deepwatch

Selecting the Right Managed Detection and Response (MDR) Provider

AN MDR BUYER'S GUIDE TO IMPROVED SECURITY OUTCOMES

Table of Contents

Introduction

Managed Detection and Response (MDR) is changing the way businesses address their security risks, and the move to MDR is projected to continue for years to come. The tipping point on the long-predicted shift, according to Gartner Research, comes **in 2025, when over 50% of organizations will have adopted some level of MDR service** for 24/7 monitoring, threat detection, and incident response.[1]

What's behind this shift to outsource the critical functions of detection and response to a Managed Security Service provider?

Several reasons are driving the demand for MDR services into the future. These trends are market forces behind the MDR movement:

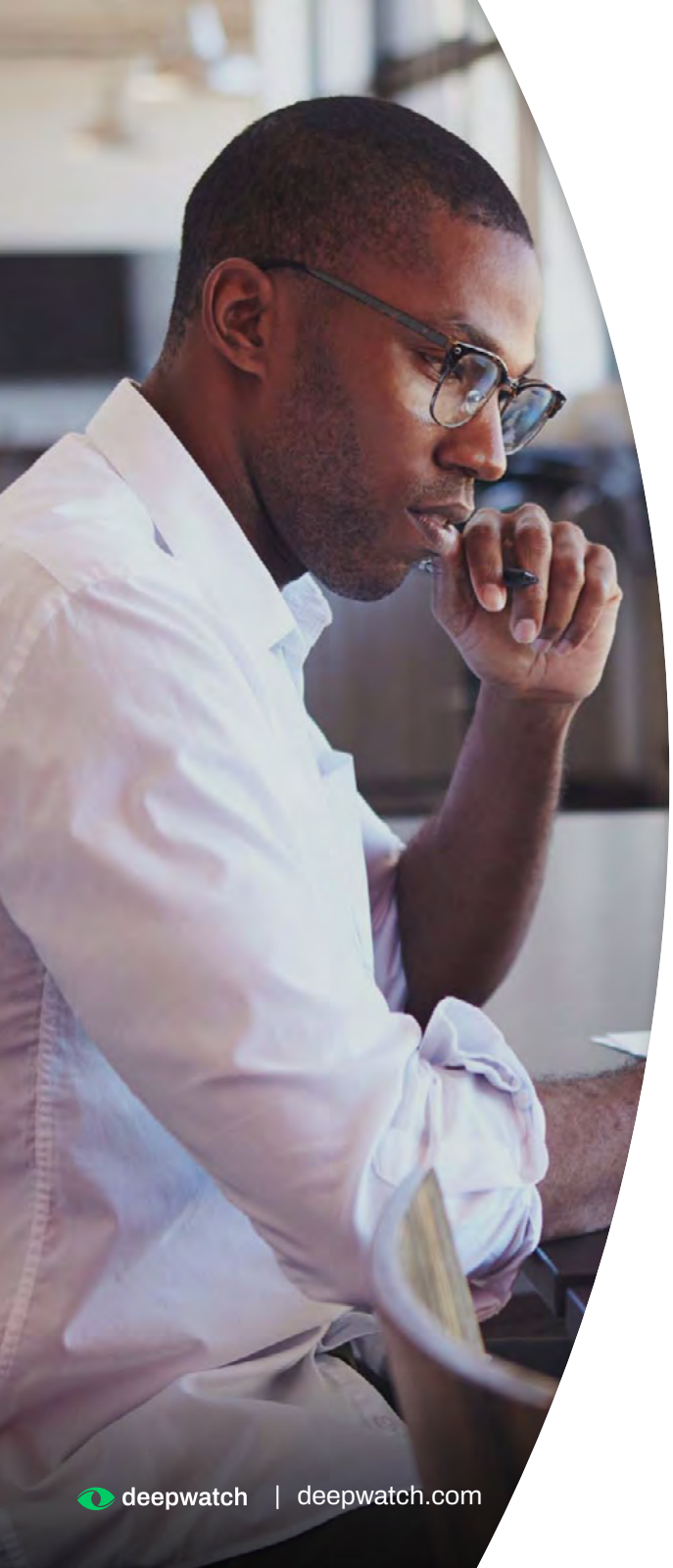
- **Experienced cybersecurity talent is in-demand** and hard-to-hire.
- **Transformative technology and legacy systems co-exist** on the same network.
- **Zero-day and unmitigated vulnerabilities will continue** to be exploited by threat actors amassing footholds.
- **The distributed workforce and work-from-home trends will remain** part of the way business is conducted in a post-pandemic world.
- **Cloud security challenges will continue as companies migrate** on-premises systems to hybrid and multi-cloud environments.
- **Threat actors will continue to evolve TTPs**, attack "non-traditional" targets, and taking upon the easiest pathways to make a profit (i.e., ransomware-as-a-service).
- **100% threat prevention is not possible today**; therefore, security programs need to be staffed and ready to detect threats and respond to attacks around the clock.

