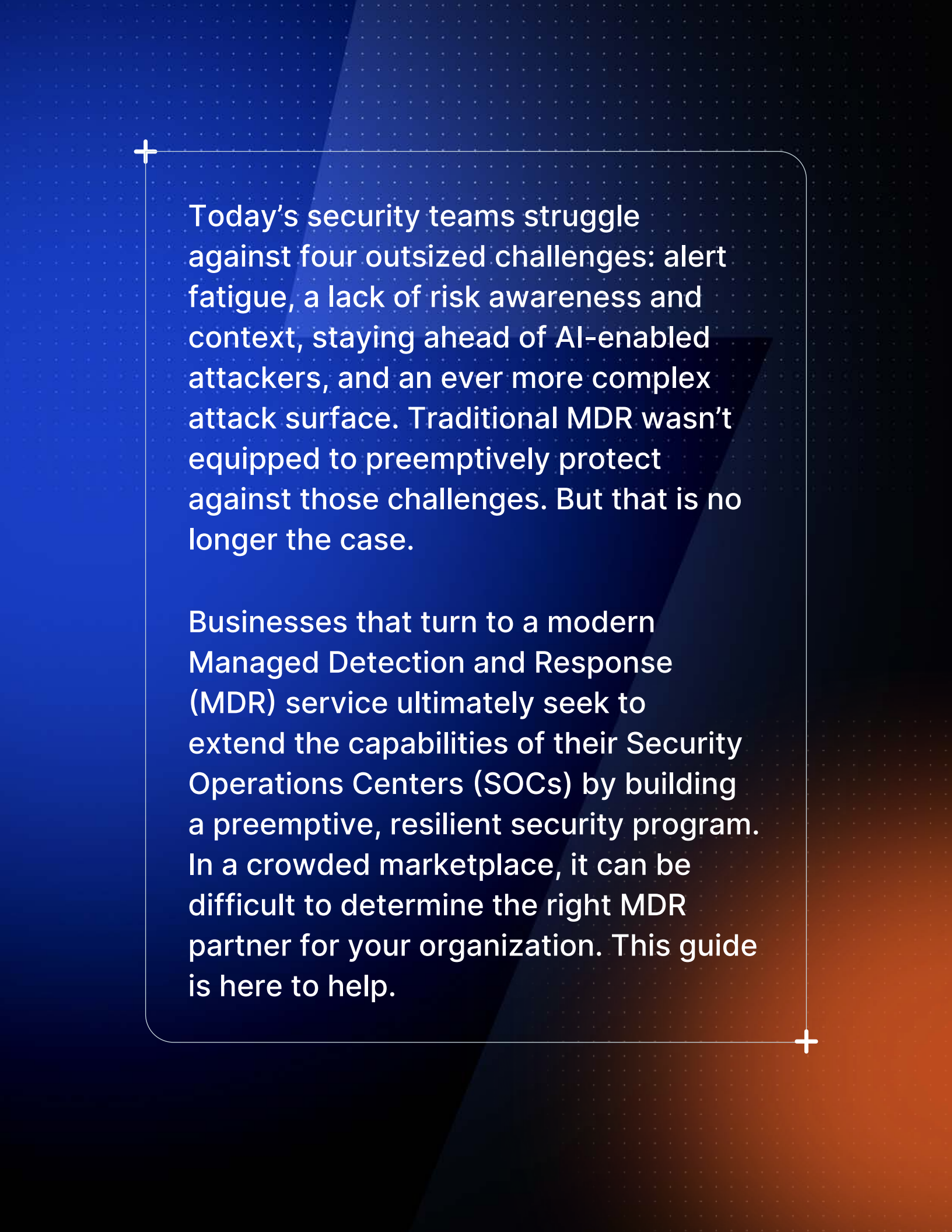


THE COMPLETE MDR BUYER'S GUIDE

Confidently evaluate modern Managed Detection and Response (MDR) solutions.





Today's security teams struggle against four outsized challenges: alert fatigue, a lack of risk awareness and context, staying ahead of AI-enabled attackers, and an ever more complex attack surface. Traditional MDR wasn't equipped to preemptively protect against those challenges. But that is no longer the case.

Businesses that turn to a modern Managed Detection and Response (MDR) service ultimately seek to extend the capabilities of their Security Operations Centers (SOCs) by building a preemptive, resilient security program. In a crowded marketplace, it can be difficult to determine the right MDR partner for your organization. This guide is here to help.

CONTENTS

Executive Summary	4
--------------------------	----------

Cost Justification	5
---------------------------	----------

What kind of MDR partner should you look for?	6
--	----------

1. Headcount and expertise	9
----------------------------	---

2. Technology	11
---------------	----

3. Managed Detection and Incident Response	13
--	----

4. Exposure Management	15
------------------------	----

5. AI-powered automation and response	18
---------------------------------------	----

6. Simple Pricing that Works With You	21
---------------------------------------	----

7. Threat hunting	22
-------------------	----

8. Process and service expectations	24
-------------------------------------	----

Effectively build cyber resilience with Rapid7 MDR	25
---	-----------

MAKE THE RIGHT MDR DECISION WITH CONFIDENCE

Choosing an MDR provider has never been more difficult, or more important. As vendors race to add AI, exposure management, and automation to their offerings, it can be hard to separate meaningful capabilities from marketing claims. Today's MDR solutions need to do more than monitor and respond to threats. They should help organizations understand and reduce risk before attackers can exploit it.

This guide gives security leaders a practical framework for evaluating today's MDR solutions. Learn the questions to ask, the capabilities that matter most, and how to identify a partner that will strengthen your security operations, not just monitor alerts.

Inside you'll learn:

- The key criteria for evaluating modern MDR providers
- How the leading MDR approaches compare, and which is the right fit for your organization
- The questions experienced buyers ask during vendor evaluations and RFPs
- What capabilities drive stronger security outcomes, from exposure management to incident response

Whether you're replacing an existing provider or investing in MDR for the first time, this guide will help you make a confident, informed decision.



COST JUSTIFICATION

In the spirit of transparency, a good MDR provider can cost a lot. But it's a whole lot more economical than standing up your own 'round-the-clock SOC team with the latest technologies and security approaches. Even the most well-heeled internal security operations teams struggle with 24/7/365 staffing of a diverse team of security experts and the latest tools for them to work on.

Building a modern SOC today requires you to go beyond the "core" capabilities. In order to provide the 24/7 coverage required a bespoke SOC needs a double-digit team with the required tools, platforms, and a host of processes and playbooks.

By adding these personnel and the technology solutions and capabilities to detect threats across your environment, you're easily looking at a multi-million dollar investment for a bespoke SOC.

And that's not to mention challenges like:

- One-by-one interviewing and hiring of highly sought after, experienced staff
- Finding ways to retain that SOC staff and keep them happy (like not working night shifts)
- Implementing the latest AI and machine learning capabilities and the governance to do them effectively
- Focusing on the massively important task of building out your SOC, which means not focusing on other parts of your growing business
- Proving the value and ROI of detection and response, especially to budget-controlling stakeholders outside of the security organization

MDR will be a significant consideration when slicing and dicing your budget. But if you haven't already built out a proven SOC and have stakeholders in urgent need of comprehensive detection and response capabilities, a rapidly engaged and deployed managed services solution might be for you.

KEY QUESTIONS AND CONSIDERATIONS

- Will your provider be available for non-emergency communication, by email, phone, chat, or otherwise?
- Is the provider able to offer all components of core MDR services, including 24x7 monitoring, detections, investigation, containment, exposure management, AI-enabled automation, and threat hunting?
- Will your partner tailor their service to your organization's desired outcomes?
- Will they actually serve as an extension of your SOC with a team of detection and response experts that enable you to find and stop threats anywhere they arise?
- Will they partner with you to drive your business forward and mature your security program?

