KPMG

# How to select the right Managed Detection and Response vendor for your organization

# Contents

Introduction

What is MDR?

The ultimate checklist for selecting the right MDR vendor for your organization

Questions to ask MDR vendors to help narrow down your search

Conclusion

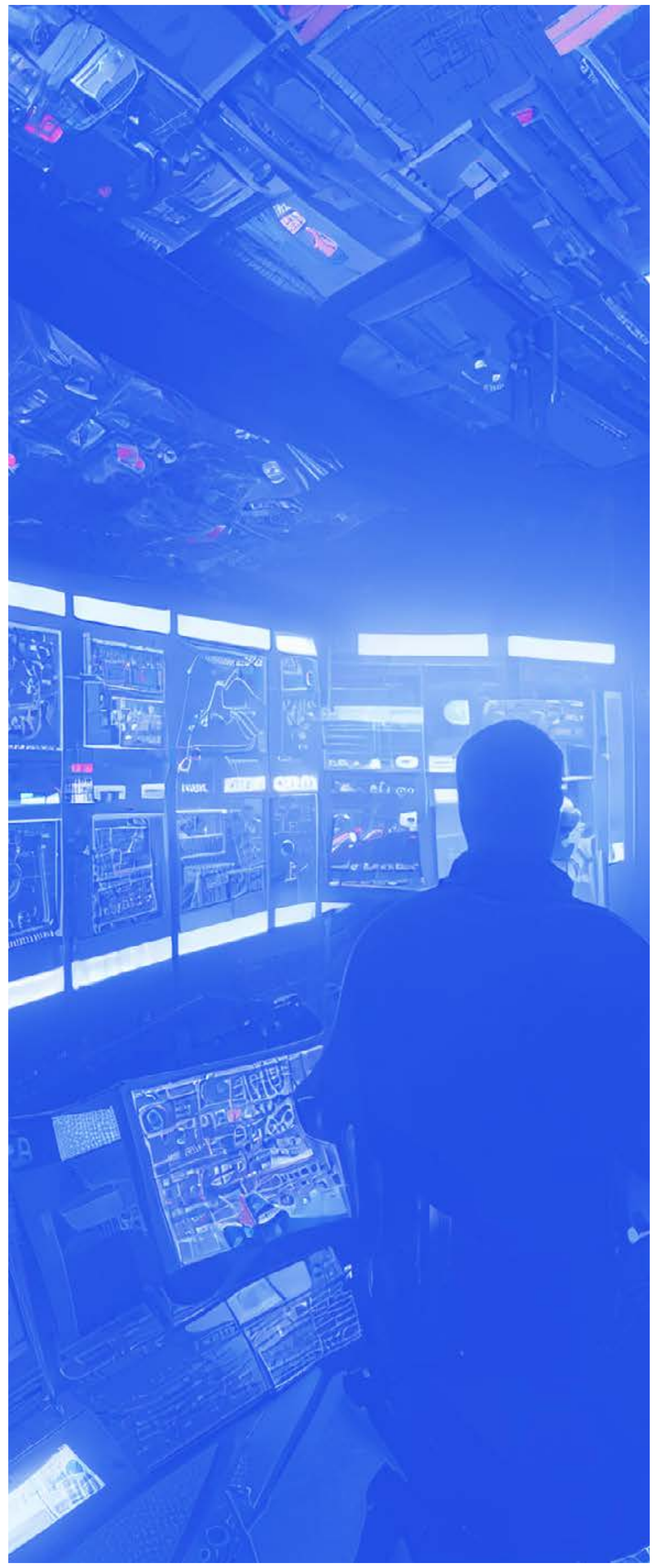
About KPMG in Canada

Contact Us

# Introduction

In today’s technology driven world, your organization faces more challenges than ever before in protecting against cyberattacks. In the aftermath of the global pandemic, an increase in remote work arrangements and the ability for employees to use multiple devices – including personal and work designated ones – has only heightened the risks. All this, while also complying with rapidly changing global regulatory requirements and dealing with skilled talent scarcity, makes the situation that much more complex.

At the same time, modern cyber criminals have become more creative with their attacks than ever. Media stories abound, detailing how high-profile organizations fall victim to cybersecurity incidents that compromise financial information, damage reputations, disrupt online transactions, cause business losses, or shut down operations altogether.



Introduction

What is MDR?