Business leaders have increased their investments in security operations. It's critical to evaluate how that return is delivering on outcomes, especially when delivered by a Managed Detection and Response provider.

This MDR Buyer's Guide is focused on the outcomes that security leaders can expect from their Managed Detection and Response provider to support and improve the overall security program.

Focus on Outcomes:
What an MDR Provider Can (and Should) Do

According to a recent survey of security leaders, 94% not using MDR today are planning to evaluate MDR within the next 18 months.[2]



MDR Services Basics

Managed Detection and Response is a "fully managed security service that includes the application of advanced security analytics, proactive threat hunting, and incident response investigative capabilities along with security automation orchestration (SOAR) for automated, manual, and on-demand response actions based on predefined and custom escalation workflows."[3] - Forrester

That same study found that 72% of security leaders that are using MDR report reducing their mean time to resolve attacks by 25-100% faster than before MDR.

With threats increasing and security teams understaffed, MDR services have become a viable option for companies of all sizes. In many cases, security risks are just as important for small companies as larger ones. **The advantage of an MDR solution is the opportunity to get the right amount of technology managed by security experts focused on the best outcomes.**

Services delivered within the "Managed Detection and Response" category can come from a mix of technologies and engineered solutions. In its broadest definition, MDR is holistic and comprehensive as it includes security experts, technologies, and log sources. **MDR provides a comprehensive view across the security environment** that one endpoint agent or SaaS cannot deliver alone.

What drives the evaluation of an MDR provider? Companies choose to invest in MDR for expertly-managed detection and response services to fulfill duties within the greater security operations program. **The triggers for the MDR investment can be anything from a recent breach, regulatory requirements, a company acquisition, or cybersecurity reports requested by the board.** These triggers are important, as are budget and executive alignment. Therefore, a focus on the security outcomes provides clarity when selecting the right MDR provider for scalable security operations that best support the overall security of the organization.

"MDR services are designed to reduce the time to detect, as well as the time to respond to threats… Additional security operations functions, such as vulnerability management and log management, which are typically offered by managed security service providers (MSSPs), have emerged to complement the threat monitoring, detection and response offerings."[4]

- GARTNER

Achieve Four Outcomes with the Right MDR Provider

As with any technology purchase, maximizing the value realized from an investment in an MDR service provider and their offerings should be top of mind. Rather than providing a list of technical capabilities to consider, **this MDR Buyer's Guide describes the most advantageous security and business outcomes** that can be measured and reported to executives, the board, investors, employees, and shareholders alike.

These outcomes include:

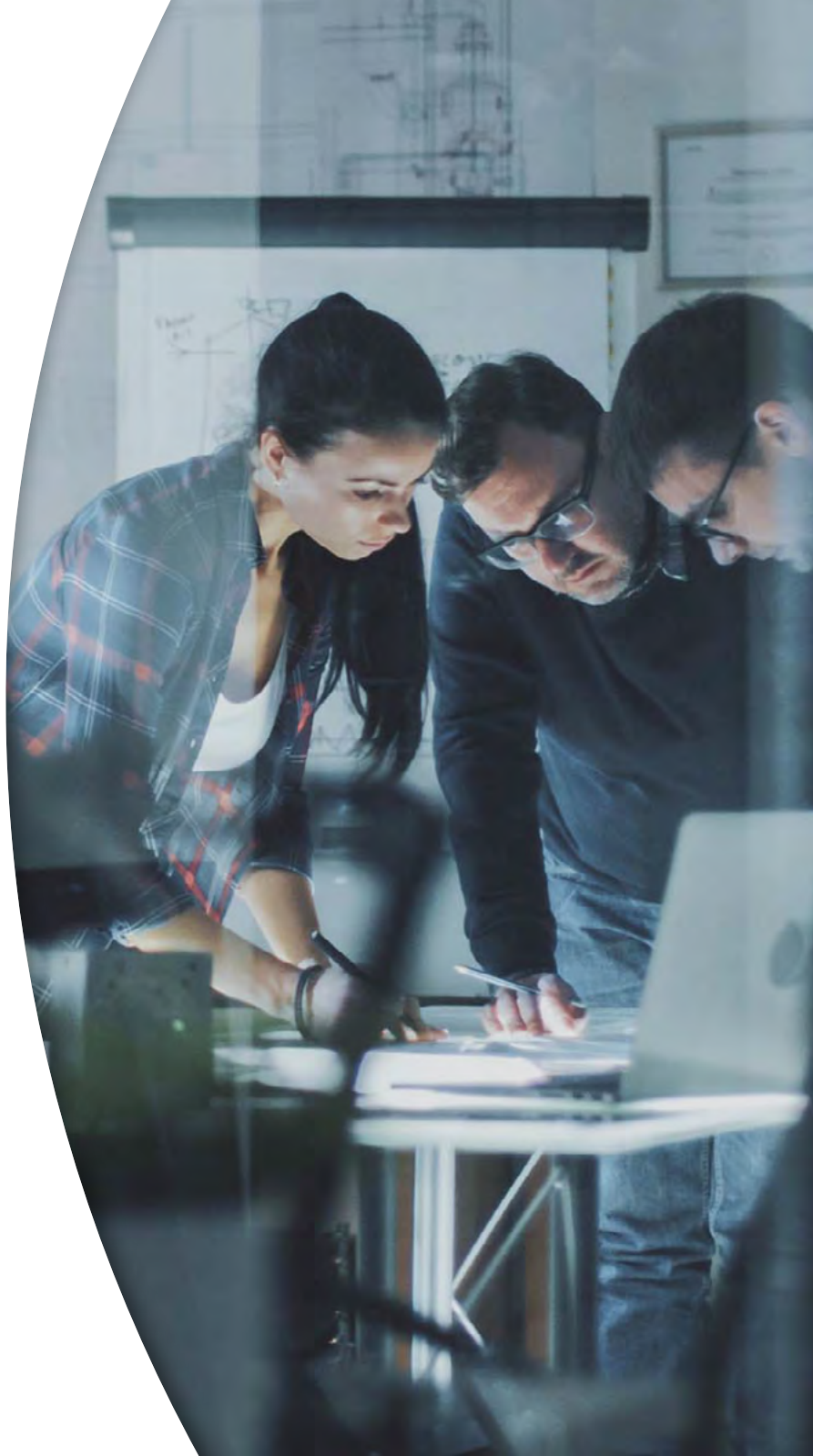
- **Strengthen the Ability to Monitor, Detect, and Respond** to security incidents 24/7/365;
- **Improve Security Posture** with a maturity model that provides recommendations, peer and industry benchmarks, and ability to measure progress;
- **Focus the In-house Team on the Overall Security Program** to manage strategic security initiatives;
- **Increase the Value from Security** investments and tools.

Strengthen Threat Detection and Response Capabilities

A modern cybersecurity program provides security leaders visibility throughout their environment to identify attacks and respond. Security experts monitor the network, including cloud and API sources, and investigate security alerts. **If a threat is detected, the security team responds to minimize the impact of the security threat as soon as possible.**

What type of MDR provider can offer the expertise, services, and technology needed to achieve these outcomes?