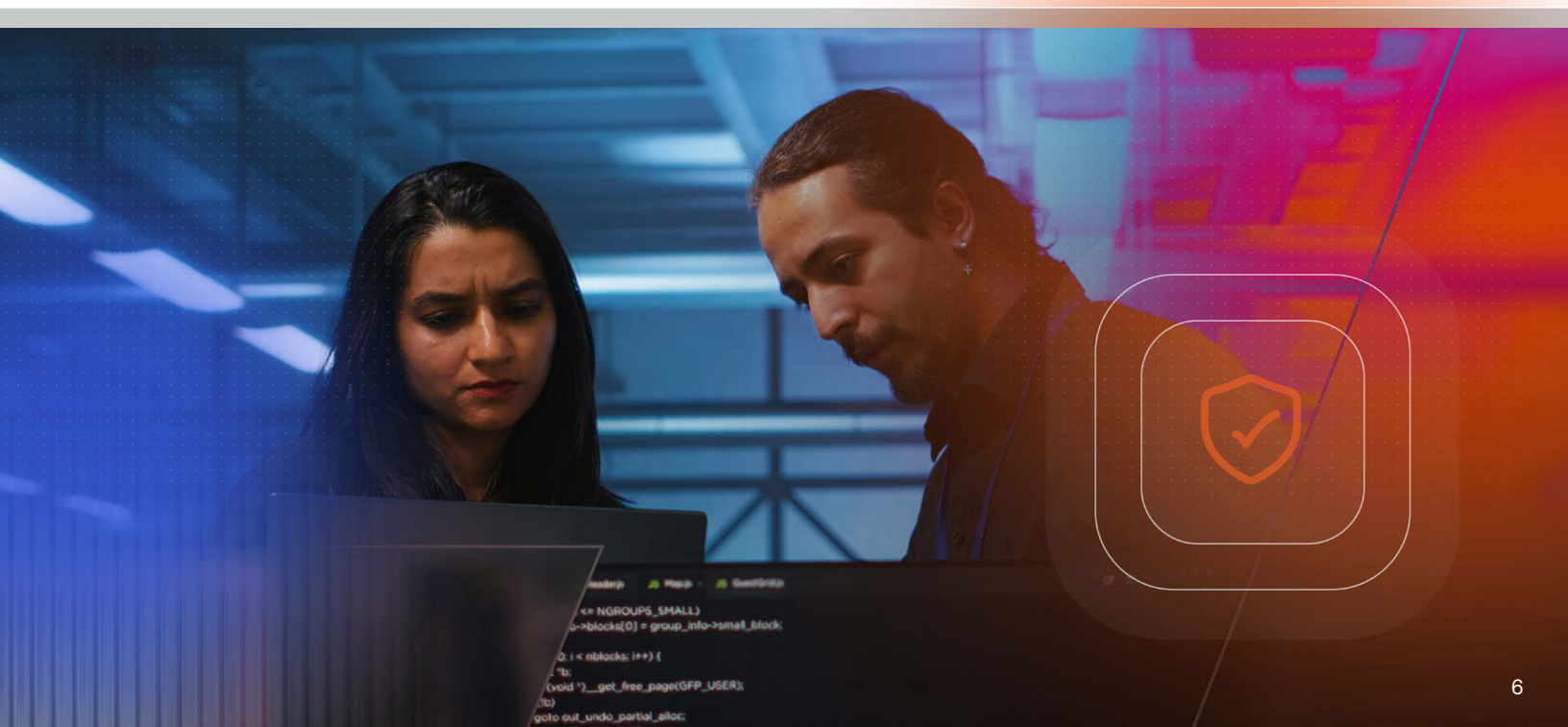
WHAT KIND OF MDR PARTNER SHOULD YOU LOOK FOR?

The MDR market continues to evolve, and not all providers are created equal. Today, security teams are increasingly choosing between four dominant approaches and understanding the distinctions is essential to making the right long-term decision for your organization.

Managed Endpoint Detection and Response (MEDR) providers are centered on delivering detection and response capabilities through endpoint protection tools. These solutions can be a good fit for teams that are already deeply invested in their endpoint tool of choice and are looking for outsourced support focused solely on that surface. However, they often fall short when it comes to holistic visibility across cloud, network, and user telemetry.

Bring Your Own Tech (BYO-Tech) MDR providers integrate with your existing stack of EDR, SIEM, and cloud tools to deliver monitoring, investigation, and response. These vendors typically position themselves as flexible and vendor-neutral, allowing customers to retain control of their security investments. But the caveat may be lower expertise with your specific stack, and issues integrating different tools together.

Managed Security Service Providers (MSSPs) are a broad category — some offer only basic alert forwarding or monitoring, while others provide more mature services such as alert triage or compliance reporting. Some MSSPs have begun introducing MDR-style offerings, but the scope and sophistication of these services can vary widely. For buyers, it's important to look beyond labels and understand what's truly included — whether that's threat detection, active investigation, or response. MSSPs can be a fit for more mature organizations looking for cost-effective coverage or compliance support. However, for teams seeking fast time to value, platform integration, and continuous improvement, it's important to compare MSSPs side-by-side with modern MDR providers.



Pure-Play MDR providers deliver a fully integrated solution: native technology and service packaged together to offer end-to-end detection, investigation, and response across your modern attack surface. These providers typically operate their own SOC's, staff expert analysts, and deliver service through proprietary platforms that include their own telemetry, analytics, and automation. As a result, Pure-Play MDR solutions can onboard faster, deliver broader visibility out of the box, and ensure tighter coordination between threat detection and real-time response. This approach is particularly well-suited to security teams seeking to consolidate tooling, streamline operations, or expand coverage without dramatically increasing internal headcount

As you can see, MDR vendors are leveling up their programs' abilities to address more sophisticated threats across the entire attack surface. The effectiveness of solutions that work together to pick up where another has ended – all through a single pane of glass — is helping to extend the SOC's reach and enable faster threat takedowns. This new generation of multifaceted detection and response requires a dedicated SOC staffed with highly skilled security experts using the best technology, cutting-edge threat intelligence, and forensic tools to reveal and report problems to ensure stealthy attackers have nowhere to hide.

KEY QUESTIONS AND CONSIDERATIONS

- Which components of a managed service are most important to your organization?
- Is consolidating functionality into a single service a priority? What can be consolidated and what do you want to remain an in-house function?
- What does your existing workflow between detecting and responding to threats look like?
- Where, along that workflow, is most important to augment and reduce overall Mean Time to Respond (MTTR)?
- How would you prioritize extending the visibility and efficacy of your internal security team?

MDR service delivery spans both core threat detection and response capabilities and adjacent services that enhance threat visibility and improve security outcomes. Effective MDR providers deliver these capabilities through a remotely delivered, provider-operated technology stack that integrates endpoint, network, log, and cloud telemetry. Increasingly, MDR services also incorporate identity data, SaaS signals, and third-party integrations to strengthen threat detection and contextual understanding.

Detection engineering remains critical, with providers building, tuning, and continuously evolving analytic content and workflows. Threat intelligence is applied from both internal and external sources. Providers are expected to deliver human-led detection, investigation, and threat hunting, and to take mitigative response actions (e.g., host isolation, account lockout, network blocking) based on predefined customer agreements. Adjacent services now often include exposure assessments, attack surface analysis, breach and attack simulation (BAS), and incident response support — expanding the MDR role from pure detection into proactive security posture management.