The ultimate checklist for selecting the right MDR vendor for your organization

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

41% of IT leaders reported an increase in cyber security incidents since the pandemic began. [2]

83% of companies say they've suffered at least one cyberattack over the last 12 months. [3]

Reporting a rise in the frequency of various kinds of attacks, incidents of phishing were cited by 44% of companies, followed by scamming (33%), malware (22%), and ransomware (20%). [4]

According to the Identity Theft Resource Centre's 2021 Data Breach Report, there were 1,862 data breaches in 2021, surpassing both 2020's total of 1,108 and 2017's record of 1,506.[1]

A breach lifecycle under 200 days costs $1 million less than a lifecycle over 200 days. [5]

**Introduction**

What is MDR?

The ultimate checklist for selecting the right MDR vendor for your organization

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

[1] Data Breach Report, USA, Identity Theft Resource Centre, 2021.
[2] CIO Survey, KPMG US/Harvey Nash, 2020.
[3] KPMG Fraud Outlook 2022: "A Triple Threat Across Americas", KPMG US, 2022.
[4] Ibid.
[5] Cost of a Data Breach Report, USA, IBM Security, 2020.

Defending against cyberattacks requires your organization to continuously monitor its technology assets for potential breaches, quickly identify attacks in real time, efficiently defend against or contain them, and even anticipate potential threats to help mitigate them before they occur.

The volume of day-to-day monitoring and tools required to stay ahead is vast and costly. Retaining skilled cybersecurity talent is becoming harder, however, and existing teams often don't have the capacity to continuously monitor systems, while also focusing on innovative thinking and strategic improvements that reduce cybersecurity risk.

To address this urgent market need, many organizations look to dedicated, external managed detection and response (MDR) service providers. MDR can help solve complex cybersecurity issues that your organization might struggle with on its own. And with the right provider, MDR can be more than transactional; it can add value and manage security solutions in a way that's aligned with your business goals, reduces risk exposure, manages your threat landscape, and builds a consistent model to achieve the best outcomes for you.

**This guide walks you through a checklist for selecting a MDR vendor including a list of questions you can ask so you find the company that meets your needs and fits best with your organization.**

**Let's get started.**

# What is MDR?

First, a little more about what MDR is all about. MDR monitors your organization’s network, servers, and cloud services for any potential threats, triggers a response to contain or neutralize the threat, and helps prevent similar future occurrences. As part of a Security Operations Centre (SOC), MDR operates 24x7x365, managing a vital part of your business for you.

Introduction

**What is MDR?**

The ultimate checklist for selecting the right MDR vendor for your organization

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

# The ultimate checklist for selecting the right MDR vendor for your organization

With so many MDR service providers out there, it can be a challenge finding the vendor that best suits your needs, understands your industry and business, and can help you meet your goals. Here are the key steps you should consider when selecting the best MDR vendor for you.

## 1. Understand the problem you're trying to solve

There are many reasons why you might consider using an MDR service provider. You may not have full visibility into threats within your organization. Or you might lack skilled resources to "watch the scopes" and respond to alerts. Either way, being strategic and clear about what you need is the first step in finding the vendor for you.

## 2. Define your short- and long-term security needs

Outline the type of immediate threats you're facing and the level of protection you need, while always keeping in mind how the service might meet new or emerging threats and adapt to your business strategy, as it evolves.

Introduction

What is MDR?

**The ultimate checklist for selecting the right MDR vendor for your organization**

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

## 3. Research MDR providers

Look for vendors that have prior experience delivering MDR services, specialize in your specific security needs, and have proven track records of success. Consider additional services the providers offer to help your organization, either during an incident, or more broadly to support your strategy. Understand their approaches to the service, and flexibility to meet your specific needs – today, and tomorrow.

## 4. Create your shortlist and evaluate vendors' capabilities

Ensure the MDR providers you're considering have best-of-breed integrated security technologies (SIEM/SOAR, ITSM, Threat Intelligence), highly skilled and certified staff, well-established processes, and experience in your industry. If their services require additional hardware or software, can they provide it? What work will be left to your team? And do you have the capacity to manage it?

You'll need to provide the vendors with insight into your organization. A good provider will come armed with a list of questions, but remain flexible enough to draw out the additional elements you need to meet your organization's objectives, rather than drive a transaction.

Consider the level of visibility into the service that you need. What reports do the vendors provide, and how beneficial are the insights? Will they inform your strategy and add tangible value to help you reduce risks?

Introduction

What is MDR?