First, an MDR service provider worth considering will be cloud-capable, with experts watching and ready to respond 24/7/365 with clear escalation paths. This approach provides visibility and facilitates rapid incident response to minimize threat dwell time.



Dwell Time Is Money

287 days

In 2021, it took an average of **212 days** to identify a breach and an average **75 days** to contain a breach, for a total lifecycle of **287 days**.

$4.87m

The average cost of a breach with a lifecycle over **200 days**.[5]

WHAT ELSE IS KEY TO STRENGTHENING DETECTION AND RESPONSE?

There is an essential set of MDR service provider capabilities proven to help companies manage the most challenging security risks in today's landscape.

Threat Detection

WHY IT WORKS

Use of the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations

The MITRE ATT&CK® framework is a leading method for security teams and MDR providers for **threat modeling and to map use cases** to established TTPs (Tactics, Techniques, and Procedures) in order to facilitate rapid incident response.

Threat Intelligence used for advanced detection and security risk mitigation, from a variety of leading resources, applied by experts in threat operations, to enhance MDR services

Expert-led curation, application, and operationalization of threat intelligence managed by the MDR provider **offers visibility into real-time insights, and accelerates response times**

Proactive Threat Hunting that leverages TTPs, Threat Intelligence, and IOCs, to create hypotheses in order to investigate and identify abnormal activity that may be malicious

Today's attackers have developed advanced TTPs engineered to evade protective controls. An MDR service provider that includes Threat Hunters – experts who hunt for security threats proactively – can **augment signature-based detections and provide insights for further investigation**. Threat hunting can be utilized to fill security control gaps within the organization and to provide a feedback loop to improve existing controls.

Use of ML, analytics, and other advanced technologies to correlate data, assign priority to alerts, and provide business context for evaluating security incidents

A security team's Mean Time to Respond (MTTR) is shorter when defenders are focused on the most actionable alerts, and **integrated ML facilitates real-time alerts** when every second matters.

Response

Standardized Playbooks for procedures used in responding to events that are discovered during threat detection

24/7/365 Security Monitoring for security events conducted by human analysts specifically assigned to your environment supported by top quality technologies and automation, who investigate alerts, escalate incidents when required, and manage cases and tickets for the customer

WHY IT WORKS

Using standardized playbooks that contain the procedures, standards, and anticipated results from incident response helps **reduce threat dwell time** and time to close the event. The playbooks should be organized according to the MDR provider's alert triage and workflow integration with the in-house security team.

Trained security analysts monitoring the network ensure threat actors are identified and responded to fast. The right MDR provider will have a team of **experienced security analysts watching the network 24/7** to ensure any abnormal activity that may indicate a threat is quickly identified for further investigation and escalation if needed.

Continued on next page

Response Continued

Endpoint Detection and Response (EDR) for real-time endpoint monitoring, mitigation, and remediation capabilities. EDR solutions should leverage technology from leaders in the EDR space, to automate and orchestrate response activity on endpoints

WHY IT WORKS

EDR technology captures data from endpoints on the network and provides remote incident response capabilities, including the ability to contain, isolate, and remove threats. When leveraging EDR as a service, a team of experts **manages the EDR technology to detect and respond to threats on endpoints** within the customer environment.

A NOTE ON EDR VS. MDR SERVICES

Threat detection on the endpoint is critical. It is not unusual for attacks targeting endpoints to evade detection, prevention or control solutions and cause problems on the endpoint. Managed Detection and Response supports a broader, defense-in-depth strategy. Endpoint Detection and Response (EDR) offerings and technology tend to focus solely on the endpoint for detection and control. With integration of endpoint technology, the right MDR provider will provide the ability to review and utilize all embedded capabilities within the security architecture beyond a single line of defense at the endpoint.

Vulnerability Management (VM) to ensure a full understanding of the assets in the environment and their susceptibility to attack by actors exploiting known vulnerabilities. VM directs mitigation and patching efforts efficiently

Vulnerability management is a critical component within the greater security program. Maintaining a proactive VM program has become an important way to **identify and patch security issues fast**, as threat actors scan the internet to prey upon targets with unpatched systems and assets.