But as you've probably seen, almost every vendor claims they are consolidating these many solutions to offer a more empowered MDR program which is why it's so difficult to begin to tell fact from fiction when launching the search for a vendor. To navigate the crowded market, try to ensure you're evaluating each vendor across eight of the most critical core capabilities and expectations:

CORE CAPABILITIES & EXPECTATIONS TO EVALUATE IN AN MDR PARTNER

1. HEADCOUNT AND EXPERTISE

2. TECHNOLOGY

3. MANAGED DETECTION AND INCIDENT RESPONSE

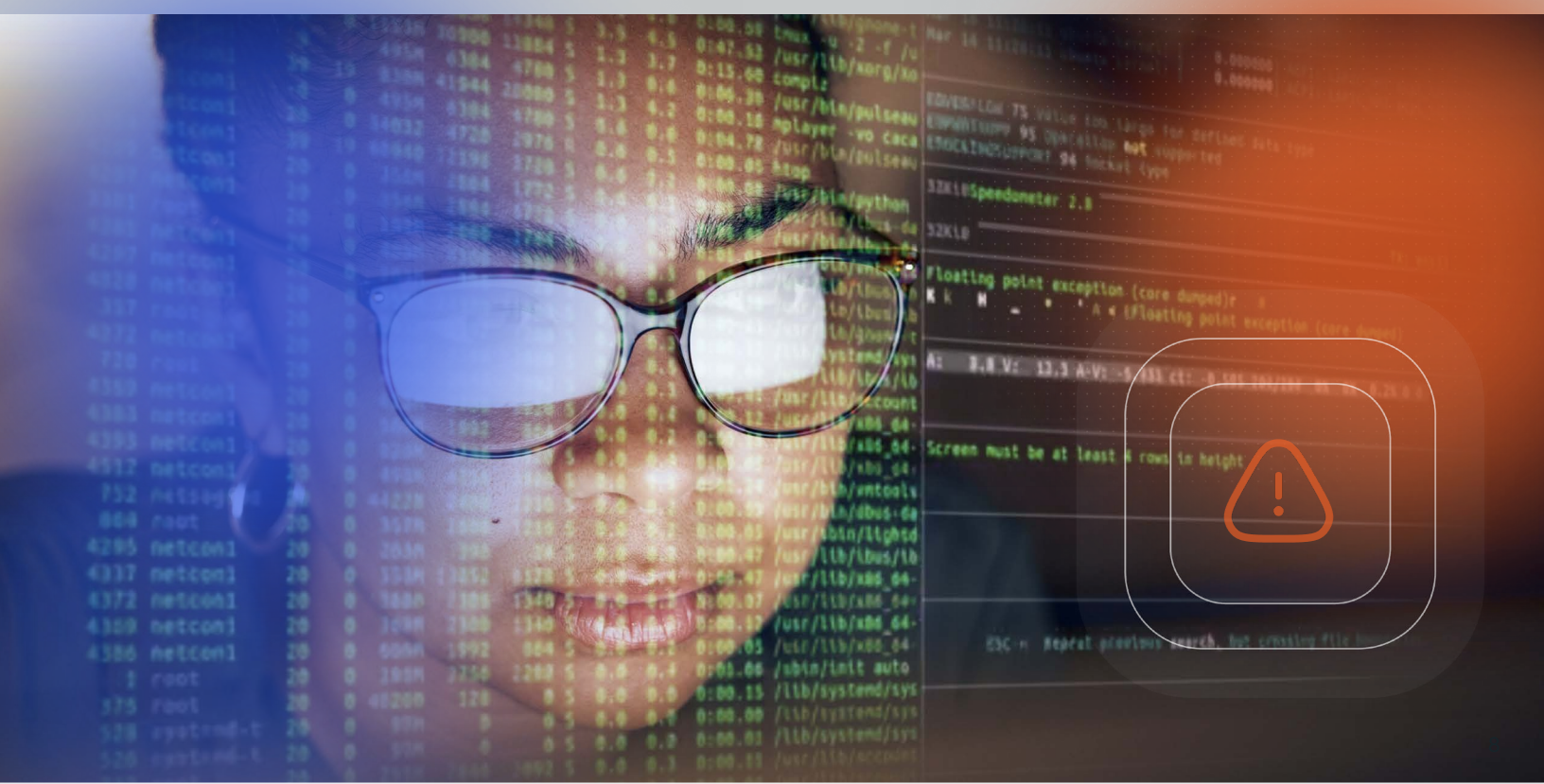
4. EXPOSURE MANAGEMENT

5. AI-POWERED AUTOMATION AND RESPONSE

6. SIMPLE PRICING THAT WORKS WITH YOU

7. THREAT HUNTING

8. PROCESS AND SERVICE EXPECTATIONS



1. HEADCOUNT AND EXPERTISE

Round-the-clock monitoring by SOC experts is crucial in the seemingly forever-war against today's attackers. They don't sleep, so why should your MDR? In many instances, attackers target organizations when they're likely to be weakest, in their off hours. You want your headcount and specialist personnel freed up to innovate, push forward long-tail security initiatives, and provide increasing value to the business.

Staffing and headcount

If your company is facing staffing issues in skilled security and IT positions, you're not alone. The post pandemic world still places a premium on security talent – no matter where they're located. Therefore, small-to-midsize companies may not be able to pay ultra-competitive salaries that some world-dominating firms can.

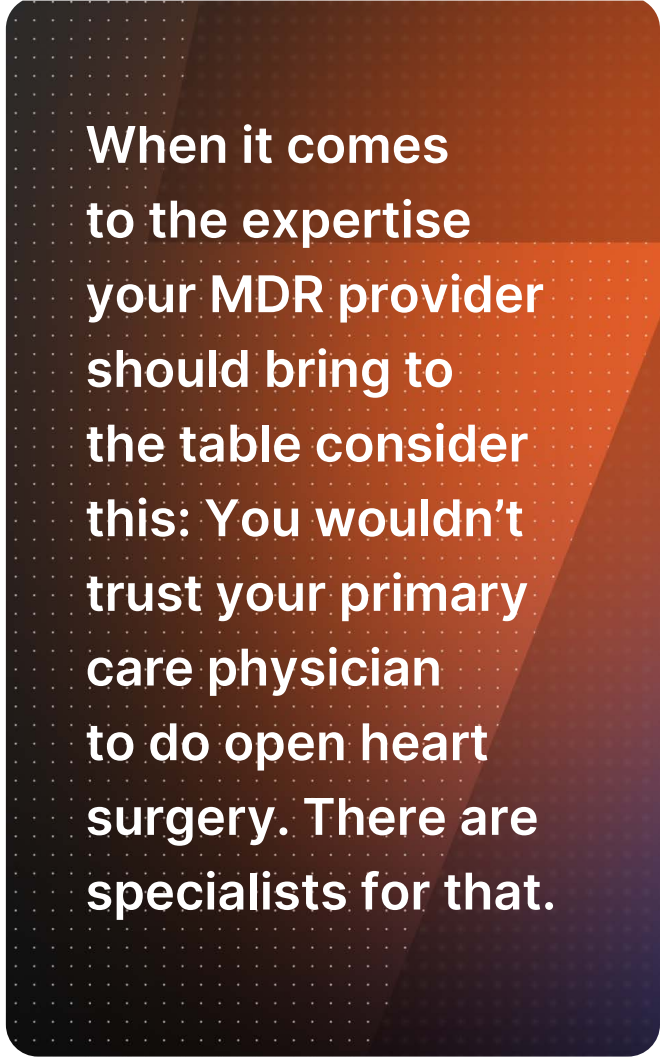
So, if you see a shortage of security personnel now or in the near future, it will become extremely necessary to find value in your MDR provider of choice. If a vendor is focusing solely on your organization's detection and response capabilities, you should ultimately experience shorter response times after a detection is validated, especially in an automated-workflow world.

