HUGHES®
An EchoStar Company

UNLOCKING MDR SUCCESS

A Buyer's Guide to Cybersecurity Resilience

CONTENTS

INTRODUCTION

Cyber threats are escalating. According to research by MIT Sloan, data breaches are now at an all-time high for US organizations. In just the first nine months of 2023, data breaches in the US increased by nearly 20% compared to all of 2022, and organizations around the world have faced similar trends.

The increase in remote working and the proliferation of devices for both work and personal use have only increased cybersecurity risk. Users are working in the office, at home, or, frequently, on the move. Meanwhile, company data can be stored on premises, in the cloud, and on the devices of geographically dispersed employees.

Adding to this complexity are the challenges of dealing with changing regulatory requirements and difficulty in fin ding and retaining talent with cybersecurity expertise. IT security issues are overwhelming in-house IT teams. This is especially true for small- and medium-sized businesses (SMBs) who often lack IT resources able to effectively detect and respond to security threats, making them a primary target for cyber attacks. Cybercriminals are opportunistic and see SMBs as prime targets because they perceive them to have weaker cybersecurity defenses. According to Accenture, 43% of attacks are aimed at SMBs, and only 14% of these businesses are prepared to defend themselves.

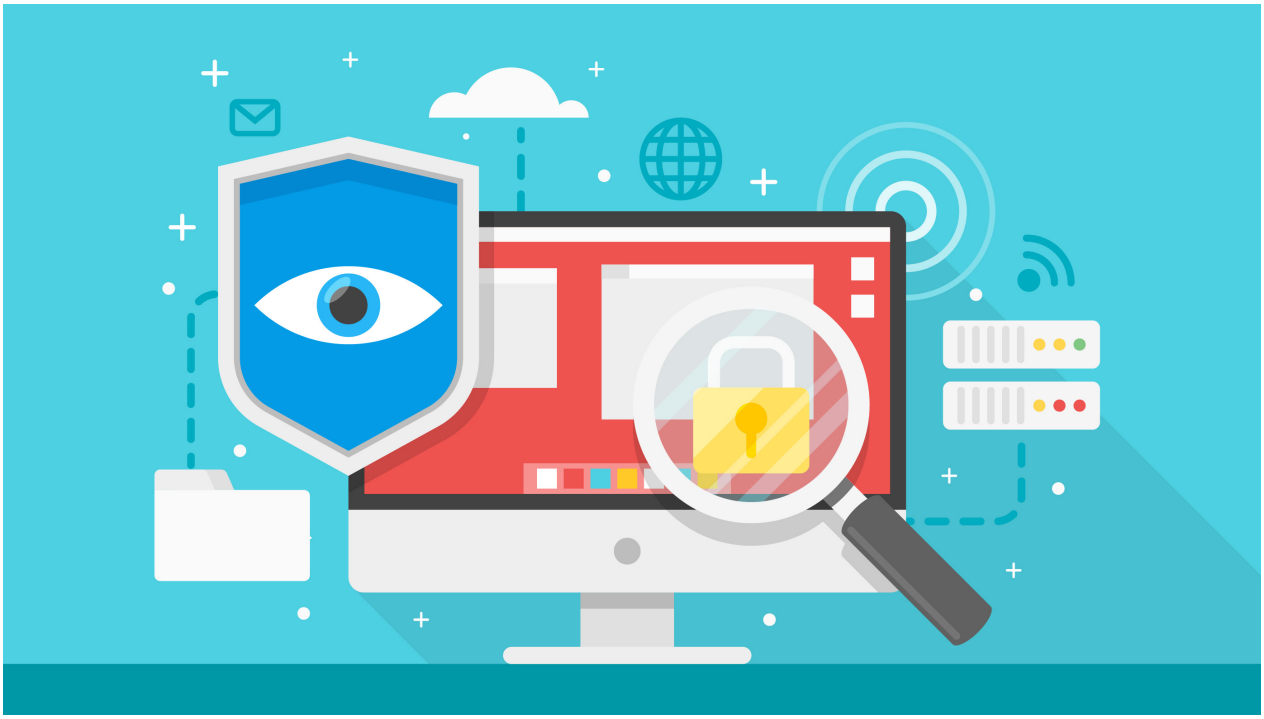
It's impossible to defend without a 24/7 detection and response team. This is why many organizations are relying on Managed Detection and Response (MDR) services to enhance their in-house security operations capabilities.

What is MDR?