Improve the Organization's **Security Posture**

Security leaders need in-depth insights to quantify and map their security risks to business goals in order to create a path to a more mature security posture. **Typical methods may involve a risk management framework, like NIST CSF, and/or a security maturity model.** These methods provide ways to quantify risk and prioritize what needs to be addressed, and what can be de-prioritized.

An MDR provider should be able to put some type of measurement or methodology in place to help the organization establish a baseline of security maturity during the on-boarding process. Going forward, the **MDR provider should offer recommendations to help continue improvement in this measurement year over year.**

Proven methods that strengthen security posture when working with an MDR service provider include:

	HOW IT IMPROVES SECURITY POSTURE
A Methodology to Measure Security Maturity of the organization's use of log sources and technology based on cyber resilience best practices, the current threat landscape, and criticality of security risks to the business	Maturity modeling can benchmark a security posture against industry peers and provide a well-defined roadmap to continuous improvement. This can help companies **realize cost savings, fill security gaps, and improve key metrics** with the MDR provider.
Prioritization of Data Sources available in the environment, with recommendations on high-value, critical data sources, and assurance that all data sources are tuned for maximum security fidelity	Not all data sources provide the same value. The wrong data sources can lead to alert fatigue, increased storage costs, and wasted time investigating false positives. Data sources should be selected to streamline identification and detection of **confirmed threats that require rapid response.**
24/7/365 Access to Security Experts and Best Practices to address gaps in technology, policies, and procedures	An in-house security team can move the security needle by working with the MDR provider to **address identified issues, manage cases, and implement recommendations** on the in-house team's schedule.
Use of Proprietary and Comprehensive Content Libraries and response playbooks that are kept up-to-date	The right MDR provider will bring a robust content library to curate use cases for advanced threat detection, and response playbooks to coordinate incident response **with the in-house team.**

Mature the Security Program with the **In-House Team**

One of the universally identified issues in every security team is the difficulty hiring and retaining security talent—businesses have experienced a **cybersecurity skills gap** for decades. **Security operations roles, such as security analysts, report extremely high burnout rates, causing them to leave critical SecOps roles needed for 24/7 security operations.** Once security analysts leave, companies may ask their senior resources to perform those critical security tasks, which often further exacerbates staffing issues, such as declining job satisfaction and increasing employee turnover rates.

A good MDR solution won't simply bring another tool to an overworked and understaffed security team. **The right MDR provider will bring an expert team of focused resources** who will remove the load of those activities from the in-house team's plate.

This frees up the in-house team to level-up the overall security program. With more hours in the week working with experts, the in-house team gains on-the-job experience as they measure their progress with the extended MDR team. Ultimately, the right MDR provider can help positively influence job satisfaction and employee retention of expensive, in-demand security talent.

SKILLED CYBERSECURITY EXPERTS NEEDED!

In a recent survey, **43% of CISOs** noted a **lack of skilled staff** as their biggest stumbling block in **rapid incident detection and response**.[6]

The following essential MDR service provider capabilities provide critical support for the security operations center (SOC) and quantifiably relieves the in-house team, giving critical time back to focus on overall strategic security initiatives.

HOW IT HELPS THE IN-HOUSE TEAM

A quality MDR provider has cybersecurity experts on staff who know how to interpret and correlate data and tune Security Information and Event Management (SIEM) technology. These experts work on customer environments to **improve security fidelity and help reveal true threats**. This expertise helps the in-house team prioritize and triage millions of daily security alerts.

Assignment of an Experienced Security Team to work with the in-house staff on a daily basis: senior security individuals with years of experience working in security operations, and invests in on-going training and education for their teams

Establishment of a Clear Escalation Path that makes it clear when threats are discovered which remediation steps can be taken by the MDR provider and instances where a more consultative approach together with the customer is needed

When a security incident occurs, it is important that the in-house team **knows who to call, what the communication flow is, and how incidents will be responded to** and resolved quickly.