Therefore, it's critical for the specialists you do have to push strategic objectives, implement security best-practices, and build resilience within their organization and overall program.

Expertise

The same is true for cybersecurity. A security generalist might be able to monitor technology for alerts, but they're certainly not going to be able to do deep investigations, malware forensics, or scope and respond to a breach. That's why it's critical to bring in specialized capabilities like:

- **Integrated threat intelligence** — Pulling in data and insights from multiple telemetry sources — internal and external — is the basis of XDR. This type of advanced threat intelligence leads to smarter, more actionable, and more precise threat-hunting capabilities. Taking all of this into account, an MDR provider should be able to alleviate SOC teams from dealing with the sheer number of false positives pouring in as organizations race to adopt cloud infrastructure and scale up.
- **Breach-response capabilities** — When it comes to "incident response," make sure you're going to get what you pay for.



When it comes to the expertise your MDR provider should bring to the table consider this: You wouldn't trust your primary care physician to do open heart surgery. There are specialists for that.

Every MDR vendor will tell you their people are experts who can respond to incidents. But most are minor incidents. The best MDR providers are staffed with analysts and DFIR experts able to fully respond to major incidents within an organization's environment to fuel faster response and reduce downtime. They have logged thousands of hours of experience handling some of the most advanced data breaches in history.

- **Named cybersecurity advisor as your main POC** — Appointing a security-program advisor as each customer's point of contact (POC) is a main piece of criteria against which an MDRs provider's effectiveness will be judged. Advisors should learn about customer environments, goals, and limitations so they can provide the fastest breach notification and response, as well as guidance for program improvement

As a prospective customer, try to dig deep into what your relationship and engagement model will look like so an MDR partner brings real benefits to your team and acts as a true partner rather than a "human SMS" system. Your cybersecurity advisors should be available to provide regular updates in the form of monthly consultations and/or service report reviews.

KEY QUESTIONS AND CONSIDERATIONS

- What is the experience level of the MDR SOC team that will be monitoring my environment?
- What is the tenure and attrition rate of the team?
- How many MDR analysts are assigned to monitor my environment?
- How does the MDR provider ensure 24×7 coverage? Is it a follow-the-sun model?
- How does the provider integrate threat intelligence into the service?
- What is the process if the MDR provider misses a confirmed breach in the environment?
- What is the ratio of MDR SOC analysts to customers? Security Advisors to customers?
- How quickly can your SOC team scale up to detect and respond to larger incidents, like a supply chain breach?

2. TECHNOLOGY

The best MDR services combine deep observation of endpoints, real-time forensics (DFIR), authentication, network, and log data with functionality that tackles rapidly scaling cloud environments and pulls in context from native and 3rd party sources. More recently, these services are incorporating practical applications of AI, like AI-powered workflows for investigative tasks, that scale human decision making leading to smarter, more efficient outcomes for customers.

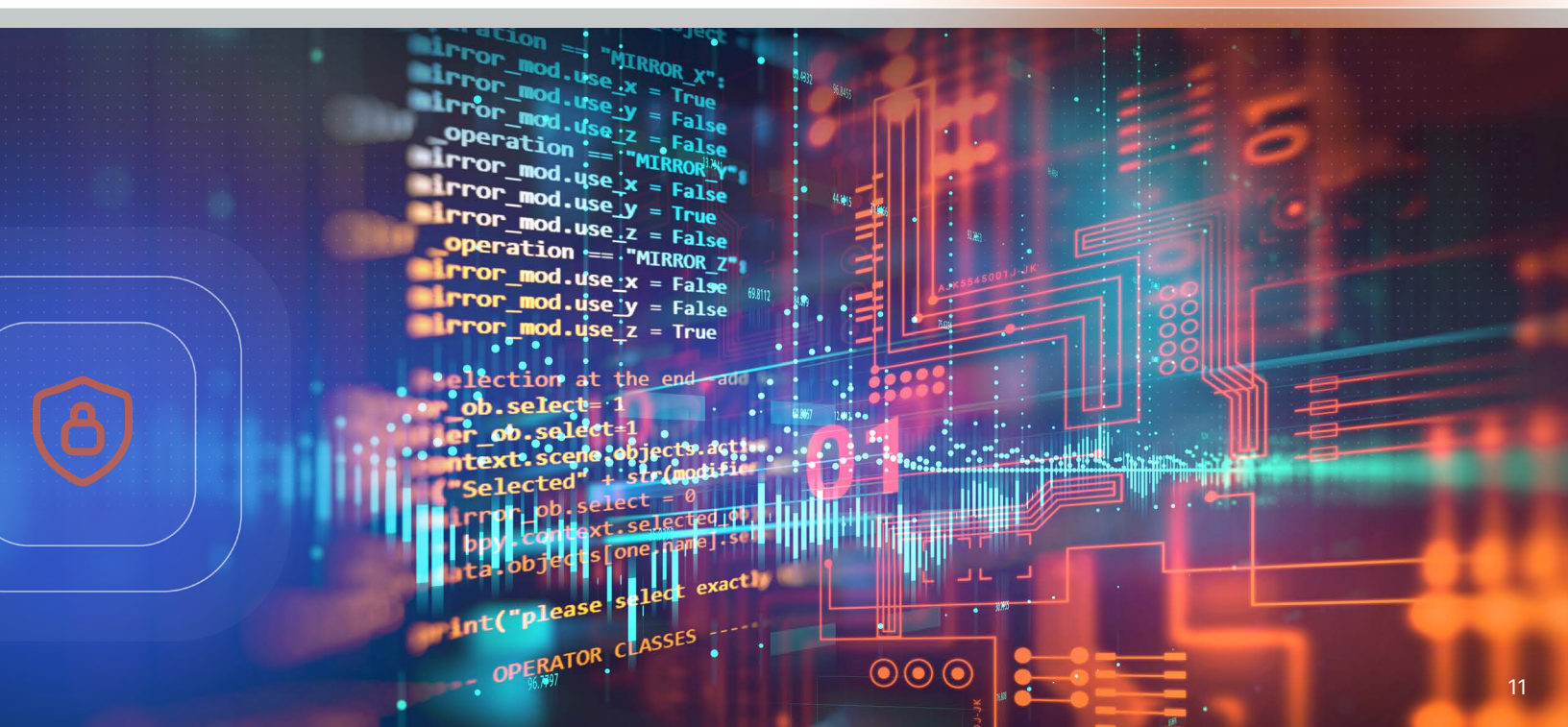
Experts are extending MDR SOC functionality to tackle rapidly scaling cloud environments. This combined approach is a cloud-native platform that enables security teams to optimize threat detection, investigation, response, and hunting in real time, with scalability and opportunities for automation.

Since threats are coming from anywhere and everywhere along the modern network attack surface, greater scope of visibility means having a more cohesive view of related events so you can elevate outcomes by detecting threats faster. Without multiple sources of telemetry, your depth of defense could be lacking, leaving your environment exposed.

User-endpoint Telemetry — User telemetry provides insights on file-and-network access, registry access or manipulation, memory management, and start-and-stop activity. Unusual behavior detected can include processes that spawn command shells, memory injection attempts, or accessing unusual file locations.

Server-endpoint Telemetry — Server telemetry provides information on extremely differentiated data. Since servers handle so much crucial organizational functionality, XDR telemetry can help prioritize investigations and remediations of incidents on a more macro level.

Network Telemetry — Network telemetry provides insights on traffic, particularly a sudden increase in volume, new network protocols, or anomalous privilege escalations. Advanced encryption methods can often hinder deeper network analysis that could otherwise thwart threat actors. But make no mistake: Combined with endpoint telemetry, network traffic analysis (NTA) can be a cornerstone of an XDR offense.