**The ultimate checklist for selecting the right MDR vendor for your organization**

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

## 5. Assess vendors' ongoing service commitment

Do the services include a dedicated service business account manager, technical account manager, and service delivery manager to ensure the vendors meet SLAs, deliver reports at agreed times, make continuous improvements to the services, manage escalations in a timely manner, and entertain new or additional requests? Will they create additional value for your security and IT executives, helping interpret reports and observations in a way that informs your strategy and decision making? Can they present their findings in business terms, and express MDR needs in a way your decision makers can understand, and are they flexible enough to do so?

## 6. Assess providers' reputations and credibility

Check each provider's reputation by reading customer reviews, case studies, and industry awards. Consider any other ratings or accreditations that might give you more comfort, and if they align with your own security frameworks (for example, Service Organization Controls/SOC2 or ISO27001). Also, evaluate the credentials of the executives and downstream professionals delivering the services. Have they done this before? Are they truly security operations professionals, or transplanted executives that may focus on strong financials over the interests of their clients?

Introduction

What is MDR?

**The ultimate checklist for selecting the right MDR vendor for your organization**

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

## 7. Consider pricing

Look for flexible/predictable, growth-based pricing models designed around your infrastructure and data volume tiers. Do the solutions include additional hardware, software, or licensing required to power the services? Will there be specific tasks left to your organization, post implementation, and what skills will your team require to complete them? Balance this against the cost of potential data breaches (loss of IP and reputation damage, compliance violations fines, ransomware payments, transaction, or business loss, etc.), the capabilities these services replace or offset in your organization, and how you might redeploy skills to focus on higher value security work.

Quality comes at a price. Contributing additional value, such as the expert representation of findings, boardroom presence, industry connections, and the ability to bring broad subject matter expertise to bear (beyond cyber), matters.  Consider these when evaluating your service provider, if this is important to you.

## 8. Evaluate the contract terms

Examine the length of the contracts, and the service providers’ terms and conditions to ensure they: a) are flexible enough to meet your requirements, b) adequately protect your interests, c) clearly reflect the deliverables from the implementation and steady state phases, and d) indicate how the services will be measured, to what standard, and the redress options if they’re not (including the SLAs, SLOs, and KPIs they will provide to prove them). Including rate cards for common security or non-security services can

Introduction

What is MDR?

**The ultimate checklist for selecting the right MDR vendor for your organization**

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

help expedite programmatic improvements to your business, by providing extensible options and reducing the time to implement them.

## 9. Consider differentiators

Do the providers present elements of their solutions as differentiators among other vendors in the market? If so, do those differentiators resonate with you and support your strategy?

## 10. Request a demo

Ask for demonstrations of the MDR solutions to see how they work and if their key features meet your needs. Will the solutions integrate well with your technologies (for example, B2B integration with your ticketing system), custom use cases, playbooks, reports, and dashboard? Is customization required? Will your data be hosted in Canada? Are you comfortable with the balance of human expertise and automation the services offer?

Introduction

What is MDR?

**The ultimate checklist for selecting the right MDR vendor for your organization**

Questions to ask MDR vendors to help narrow down your search

Conclusion

About KPMG in Canada

Contact Us

# Questions to ask MDR vendors to help narrow down your search

## 1. Experience/expertise/references

- What are the capabilities of your SOC and where is it located?
- What are your security staff hiring and training practices?
- What's the training and progression path for your analysts? How is the turnover?
- Will you provide a dedicated team of experts to work with our organization?
- Can you provide 4 to 6 client references?

## 2. Compliance and industry benchmarks

- Are you aligned with SOC2 or ISO 27001?
- Have you adopted frameworks, such as NIST and MITRE ATT&CK?

## 3. Costing model

- How is your service priced?
- Do you require a monthly, quarterly, or yearly payment?

## 4. Data residency

- What data do you collect from us to provide your services?
- Where will you host our data? Where will you access it from?
- Will our data be hosted within the geographic boundaries of Canada?
- How do you collect, store, process, and analyze our data?

## 5. Technologies

- Can you use our existing security technologies/ investments, or does our organization need to implement new technologies?
- What technology stack do you offer to deliver end-to-end MDR services, and why were they selected?
- Are your technologies cloud-native or do we need to implement on-premises solutions?
- What security technologies do you integrate with?
- How does your MDR strategy differ among on-premises technology, cloud infrastructure, and cloud applications?

## 6. Customization

- Can your services be customized to suit our organization?
- Can you provide examples of ways you've adapted your service to your client's environments?
- Do you provide custom reports and dashboards?
- Are custom use cases and playbooks part of your service delivery model?