HOW IT HELPS THE IN-HOUSE TEAM

24/7/365 Security Monitoring Services by Experts working as an extension of the in-house security team, providing up-to-date contextual awareness of the security environment and supporting optimal alert fidelity

The in-house team has other security initiatives they need to support in addition to prioritizing which security events require investigation and response every day. The MDR service provider can **investigate alerts, tune the SIEM, and manage security monitoring around the clock** so the in-house team can focus on what's most important, **versus chasing down false positives.**

Customer Portal with Mobile Application to track the MDR services' activities, manage cases, generate reports, get threat alerts, and communicate with assigned security experts real-time (i.e., Slack channel)

Daily communication via multiple channels **ensures transparent collaboration between the MDR provider's team** and the in-house team, and validates that the context of the customer's environment
is understood.

Sufficient Levels of Assigned Staffing to ensure the MDR provider is focused on the customer environment 24/7/365, and isn't diverting a named team's time elsewhere

The extended team of experts from the MDR provider is assigned talent focused on the customer's security environment. This means that in-house staff can **count on these specific experts to monitor the security environment with 24/7 eyes-on-glass, and are always accessible to communicate real-time** with the customer.

Increase the Value from Security Investments and Tools

Businesses look for a demonstrably strong ROI on any investment in security solutions—and an MDR service that includes technology is no exception. That includes:

- **Paying the right amount** as needed at any given time, with the **ability to scale services** when requirements change;
- **Fully leveraging the investments already made** in technology, with the **ability to benefit from new features** as they are introduced.

DISAPPOINTING ROI?

Despite spending on average $18.4M on security investments, a recent survey of cybersecurity professionals found that only 39% of respondents felt they were getting the full value from those investments.[7]

There are some key attributes to look for in an MDR service provider to realize better ROI from security investments.

Integration of Best-in-Class Security Products, such as a SIEM, **Security Orchestration Automation and Response (SOAR)** solution, and other tech within the existing security stack

WHY IT IMPROVES ROI

An MDR service provider can leverage many of the investments already made by the customer to get more value from those tools. The right MDR service provider can **streamline data into one security operations platform for improved visibility, enriched use cases, and coordinated response.** When unnecessary or duplicative technologies are up for renewal, the customer can work with their MDR provider to streamline investments.

Unmetered Contact and Assigned Support with a consistent and predictable pricing model

An MDR partner has a vested interest in helping customers make security improvements; a true partner wants to help their customers stay ahead of evolving threats. A long-term partnership should be focused on **comprehensive services that improve customer outcomes, not maximizing billable hours** to provide capabilities that should be part of the MDR service (i.e., SIEM tuning, 24x7 SOC, threat hunting).

WHY IT IMPROVES ROI

Right-sized Security Services that Scale according to the business requirements and budgets today, with the flexibility to expand as businesses grow—especially in the cloud

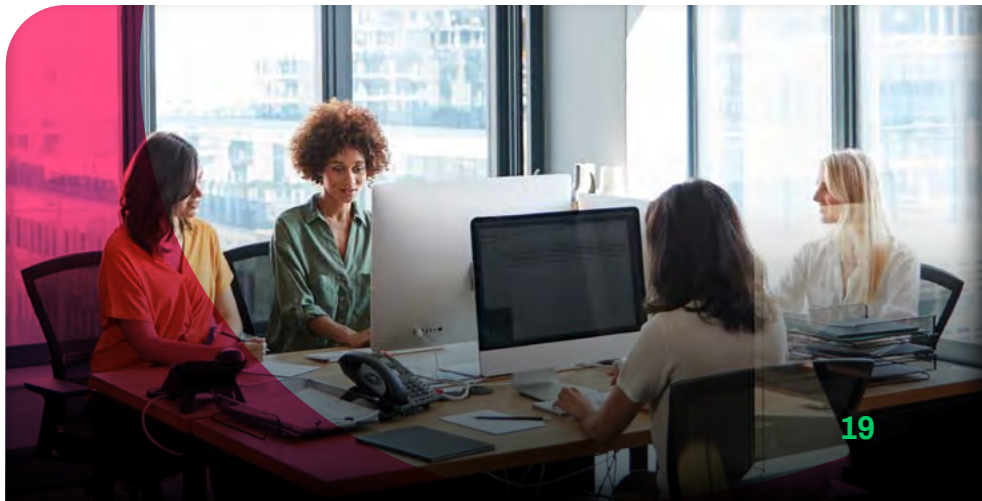
Businesses grow and staffing talent will shift. An MDR service provider should **make it easy and cost effective** for customers to add and subtract technologies and assets as the business needs change.