Cloud Telemetry — Cloud telemetry provides insights on infrastructure. This can include detecting security anomalies for any cloud workloads or components deployed. Attackers specifically targeting an organization's cloud components can easily gain access with the proper credentials, so it is of critical importance to leverage the advanced detection technology of XDR to hunt threats faster and fortify cloud environments.

When an MDR solution is built on top of native XDR technology, customers get deep visibility into their scaling environments and coverage from advanced threats. It's important to note that increasingly, MDR providers are tasked with understanding customers' risk profiles and remediating — exposures, vulnerabilities, misconfigurations, and more — before an environment is breached.

KEY QUESTIONS AND CONSIDERATIONS

- How does the provider detect threats that bypass preventative controls?
- Will you have full access to the MDR partner's back-end technology?
- If full access is not provided, can you self-service log search and dashboards?
- Is there any ability to create customizations within the technology?
- Is there an included or adjacent SOAR tool that allows for custom automation based on your environment's needs?
- Can your MDR provider tell if a potential threat is an outside attacker impersonating an employee?
- How does your MDR provider detect if an actual employee is presenting risk, whether through negligence or malice?
- What's your MDR provider's process for detecting and responding to unusual user behavior?
- Can the provider support other assets and environments like public and private clouds (IaaS, SaaS, PaaS), Operational Technologies (ICS/SCADA), and internet-of-things (IoT) devices?

3. MANAGED DETECTION AND INCIDENT RESPONSE

Limiting an attacker's ability to execute is perhaps the most crucial consideration after detection, especially if an attacker is proficient at bypassing proactive security controls. So there are two considerations for effective incident response:

- Act with urgency
- Leverage a strategy that goes beyond only securing affected endpoints

An effective response should include commanding your attack surface to cut attackers off at both the endpoint and user-account levels, and your MDR provider should be able to take action immediately in the wake of detecting confirmed malicious activity.

Managed response

The worst thing your MDR partner can do is tell you “we found this threat, now you have to go take care of it.” You should find an MDR provider that can help you take action at any time, day or night, with whatever level of collaboration and control you specify.

Gartner sees this as a core capability for MDR providers: “The key value proposition of MDR is the human interpretation of cybersecurity incidents and identified threat exposures, outlining their potential impact on an organization. MDR also provides guidance on remediation and, in many cases, will perform the initial mitigation steps: Provide guidance in a consumable format that would commonly be complex to understand and enact. By providing context-led investigation, analysis, and mitigation (taking action to disrupt or contain an attack or mitigate an exposure to a risk), the MDR provider can buy time for the customer to perform further investigation and ultimately remediate discovered issues utilizing their internal standardized response processes.”¹

This type of provider is more aligned as a partner for your business than a transactional, service-oriented relationship. Look for a service provider who will be working shoulder-to-shoulder with your team in the event of a breach. No time should be lost when minutes are critical.

Digital forensics and incident response

When something really bad happens, you don't want to be referred down the line to another third party all because your MDR provider's SOC “can't handle it.” And who wants to deal with fighting for incremental budget for yet another provider when you only thought you'd be dealing with one? The best MDR providers have breach-response expertise on staff and are included as part of their MDR service. This level of integrated, in-house team should be able to quickly pivot to forensic investigation mode once a confirmed breach is detected, particularly if it has affected multiple endpoints, lateral movement is occurring, or there is active data exfiltration.

¹ Gartner. Market Guide for Managed Detection and Response Services. Shoard, Davies, Berrios. October 1, 2025.

Continuous monitoring

In the spirit of assuming full command of the attack surface, the SecOps loop continues unabated. Because after the incident has seen proper response and the investigation has concluded, vigilance must remain. This means continued and always-on monitoring for vulnerabilities as well as regularly enlisting your managed vulnerability management partner to help ensure your resilience isn't revoked. They can do this by accelerating your ability to:

- Discover risk
- Prioritize vulnerabilities
- Remediate accordingly
- Track progress
- Optimize your program

Because after a breach is contained, it's critical to keep proactively closing doors before attackers have a chance to break through.

Breach protection

A good MDR provider stands by their work with real accountability. If a breach protection warranty is offered, make sure it is worth the paper it is written on. Look for assurances that in the event of a breach, there are no hidden strings that diminish the quality of the warranty, funnel reimbursements back to the company, and that true unlimited incident response is included to avoid sudden decreases in coverage.

KEY QUESTIONS AND CONSIDERATIONS

- What types of managed response actions can their SOC take?
- How can I deny the containment response if I don't want the SOC team to take action, especially if the action is automated?
- Can the provider articulate a top-level before, during, and after attack plan for cyber resilience?
- What types of responses are in-scope for the provider? What will you be on the hook for?

4. EXPOSURE MANAGEMENT

Effective detection and response begins with understanding exposure. The most effective MDR providers help organizations do more than identify and contain threats, they help reduce the likelihood of those threats succeeding in the first place. Attackers do not think in terms of alerts, vulnerabilities, or tools. They think only in terms of opportunity, looking for exposed assets, weak identities, missing controls, and attack paths that allow them to move through an environment undetected. This is why exposure management has become a critical component of modern MDR.

Without visibility into the exposures that create risk, MDR teams are left responding to incidents after attackers have already found a way in. By combining exposure management with detection and response, organizations can shift from a purely reactive security model toward a more preemptive approach that continuously reduces risk.

Anticipate: Understand risk before it becomes an incident

The best MDR providers help organizations anticipate attacks by continuously assessing their attack surface and identifying the exposures most likely to be exploited.

This starts with establishing a complete view of the environment. Security teams need visibility into every asset across cloud, on-premises, SaaS, and hybrid environments. Unknown assets, shadow IT, unmanaged devices, and risky identities all create opportunities for attackers.

An exposure-aware MDR service should help organizations:

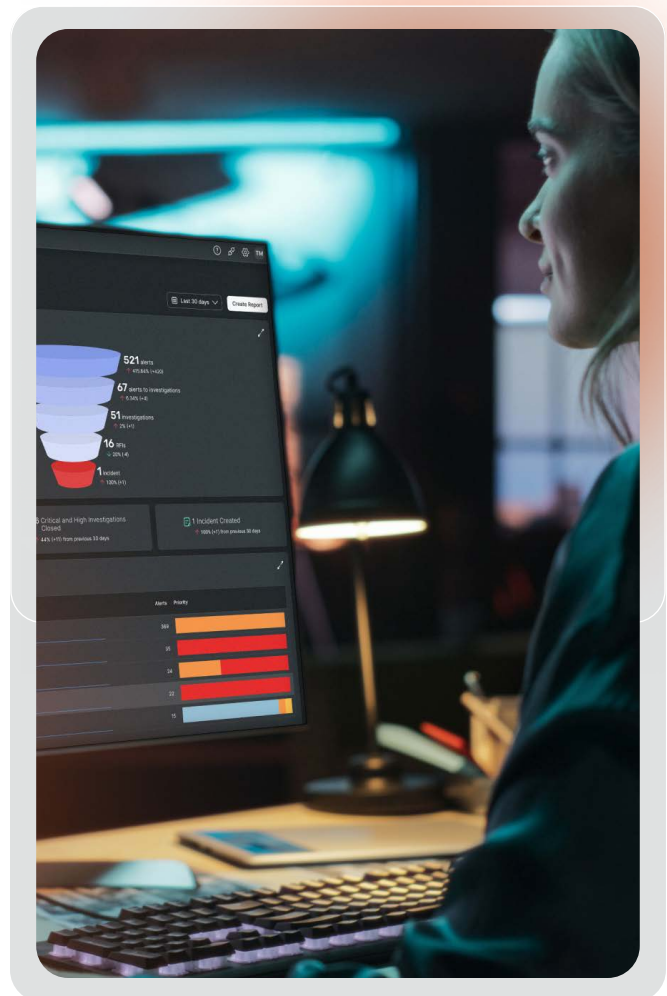
- Establish a single source of truth for assets across the environment
- Continuously discover and inventory known and unknown assets
- Identify security gaps such as missing endpoint protection, vulnerability scanning, or multi-factor authentication (MFA)
- Evaluate exposures based on real-world exploitability and business impact
- Leverage threat intelligence to understand which risks attackers are actively targeting

By understanding where risk exists before an alert is generated, security teams can reduce the number of opportunities available to attackers.

