXT

Steps

Choosing the right MDR provider is a strategic decision, and Saepio is here to guide you every step of the way. Here's how we help customers move from evaluation to a confident selection:

Step 1. Define your requirements

We work with you to understand your unique environment, challenges and goals, including identifying your key drivers, mapping your current security stack and operational maturity, and clarifying your expectations around response, visibility and integration.

Step 2. Build a shortlist of providers

Using our extensive market knowledge and vendor-neutral approach, we help you narrow down the MDR landscape to a shortlist of providers that align to your needs, highlighting the strengths and trade-offs of each option based on your environment.

Step 3. Use the Saepio MDR Evaluation Matrix

We provide a structured evaluation matrix to allow you to compare providers across technical, operational and commercial dimensions, scoring each solution based off your priorities.

Step 4. Facilitate demos and proof of concepts

We coordinate technical deep dives, demos and proof of concept engagements so you can understand how each solution performs in your environment, and validate detection quality, response workflows and analyst transparency.

Step 5. Procurement and onboarding support

Once a vendor is selected, we assist with contract negotiation and commercial alignment, as well as ensuring onboarding plans are realistic and aligned with your internal timelines.

True resilience comes from clarity, not complexity.

Saepio partners with over 1,000 UK organisations to expose hidden risks, align security with business capacity, and embed solutions that actually deliver.

Our independent experts combine board-level consulting with hands-on technical know-how, giving you the confidence to make sharper risk decisions at the speed of business. From governance and compliance, to best-fit technology integration, we help you cut through the noise and focus on what matters most:

Reducing risk and building lasting resilience.

SAEPIO.CO.UK

SAEPIO
INFORMATION SECURITY

Assured Service Provider

in association with
National Cyber Security Centre