Managed Detection and Response (MDR) is a service that provides a business with a team of experts—part of a remote Security Operations Center (SOC)—who use advanced tools to actively monitor the network. The team monitors your organization's cloud services, network traffic, servers, and endpoints; identifies potential security threats; and triggers a response to mitigate those risks before they can cause harm, with the goal to detect and neutralize the threats and prevent similar future occurrences.

Traditional security solutions, such as firewalls, anti-virus software, and intrusion detection systems, typically address only a single aspect of security. Businesses must therefore cobble together protection from disparate piece-parts and ensure they are kept up to date on the latest threats through patches and upgrades. On the other hand, MDR provides a proactive, integrated approach to security that is far more effective.

A Managed Security Service Provider (MSSP) equipped with a 24/7 SOC can implement MDR service to SMBs who may not be able to staff their own cyber professionals or who struggle to keep up with network monitoring activities.



MDR solutions enable your organization to:

- Enhance visibility by continuously monitoring cloud, network, and endpoint activities
- Prioritize incidents by employing detailed threat analysis, human intelligence, and specialized tools
- Utilize comprehensive data to gain contextual insights and make informed decisions
- Reduce costs by eliminating the need to invest in security software, equipment, and in-house staff
- Minimize risk and respond faster to security threats
- Strengthen your security posture and proactively prevent potential cyber attacks

This buyer's guide provides guidance on choosing an MDR solution and MSSP. It includes a comprehensive checklist and complete set of questions to aid you in identifying the company that aligns with your needs and complements your organization most effectively.

With so many MSSPs and MDR solutions available, it can be overwhelming to identify the vendor that best aligns with your requirements, understands your industry, and can assist you in achieving your objectives. The following checklist provides the essential steps to take when choosing the MDR vendor for your needs.

Ten Essential Steps When Choosing an MDR Vendor

1. **Be clear on what problem you are trying to solve**
   It's important to be strategic and clear on what kind of business outcomes you are searching for from an MDR provider.

2. **Define your short-term and long-term security goals**
   Outline the immediate threats that must be addressed now, while looking out for future threats.

3. **Research MDR vendors and identify differentiators**
   Look for vendors with experience that have a proven track record of reliability, quality, flexibility, and technical expertise.

4. **Create your short list and evaluate vendors' capabilities of products and services**
   Look for vendors with all of the security capabilities to meet your needs and goals. Vendor consolidation is a powerful tool that can make managing your security more efficient and leaves less room for error, including gaps or overlap in your security posture.

5. **Assess vendor's ongoing service commitments**
   Ensure the MDR solution includes dedicated resources to assist you on a daily basis and offer adherence to deliverables in the form of Service Level Objectives (SLOs) or similar commitments.

6. **Assess vendor's viability and reputation**
   Examine vendor's financial viability and reputation by reviewing industry accolades, customer feedback, and case studies. Assess the qualifications of professionals delivering the service.

7. **Consider pricing**
   Quality typically commands a higher price, and it also brings more value. Assess the potential business impact and financial costs of a breach against the cost of the MDR solution. A cost-benefit analysis can help companies determine if it is an investment that makes sense for their organization.

8. **Evaluate contract terms carefully**
   Review the terms and conditions to ensure it offers flexibility, safeguards your interests, clearly outlines deliverables, and specifies how services will be assessed, standards upheld, and recourse options if they fall short.

9. **Request a demonstration**
   Request a demonstration of the MDR solutions to assess their functionality and determine if the core features meet your requirements. Some providers may also have trials that can help you see the value they bring to the table.

10. **Ask for references**
    Nothing is more important than speaking to existing clients about their experience working with the vendor.

Selecting the Right MDR Solution

To gauge the effectiveness of an MDR solution, it is crucial to evaluate all the associated cybersecurity products, services, and processes. The MDR solution should be comprehensive and combine cutting-edge technology, experienced security analysts, and real-time threat intelligence to detect and respond to cyber threats. An experienced MDR provider will skillfully blend technology with human intuition to elevate detection capabilities. Here are key capabilities that should be included in the MDR:

Security Operations Center (SOC)

A SOC delivers a full-time operational team 24/7, armed with tools and technologies for real-time threat detection and mitigation. Standing up a SOC can cost millions of dollars, and millions more in recurring costs annually to run it. Additionally, recruiting, hiring, and training an IT security team is often too cost prohibitive for SMBs. While each SOC team is unique, it's important that it include the following key roles:

- **Security analysts** who serve as cybersecurity first responders. They are on the frontlines identifying and reporting threats and implementing changes to protect the network and the organization.
- **Security engineers** are the software and hardware specialists who deploy, maintain, and update all the tools, technologies, and systems involved in securing the critical infrastructure, as well as documenting the security protocols.
- **The SOC manager** directs the team of analysts and engineers and orchestrates any responses to major security threats.