Pinpoint: Focus on the risks that matter most

One of the biggest challenges facing security teams today is prioritization.

Most organizations are not struggling with a lack of findings. They are struggling with too many



findings and too little context. Exposure management provides the context necessary to pinpoint the most critical and actionable risks. Rather than treating every vulnerability equally, leading MDR providers help customers understand:

- Which exposures attackers are most likely to exploit
- Which assets are critical to business operations
- Which attack paths create the greatest risk
- Which vulnerabilities are actually reachable within the environment
- How vulnerabilities, misconfigurations, identities, and missing controls combine to create risk

This allows teams to focus remediation efforts where they will have the greatest impact on reducing overall exposure.

Act: Turn insights into measurable risk reduction

Identifying risk is only valuable if teams can act on it. Modern MDR providers should make remediation an integrated part of the workflow rather than a disconnected process. Exposure management should help eliminate silos between security, IT, cloud, infrastructure, and development teams.

Look for providers that enable teams to:

- Group exposures by root cause to "act once, fix many"
- Integrate remediation workflows directly into existing systems and processes
- Assign remediation owners and track progress against service-level agreements (SLAs)
- Monitor risk reduction across teams, assets, and business units
- Leverage expert guidance to determine the most effective remediation strategy

The goal is not simply finding more issues. It is reducing exposure faster and more efficiently.

Value: Demonstrate measurable outcomes

Security leaders are increasingly expected to demonstrate the value of security investments in business terms. Exposure management helps bridge the gap between technical findings and business outcomes by providing measurable visibility into risk reduction over time.

An exposure-aware MDR program should help organizations:

- Track risk trends using normalized risk scoring
- Measure the impact of remediation efforts
- Demonstrate improvements in security posture
- Simplify compliance reporting and audit preparation
- Align security priorities with business objectives and operational resilience

The result is a clearer understanding of how security activities reduce risk, support compliance initiatives, and protect critical business operations.

KEY QUESTIONS AND CONSIDERATIONS

- Does the MDR provider offer continuous visibility across internal, external, cloud, SaaS, and hybrid environments?
- How does the provider identify unknown assets, shadow IT, and risky identities?
- What methodology is used to prioritize exposures beyond CVSS scores?
- Can the provider identify attack paths and show how exposures could be chained together by an attacker?
- How does the MDR service integrate threat intelligence into exposure prioritization?
- Are remediation workflows integrated into existing tools and operational processes?
- How does the provider measure and report on risk reduction over time?
- Can the provider demonstrate how exposure management improves detection and response outcomes?
- What visibility will security leaders have into exposure trends, compliance posture, and business risk?

Organizations that combine exposure management with MDR gain more than faster detection and response. They gain the ability to continuously reduce risk, strengthen resilience, and stay ahead of attackers before an incident occurs.



5. AI-POWERED AUTOMATION AND RESPONSE

Modern MDR is no longer just about monitoring alerts and escalating incidents. As attackers move faster, security teams need the ability to investigate, validate, and respond at a speed that manual processes alone cannot match. This is where the combination of artificial intelligence (AI), security orchestration, automation, and response (SOAR), and human expertise becomes critical.

The most effective MDR providers use AI and automation to accelerate security outcomes across the entire attack lifecycle. Rather than replacing human analysts, AI enables them to focus their expertise where it creates the greatest value: validating threats, containing incidents, and guiding recovery.

Before: Readiness informed by exposure and asset context

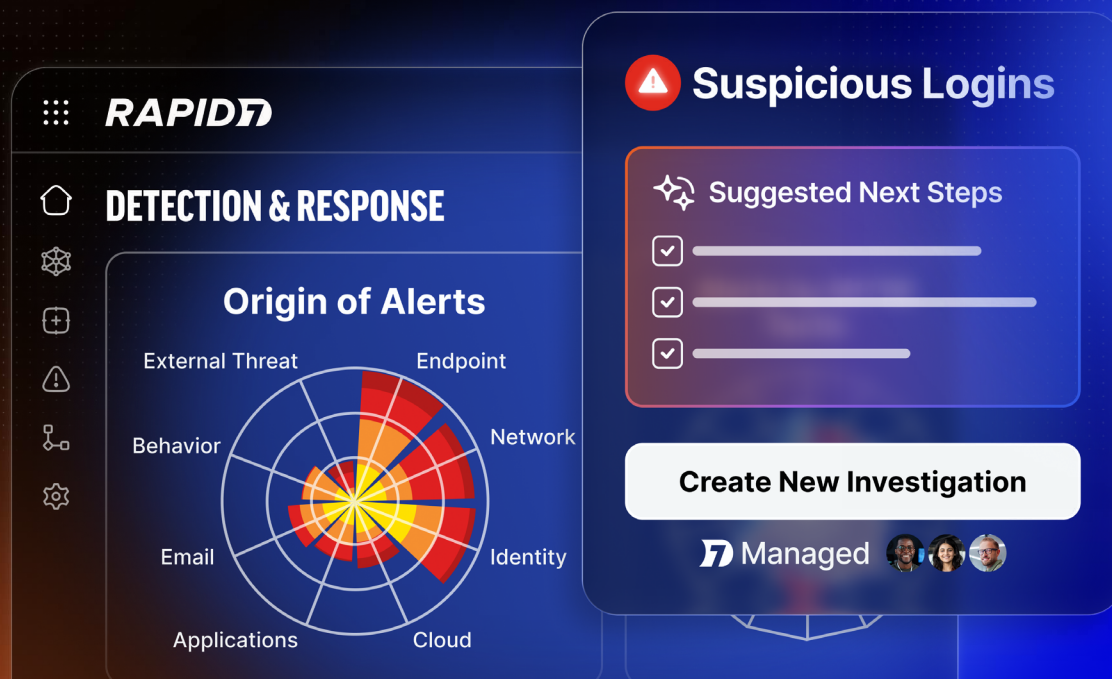
Effective response begins long before an alert is generated. Modern MDR services should combine exposure management, asset intelligence, vulnerability findings, and threat intelligence to understand where attackers are most likely to succeed. This context helps security teams proactively reduce meaningful risk by identifying exploitable weaknesses, critical assets, and likely attack paths before they become incidents.

AI can continuously analyze exposure data at a scale that would be impossible for human analysts alone, helping organizations prioritize remediation efforts and focus resources where they will have the greatest impact.

During: Faster detection and investigation powered by AI

Security operations centers receive thousands of alerts every day and the biggest challenge they face is determining which ones actually matter and what the best next steps are when responding.

AI-powered MDR solutions help scale detection, triage, and investigation workflows by automatically enriching alerts with contextual information from across the environment. Endpoint telemetry, network activity, identity signals, threat intelligence, cloud events, and asset context can be correlated automatically to build a complete picture of potential attacker activity.



This enables security teams to:

- Reduce false positives and alert fatigue
- Prioritize investigations based on risk and business impact
- Accelerate threat validation and incident scoping
- Surface hidden attacker behaviors that may otherwise go unnoticed
- Deliver more detailed and actionable incident reporting

The most effective MDR providers deliver transparent, explainable AI outputs that allow analysts and customers to understand how conclusions were reached. Human experts remain responsible for validating findings, making containment decisions, and ensuring the appropriate response.