## 7. Onboarding

- What's your onboarding process like?
- How long, on average, does it take to fully onboard a client?
- What activity/task marks the end of onboarding?

## 8. SLAs/incident management

- What's your typical SLA and incident response plan?
- How do you identify and block threats to our systems?
- How do you contain/respond to threats?
- How often do you perform proactive threat hunting?
- What's your Mean-Time-To-Detect (MTTD) and Mean-Time-To-Respond (MTTR) for a critical security incident?
- How can we expect you to interact with us during a security incident?
- What's the process if you miss a threat?
- What's your 'continuous improvement' process?
- How have you enhanced your service as a result of your clients' past security incidents?

## 9. Reporting and Dashboard

- What types of reports should we expect and how frequently do you share these reports?
- How will you give our organization the visibility we need to be confident your SOC is making the right decisions for us?
- How do we know the service is working and making our organization secure?
- Do you provide regulatory compliance reporting?
- Do you have a customer portal where we can view our own data and see the alerts?

# Conclusion

Selecting the best MDR vendor for your business starts with considering your strategy and key business needs, and then researching, evaluating, and assessing vendors’ experience, capabilities, service quality, and pricing. Be prepared to ask lots of questions to determine if the vendors you’re considering align with what your organization needs and what your cybersecurity goals are. Ensure you speak to references, get demonstrations of the services, and understand what your relationship with the vendor will be like going forward.

Introduction

What is MDR?

The ultimate checklist for selecting the right MDR vendor for your organization

Questions to ask MDR vendors to help narrow down your search

**Conclusion**

About KPMG in Canada

Contact Us

# About KPMG's MDR services

Most businesses are already vulnerable to cyber-attacks and will become more so if they don't act quickly. Prevention is the key – and KPMG's Managed Detection and Response (MDR) service is one of the critical ways organizations are enhancing their cyber resilience in today's hostile environment.

Where the "M" and the "D" in MDR are the main focus for many security providers, KPMG extends our coverage to fully address the "R" – responding to and stopping cyber threats before they can impact your business.

We can help you shorten response times, reduce costs, and minimize the impact of a threat event by:

01 Seamlessly integrating with your existing security teams and tools, so you can maximize your return on investment on existing, expensive security technologies.

02 Taking on some or all of your organization's day-to-day monitoring based on your specific needs, freeing up your internal teams to focus on your core business.

03 Informing your security strategy with enhanced reporting in the context of your business.

04 Quickly and automatically identifying and containing attacks, limiting the impact of remediation efforts and the need for extensive cyber 'firefighting' activities.

05 Delivering a collaborative service model that provides your organization with proficient subject matter experts. Our cyber professionals will contextualize observations, explain them to you and your stakeholders, and offer recommendations on effective methods to tackle them – an essential component of successful cybersecurity management.

Introduction

What is MDR?

The ultimate checklist for selecting the right MDR vendor for your organization

Questions to ask MDR vendors to help narrow down your search

Conclusion

**About KPMG in Canada**

Contact Us

Do what you do best, we do the rest! Let us handle the complex, time-consuming, repetitive work involved in MDR.

Our service is unique in the industry, bringing global reach and access to a pool of subject matter experts who are committed to your success:

## Benefit from our analytics-driven and predictive approach

Be more prepared for a potential attack before it occurs and lower your risk for major disruptions with reliable and resilient processes.

## Improve accurate financial forecasting in an inflationary environment

Sign a multi-year contract with us, allowing you to build financial forecasts around security operations more accurately.

## Access speed to value

Amid constant change, we're recognized for the speed at which we help clients respond to disruption. Our MDR service distills decades of experience into pre-configured components, accelerators, and market tested implementation roadmaps – tailored to your requirements – to help you quickly achieve your cybersecurity objectives.

Introduction
What is MDR?
The ultimate checklist for selecting the right MDR vendor for your organization
Questions to ask MDR vendors to help narrow down your search
Conclusion
**About KPMG in Canada**
Contact Us

# Contact Us

**Click here to learn more** about our
Managed Detection and Response Services

**Robert Moerman**
Partner, Cyber Defense &
Managed Security Services Leader
KPMG in Canada
416-777-8308
rmoerman@kpmg.ca

**Guillaume Clément**
Partner, Advisory, Cybersecurity and
President of KPMG Egyde Conseils
KPMG in Canada
418-653-5335
guillaumeclement@kpmg.ca

**Hartaj Nijjar**
Partner, National Cyber
Security Leader
KPMG in Canada
416-228-7007
hnijjar@kpmg.ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

**kpmg.com/ca**