Security Information and Event Management (SIEM)

SIEM collects event log data from a range of sources to identify activity that deviates from the norm with real-time analysis to drive action. An advanced SIEM platform dashboard should provide a clear view of your network's real-time posture and provide monthly executive summary reports detailing trends, updates, improvements, and daily and weekly critical observations. SIEM combined with a SOC can combat cyberattacks 24/7 all year round.

Endpoint Detection and Response (EDR)

Organizations, regardless of size, are confronted with an expanding array of devices, each contributing to their vulnerability to cyber attacks. EDR continually monitors end user devices to identify threats, like ransomware and malware. It is important that the MDR provider offers endpoint protection and has the expertise that is needed to navigate today's complex threat landscape.

Quality MDR providers should be focusing not only on the detection and response, but also the prevention. A prevention tool commonly paired with EDR is Endpoint Protection (EPP), something besides a firewall that helps scan and filter data before you allow it on your network in the first place. It's hard to detect every threat and respond appropriately if you let them in through the front door. Preventative measures can help drastically reduce the strain on the SOC team and your own internal IT/security staff.

Network Monitoring

Effective network monitoring provides network administrators with real-time insights necessary to determine whether a network is operating optimally. It provides real-time, end-to-end visibility needed to identify early indicators of compromise associated with an active cybersecurity event.

A robust MDR solution should include Network Detection and Response (NDR) capabilities to provide a holistic perspective on all enterprise devices, entities, and network traffic, continuously monitoring and analyzing real-time traffic flow across the network. NDR provides context-rich visibility, not only at the entry and exit points, but also for lateral movements across the network, strengthening network monitoring, detection, and prediction capabilities across cloud-native or hybrid-cloud network environments. NDR has the ability to protect any device that is connected to the network, including IoT and OT devices that traditional EDR cannot cover.

Threat Detection Capabilities

An effective MDR solution should have the ability to detect both known and unknown threats, utilizing advanced threat technology within NDR and EDR, along with human expertise.

NDR and EDR solutions leverage a combination of network traffic analysis, protocol analysis, signature-based detection, endpoint monitoring, behavioral analytics, indicators of compromise, threat hunting, and human expertise to detect and respond to cybersecurity threats within a network environment and at the endpoint level.

By providing comprehensive visibility into network and endpoint activity and identifying malicious behavior in real-time, these technologies help organizations strengthen their security posture and defend against advanced cyber threats.

Incident Response

The MDR solution should have an organized and strategic approach for identifying, investigating, and responding to potential threats, to minimize damage, recovery time, and total costs. For example, when NDR sees a possible threat, it can automatically take action by quarantining the problematic area and immediately notifying the SOC.

A well-structured incident response process requires planning, skills, coordination, and automation to ensure a prompt and precise response, and should work together with your business continuity and disaster recovery plans.

An incident response plan might entail the following steps:

1. An analysis of the network logs to identify and determine the extent of the breach
2. Isolation of the compromised server and strengthening access controls
3. Removal of the unauthorized user and a thorough review of all systems
4. Data backups are restored to recover lost or compromised data
5. Systems are gradually brought back online, while documenting lessons learned and recommendations
6. Notify all relevant stakeholders, including affected customers, of the incident

Having these items in place takes a lot of staffing power, expertise, and discipline. An experienced MDR provider will adhere to these policies and explain how they can help you through each step.

Integration Capabilities

Your organization may depend on tools from various vendors to complete your security infrastructure, resulting in several standalone solutions with minimal integration or shared telemetry. This hampers the sharing of data and intelligence, preventing a unified, context-rich view of all threats across the business, making it challenging to effectively mitigate risks at scale. An efficient MDR solution will integrate across security stacks, simplifying threat detection, prioritizing incident response, and enhancing productivity for security analysts.

Managed Services Commitment

Evaluate the MDR provider's commitment to service delivery, including the availability of 24/7 support and the comprehensiveness of its service-level agreement (SLA). For example, if there is a breach or potential threat, the provider should notify the customer within a specific amount of time, such as 15 minutes or less. The service level objectives should also include daily,

weekly, and monthly critical observation reports that provide a quick snapshot of what is going on each day, week, and month.