When threats are confirmed, SOAR capabilities allow teams to execute response actions quickly and consistently through automated workflows. Examples include:

- Isolating compromised endpoints
- Disabling or deprovisioning accounts
- Blocking malicious IP addresses, domains, URLs, and file hashes
- Enriching indicators with threat intelligence
- Triggering ticketing and remediation workflows
- Coordinating containment actions across multiple security technologies

The combination of AI-driven investigation and SOAR-powered response dramatically reduces response times while maintaining analyst oversight and control.

After: Strengthening defenses through automation and analysis

Following an incident, MDR providers should leverage AI, forensic analysis, and automation to strengthen future defenses. Post-incident investigations help organizations understand attacker behavior, identify root causes, eliminate persistence mechanisms, and implement mitigation strategies that reduce the likelihood of recurrence. The bottom line is that response does not end when an incident is contained.

Automation can also streamline remediation efforts by coordinating activities across security, IT, cloud, and infrastructure teams. The result is a more resilient security program that continuously improves based on lessons learned.

Why AI and automation matter

The goal of AI and automation is not to remove humans from security operations. It is to amplify their capabilities. The right MDR provider uses AI to handle repetitive, time-intensive tasks such as alert triage, enrichment, and initial investigation while allowing experienced analysts to focus on higher-value decisions. This creates greater consistency, broader coverage, and faster outcomes while incorporating the expertise and judgment of experienced and pressure-tested human analysts.

Innovation should be grounded in proven security expertise, transparent decision-making, and measurable outcomes. When AI, automation, and human expertise work together, organizations gain the speed and scale needed to disrupt attackers while maintaining confidence in every decision.

KEY QUESTIONS AND CONSIDERATIONS

- How does the MDR provider use AI within detection, triage, investigation, and response workflows?
- Are AI-generated findings transparent, explainable, and auditable?
- What role do human analysts play in validating AI outputs and making response decisions?
- What SOAR capabilities are included as part of the service?
- Which response actions can be automated, and which require customer approval?
- Can workflows be customized to align with existing security and IT processes?
- How does the provider leverage threat intelligence to enrich alerts and improve prioritization?
- What measurable improvements in detection, investigation, and response times can be expected?
- How does AI improve analyst efficiency while maintaining accuracy and oversight?
- How does the provider use post-incident analysis to strengthen future defenses and reduce risk?

The future of MDR is not purely human-driven or fully automated. It is a combination of AI-powered scale, automated response, and experienced security professionals working together to accelerate security outcomes across the attack lifecycle.



6. SIMPLE PRICING THAT WORKS WITH YOU

Much like when buying into anything that requires a larger budgetary commitment — and protects what makes your business run — pricing should be transparent, predictable, and customized to your environment.

It should be based on:

- The number of assets (workstations, servers, etc.) in your environment
- The expectation there will be continuous, 24/7 real-time alert monitoring
- The expectation there will be a dedicated cybersecurity advisor as the main
- POCs for technical and day-to-day service delivery
- The expectation the MDR technology will begin learning its way around your systems on day one and be able to quickly start monitoring and threat protection
- Receiving detailed analysis and regular reports with tailored remediation guidance and recommendations

What it shouldn't be based on:

- How many egress points or locations you have: MDR is about monitoring your environment, no matter how big or spread out it is. You shouldn't be penalized for having multiple offices.
- How many servers you have: A threat on an endpoint is similar to a threat on a server. You shouldn't be charged for looking at endpoint threats on different machines.
- How much data you can send to MDR: Detection and response is about finding threats with context and correlation, not charging for collecting events per second. Your MDR provider should want to see the data you have, so make sure that if there is a data allotment it's enough to cover the most important sources used to detect threats.

KEY QUESTIONS AND CONSIDERATIONS

- Does the provider offer volume-based discounts for the number of assets?
- Are costs for additional services, like vulnerability management, digital forensics, major IR engagements, data overage fees, SOAR, built in or priced a la carte?
- How do they determine the price of their MDR service? What happens if you go over your allotted data limit?

7. THREAT HUNTING

Paring down data into actionable insights and detecting anomalies in customer environments is the foundation of a successful threat-hunting methodology. A provider should first get to know the ins and outs of your IT and security stacks. Then it should implement a tailored plan that incorporates multiple angles of threat hunting, allowing them to make sure they're hunting through the right information, with the right checks, at the right time to identify undetected, lingering threats. Let's now take a look at the different types of threat hunting you should ensure a provider is offering in a services package.

Intelligence-led hunting

Threat intelligence provides the foundation for identifying emerging threats, newly discovered attacker techniques, and suspicious activity that may not yet be detected through standard monitoring.

Look for providers that can:

- Leverage integrated threat intelligence from internal and external sources to guide hunting activities
- Conduct hypothesis-based hunts targeting newly identified attacker tactics, techniques, and procedures (TTPs)
- Perform retrospective hunts across historical data when new threats emerge to determine whether indicators of compromise (IOCs) were previously present
- Continuously evolve detections and investigations based on emerging threats

Exposure-informed hunting

Threat hunting should incorporate forensic and real-time data from across your environment to identify suspicious activity that may otherwise go unnoticed. By reviewing authentication events, network activity, remote access tools, cloud storage applications, and other indicators of risk, MDR teams can uncover attacker behavior that may have bypassed automated detection.

Look for providers that can:

- Analyze forensic and real-time telemetry to identify suspicious activity across endpoints, networks, and user accounts
- Investigate unusual authentication events, remote access activity, and external connections that may indicate compromise
- Identify suspicious processes and behaviors associated with reconnaissance, persistence, or lateral movement
- Review indicators that may reveal unauthorized access, misuse of legitimate tools, or other signs of attacker activity

Incident-driven hunting

Threat hunting should extend beyond alert investigation and continue after suspicious or malicious activity is discovered. When a threat is identified, MDR providers should conduct targeted hunts to determine scope, identify related activity, and uncover additional indicators of compromise (IOCs).

Look for providers that can:

- Conduct targeted hunts against specific assets, users, or asset groups following an investigation
- Expand investigations to identify related attacker activity across the environment
- Search for evidence of persistence, lateral movement, or post-exploitation activity that may not have triggered alerts
- Produce actionable findings that improve detections, strengthen response efforts, and reduce the likelihood of future compromise

KEY QUESTIONS AND CONSIDERATIONS

- Does your provider leverage the right technology to execute real-time, reactive, proactive, and targeted hunts?
- How does the provider leverage threat intelligence to identify emerging threats and guide threat hunting activities?
- How often are proactive threat hunts performed?
- What tool does the provider use to hunt? Is that tool available for use by your team, as well as the MDR provider?
- Are you able to request threat hunts based on what's targeting your location, industry, or business specifically?
- How does the provider investigate suspicious authentication activity, network behavior, remote access activity, and other indicators of compromise across the environment?
- What type of reporting is delivered after each hunt?
- When new threats are discovered, how does the team do targeted threat hunts?
- How are threat hunting findings translated into improved detections, remediation guidance, and measurable security outcomes?
- Should a hunt uncover an active compromise, what is the process to eradicate that threat? Does the MDR service include Incident Response Consultants, or are you expected to maintain a retainer?

8. PROCESS AND SERVICE EXPECTATIONS

When it comes to the actual process and service, how can organizations know their MDR will help them respond faster and build resilience for the future? A good MDR service excels at the following:

Deployment and onboarding

Every security organization is different, so it stands to reason that MDR provider onboarding should be customized to each client. Many organizations look for fast time to value, looking for their managed security provider to quickly enable them to deploy the necessary cloud-based or on-prem technologies and begin actively monitoring within the first couple of months of the service. Of course, baselining an environment takes time, but the quicker providers are able to get their new customers into their service delivery the better.