Transparency into the MDR provider's detection and response services through independent verification (e.g., independent access to SIEM)

Quality assurance is critical when it comes to confirming MDR services are performing optimally and that **the customer's requirements are being met.**

Strong Reporting Capabilities offer the business a pathway to measure and report back to executives, the board, and regulatory agencies how the MDR relationship supports the security program

One of the benefits of taking on an MDR service provider is getting the assistance needed to more easily and **clearly communicate the value of MDR** to executives and the board.



WANT TO LEARN MORE?

MINIMIZING RANSOMWARE IMPACT: 3 STEPS WITH MDR

Download Now

SEVEN QUESTIONS TO ASK YOUR MSSP

Download Now

GET THE LATEST THREAT INTELLIGENCE AT DEEPWATCH LABS

View Now

Taking the Next Step

This guide presents an approach to selecting the right MDR service provider based on the security and business outcomes that are most critical to an organization. By taking a holistic view of security outcomes, an organization can elevate their security program and take it to the next level by partnering with a trusted MDR provider that supports these outcomes. Using a **cloud-based platform that combines advanced analytics, threat intelligence, detection, and automated response capabilities together with tailored guidance from security experts,** the right MDR provider will offer a new approach to managing cybersecurity.

Improved security outcomes are within reach with proven technology and experts you can trust. Take the next step on your MDR journey by visiting www.Deepwatch.com or by reaching out to us at sales@Deepwatch.com.

READY FOR THE NEXT STEP ON THE MDR JOURNEY?

See how Deepwatch **MDR services** work for businesses across industry verticals and all sizes. Contact us for a customized MDR solution design at **Deepwatch.com/contact-us**.

deepwatch

ABOUT DEEPWATCH

Deepwatch helps secure the digital economy by protecting and defending enterprise networks, everywhere, every day. Deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts who monitor, detect, and respond to threats on customers' digital assets 24/7/365. Deepwatch extends security teams and proactively improves cybersecurity posture via its Squad delivery and patented Security Maturity Model. Many of the world's leading brands rely on Deepwatch's managed detection and response security.

Visit www.Deepwatch.com or reach out to us at sales@Deepwatch.com.

SOURCES

[1] Market Guide for Managed Detection and Response Services, Gartner, August 2020: https://www.gartner.com/en/documents/3989507/market-guide-for-managed-detection-and-response-services

[2] Managed Detection and Response, Enterprise Management Associates, July 2020: https://www.ibm.com/downloads/cas/YNKDLKBD

[3] Now Tech: Managed Detection And Response Services Providers, Q4 2020, Forrester, December 2020: https://www.forrester.com/report/Now-Tech-Managed-Detection-And-Response-Services-Providers-Q4-2020/RES161762

[4] Market Guide for Managed Detection and Response Services, Gartner, August 2020: https://www.gartner.com/en/documents/3989507/market-guide-for-managed-detection-and-response-services

[5] 2021 Cost of a Data Breach Report, IBM: https://www.ibm.com/security/data-breach

[6] More Than Half of CISOs Around the World Concerned About the Cybersecurity Skills Gap, Cyber Security Intelligence, April 2018: https://securityintelligence.com/news/more-than-half-of-cisos-around-the-world-concerned-about-the-cybersecurity-skills-gap/

[7] 53 Percent of IT Security Leaders Don't Know if Cybersecurity Tools are Working Despite an Average of $18.4 Million Annual Spend, Ponemon Study, July 2019: https://www.businesswire.com/news/home/20190730005215/en/Ponemon-Study-53-Percent-of-IT-Security-Leaders-Don%E2%80%99t-Know-if-Cybersecurity-Tools-are-Working-Despite-an-Average-of-18.4-Million-Annual-Spend