When choosing an MDR provider, make sure you understand how they integrate operationally with your existing workflow and what forms of communication will be used, such as portal, email, text messaging, and phone or video calls.

Customized Remediation Response

Assess whether the provider offers tailored products and comprehensive threat remediation and mitigation services to address the unique characteristics of your business environment. The capacity to integrate data from diverse sources and offer comprehensive customized MDR coverage throughout your business is paramount.

Depth and Breadth of Technology

Modern MDR solutions rely on innovative technologies, including artificial intelligence (AI), machine learning (ML), and threat intelligence, to continuously monitor and analyze traffic and events for signs of malicious activity. If a threat is detected, the MDR provider's security analysts must be able to immediately investigate and respond to the threat, minimizing the risk of a breach and the impact of an attack. Having the latest threat detection technologies, coupled with 24/7 monitoring and managed services, is what paves the way for protecting the network and the business.

Partnering with the Right Managed Security Service Provider

Partnering with an MSSP gives you immediate access to cybersecurity expertise, reducing the risk of cyber threats and high costs of hiring, retaining, and training cybersecurity staff. According to a research study by Stott and May talent firm, it can take anywhere from three to five years or longer for security staff to develop real cybersecurity proficiency.

Before you can begin to select the right MSSP, a thorough examination of your organization's risk needs and operational technologies is necessary. Businesses should fully understand their network's critical assets, sensitive data, existing technologies, and the threat landscape unique to their business. Armed with this knowledge, organizations can assess each provider based on their array of products and services.

Vendor Expertise

Aside from staffing the SOC, make sure the MSSP has additional resources to establish security-related strategies and policies, manage incidents as they occur, and communicate requirements and actions in the case of a significant data breach. This provides your business with access to deep security expertise and infrastructure that would otherwise be out of reach. Look for a vendor capable of delivering expert detection and response across the crucial facets of your IT environment, publishes their own research, and demonstrates thought leadership and expertise in cybersecurity. Make sure the vendor is aligned and certified in established security frameworks, such as ISO 27001 or SOC2.

Vendor Reputation

When selecting a vendor, prioritize reputable providers with decades of experience in MDR and who are known for consistently delivering dependable security. Look for a vendor with high industry rankings, recognition, and awards. Identifying vendors with a broad portfolio of products and services and a large installed base of customers is a good way to narrow your search and filter out smaller, less experienced players. The vendor should be able to provide customer references upon request.

Vendor Vision and Roadmap

It's important to select a vendor that understands cybersecurity trends, has a clear vision and roadmap, and is continually adapting its offering with innovative technologies and processes. Here are a few things to look for:

- As technologies evolve, the MDR solution should integrate with additional security solutions, such as NDR and Secure Service Edge (SSE).
- As AI and ML algorithms incorporate more advanced threat intelligence, the MDR solution should continually improve in its ability to identify and respond to threats in real-time.
- Security Orchestration, Automation, and Response (SOAR) is a group of cybersecurity technologies that allow organizations to respond to some incidents automatically. Over time, advanced tools and algorithms will enable the MDR solution to become more automated, eliminating the

manual processes involved in incident analysis and response, increasing the speed and accuracy of threat response.

- As more SMBs adopt cloud technologies, the MDR provider should have greater focus on cloud security, protecting cloud infrastructure, systems, and data.
- With more businesses adopting MDR as their primary security solution, market competition will increase, which should lead the MDR provider to lower its costs over time.

Vendor Partnerships

It's impossible for one vendor to produce every security product needed to meet the unique needs of businesses today. Therefore, many MDR providers have partnerships with other cybersecurity providers to deliver comprehensive best-of-breed solutions to their mutual customers, enabling them to leverage the latest security technologies, and provide an up-to-date defense against cyber attacks. The goal is to deliver a customized security solution which benefits and protects the customer's business and their assets.

Ensure you understand the MDR provider's partnership strategy, who they partner with, why the partner was chosen, and which technologies are provided from partners. MDR providers with successful and trusted partnerships can combine the resources and expertise of both companies to provide a more comprehensive and tailored solution to their clients.

Streamline Your Search and Ask the Right Questions

Choosing the right MSSP for your business begins with thorough research, evaluation, and assessment of the vendor's experience, capabilities, service standards, and pricing.