Look for service providers who will start protecting you as soon as you start the process, rather than waiting until everything is complete to begin delivering value. You're looking to buy into a service that extends your team, protects your environment around the clock, and saves you time.

Security posture assessment

Before you begin your service, understand how your MDR provider will ensure you're not compromised. Otherwise, they could be pointing the finger back at you. A compromise assessment should utilize a similar approach and methodology as threat hunts to spot known and unknown threats in your environment and ensure you're starting out with a clean baseline.

Metrics

To justify your MDR purchase, you'll need more than a brief alert notification when something happens. That's where detailed incident reporting comes in, down to the alerts by disposition, mapping to MITRE ATT&CK Framework, incident rebuilding, timeliness, detailed mitigation and remediation recommendations, and detail around affected assets, accounts, and their relevant IOCs. This provides your team — as well as your C-Suite — the analytics that prove your MDR partner's value.

All this integration and scale adds up to a future where teams feel confident in a consolidated approach from their SecOps partner. The future isn't buying more and more tools, it's your team, supercharged with the right partner to help them succeed.

KEY QUESTIONS AND CONSIDERATIONS

- How quickly can the MDR be onboarded and my team trained to understand how it works and where we come in?
- Is threat intelligence derived from research, previous investigations, monitoring findings, and third party sources?
- What baseline assessment is done at the start of the service to make sure you aren't already compromised?
- What detail can you regularly expect from the provider after an investigation? How do you receive that information, and at what cadence?
- Does machine learning eventually establish benchmark metrics for detection within your environment that would enable future automated response?
- Does the service provide at-a-glance summary data about outcomes?

EFFECTIVELY BUILD CYBER RESILIENCE WITH RAPID7 MDR

Put simply, MDR was broken. It focused too heavily on reacting to attacks and not enough on reducing the conditions that allow them to happen in the first place. Building a resilient security program requires more than 24x7 monitoring. It requires an operating model that helps organizations understand their exposure, prioritize risk, act before attackers can exploit weaknesses, and respond rapidly when threats emerge.

Rapid7's MDR brings together exposure management, detection and response, AI, and human expertise, delivering a preemptive security approach designed to reduce risk before it becomes disruption. It's the only MDR on the market recognized by leading analysts for these very components.

Exposure management gives organizations visibility into the assets, identities, vulnerabilities, misconfigurations, and attack paths that create meaningful business risk. Rather than overwhelming teams with endless findings, exposure management helps prioritize the risks attackers are most likely to exploit.

Detection and response provides continuous monitoring, threat hunting, investigation, containment, and response across your environment. By connecting detection activity with exposure context, analysts gain a deeper understanding of which threats matter most and how they relate to the organization's broader risk profile.

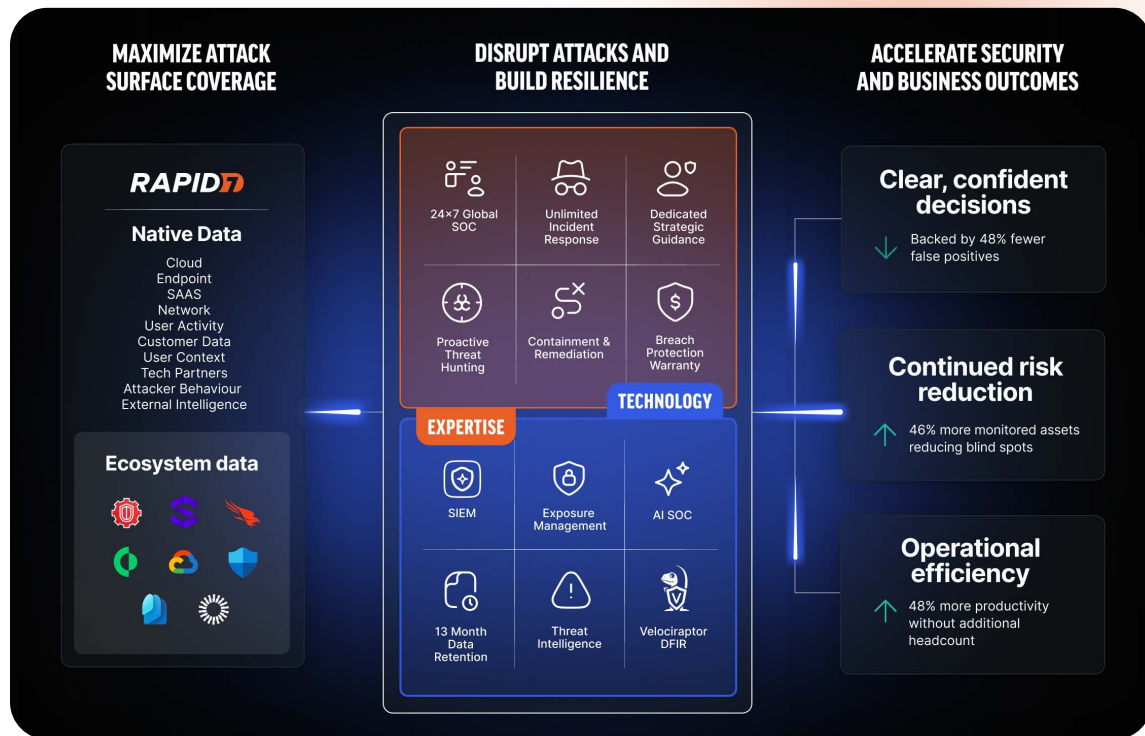
AI-enabled operations help security teams work at the speed modern threats demand. AI reduces noise, correlates signals across complex environments, accelerates investigations, and surfaces the activity most likely to require attention. The result is greater efficiency, faster response, and more time spent on meaningful security outcomes.

Human expertise remains firmly in the driver's seat. Technology can identify patterns and accelerate workflows, but security decisions require judgment, experience, and accountability. Rapid7's analysts validate threats, assess business impact, guide remediation, and help organizations make informed decisions when it matters most.

The result is a security program built around resilience rather than reaction. Rapid7 MDR lets organizations identify and reduce exposure, disrupt attacker paths, respond faster to threats, and maintain confidence in an environment where risk is constant.

EXPERIENCE THE FULL LIFECYCLE OF PREEMPTIVE SECURITY:

Outcomes through end-to-end defense



ABOUT RAPID7

Rapid7, Inc. (NASDAQ: RPD) is a global leader in AI-powered managed cybersecurity operations, trusted to advance organizations' cyber resilience. Open and extensible, the Rapid7 Command Platform integrates security data, enriching it with AI, threat intelligence, and 25 years of expertise and innovation to reduce risk and disrupt attackers. As a recognized leader in preemptive managed detection and response (MDR), Rapid7 unifies exposure and detection to transform the cybersecurity operations of more than 11,500 customers worldwide. For more information, visit our [website](#), check out our [blog](#), or follow us on [LinkedIn](#) or [X](#).

RAPID7

SECURE YOUR

Cloud | Applications | Infrastructure | Network | Data

ACCELERATE WITH

[Command Platform](#) | [Exposure Management](#) |
[Attack Surface Management](#) | [Vulnerability Management](#) |
[Cloud-Native Application Protection](#) | [Application Security](#) |
[Next-Gen SIEM](#) | [Threat Intelligence](#) | [MDR Services](#) |
[Incident Response Services](#) | [MVM Services](#)

SECURITY BUILT TO OUTPACE ATTACKERS

Try our security platform risk-free -
start your trial at rapid7.com



© RAPID7 2026 V1.0