Prepare to ask questions to ascertain whether the vendor aligns with your organizational needs and cybersecurity objectives. It's essential to engage with references, request demonstrations of their services, and gain clarity on the ongoing relationship dynamics with the vendor. The following list of questions will help you streamline your search as you reach the final stage of vendor selection.

Technologies

- ❑ Can we leverage our current security technologies and investments, or is there a requirement to implement new technologies?
- ❑ What technology stack do you provide for delivering end-to-end MDR services, and what factors influenced your selection?
- ❑ Are your technologies cloud-native?
- ❑ Which security technologies do you integrate with?
- ❑ How does your MDR strategy vary across on-premises technology, cloud infrastructure, and cloud applications?

Reporting

- ❑ What kinds of reports do you provide and how frequently are these reports shared with our organization?
- ❑ How will you ensure our organization has the necessary visibility to trust that your SOC is making informed decisions on our behalf?
- ❑ Do you offer regulatory compliance reporting as part of your services?
- ❑ Is there a customer portal available for us to access our data and review alerts?

Customization

- ❑ Are your services adaptable to meet the specific needs of our organization?
- ❑ Could you share instances where you've tailored your services to align with the unique environments of your clients?
- ❑ Do you offer personalized reports and dashboards?
- ❑ Do you incorporate custom use cases and playbooks into your service delivery model?

Data Residency

- ❑ What data do you gather from us to facilitate your services?
- ❑ Where will our data be stored and accessed from?
- ❑ What methods do you employ to collect, store, process, and analyze our data?

Compliance

- ❏ Do you adhere to SOC2 or ISO 27001 standards?
- ❏ Have you implemented frameworks, such as NIST and MITRE ATT&CK?

Experience

- ❏ What are the capabilities of your SOC and where is it geographically located?
- ❏ Could you outline your practices for recruiting and training security personnel?
- ❏ What training and career advancement opportunities are available for your analysts? How do you address turnover?
- ❏ Will our organization be assigned a dedicated team of specialists?
- ❏ Could you provide us with three or four client references?

Service-level Agreements

- ❏ What is your standard SLO and incident response strategy?
- ❏ How do you detect and mitigate threats to our systems?
- ❏ What measures do you take to contain and address threats?
- ❏ How frequently do you conduct proactive threat hunting?
- ❏ What is your mean time to detect (MTTD) and mean time to respond (MTTR) for critical security incidents?
- ❏ How will you communicate with us during a security incident?
- ❏ What procedures are in place if a threat is missed?
- ❏ Can you outline your approach for continuous improvement?
- ❏ How has your service evolved based on lessons learned from past security incidents?

Onboarding

- ❏ What are your onboarding procedures?
- ❏ On average, what is the duration for completing the full onboarding of a client?
- ❏ What specific activity or milestone signifies the completion of the onboarding process?

Partners

- ❏ Who do you partner with to deliver MDR services, and what factors influenced your selection of partners?
- ❏ What technologies do you use from third-party vendors and from in-house?

Payment Model

- ❏ What is your pricing structure for the service?
- ❏ Do you require monthly, quarterly, or yearly payments?

Protect Your Business: Act Now

MDR has emerged as an essential security solution, enabling organizations to preemptively identify, address, and alleviate threats throughout their network infrastructure. Through meticulous selection of the appropriate MDR provider and solution, organizations can bolster their security stance and protect vital assets from constantly evolving cyber risks.

Small and medium-sized businesses can greatly improve their security posture without depleting their financial reserves by implementing a strategic and calculated strategy for enterprise-grade cybersecurity protection. With MDR, SMBs can have peace of mind knowing that they have the resources, expertise, and staff necessary to protect their business from immediate and future cyber threats.

About Hughes

As a global leader in Managed Network Services and Security solutions, Hughes has been serving commercial and government customers for more than 50 years, putting enterprise-grade protection into the hands of small- and medium-sized businesses.

Hughes has a wealth of deep expertise and a wide range of highly skilled professionals who can augment your existing IT and security staff by providing not only knowledge, but also valuable resources, capabilities, and cutting-edge technologies to improve your security operations and enable your business to stay on top of emerging threats.

For more information on Hughes Managed Detection and Response solutions, visit our website.

For additional information, please call 1-888-440-7126 or visit www.hughes.com.

HUGHES®
An EchoStar Company

11717 Exploration Lane
Germantown, MD 20876 USA

www.hughes.com