deepwatch

Choosing a Managed Detection & Response Partner for Your Healthcare Organization

A BUYER'S GUIDE TO IMPROVED SECURITY OUTCOMES

Table of **Contents**

Introduction

Healthcare Delivery Organizations (HDOs) face an ever expanding threat landscape and often struggle with limited budgets to acquire the staff, skills, and advanced technology they need to prevent costly data breaches and disruptions to patient care. Partnering with the right Managed Detection and Response (MDR) provider helps hospitals, outpatient clinics, and other healthcare settings address their security risks through 24/7 monitoring, threat detection and response.

Healthcare data breach costs increased by over $2M dollars from an average of $7.13M in 2020 to $9.23M in 2021.[1]

A shift to MDR for healthcare is driven by a number of factors:

- Healthcare security programs need to be staffed and ready to detect threats and respond to attacks around the clock; however, they often **lack funding to hire skilled staff to cover 24/7 network monitoring**. Experienced healthcare cybersecurity **talent is also hard-to-hire and takes an average of 100+ days to fill.**[2]
- **Healthcare hospitals and outpatient facilities are increasingly targeted by ransomware** due to their lucrative ePHI data that is worth millions in black market.
- **Cyber attacks leading to network outages that prevent access** to medical records, radiology imaging, and other services resulting in impact to healthcare delivery and possible ambulance diversion.
- **Advanced technology and legacy systems co-existing on the same network** can increase risk exposure due to unpatched vulnerabilities that can be exploited by attackers.
- **System mergers and acquisitions** migrating on-premises systems to hybrid and multi-cloud environments that could risk ePHI data security.
- **Fines and penalties for not meeting HIPAA healthcare data compliance requirements when ePHI data breaches occur.**

Hospital boards and healthcare leaders need to see how their security operations investments are maturing and aligning to their organizational goals. This Healthcare MDR Buyer's Guide is focused on the outcomes that security leaders can expect from their MDR provider to support and improve the overall security program, reduce organizational risk, secure patient data and protect access to patient care.

Focus on Outcomes: **What a Healthcare-focused MDR Provider Can (and Should) Do**

Protecting Hospital and Clinic Operations, Patient Care and their ePHI data.

According to a recent survey of security leaders, 94% not using MDR today are planning to evaluate MDR within the next 18 months.[3]

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."[4] - Forrester

A Forrester report states 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 healthcare threats increasing and security teams understaffed, MDR services are a vital solution to strengthen HDO security posture and protect patients.

Patient care availability is better protected, patient data is better secured and financial impact from a security event is minimized **with a team of Security Experts who know your environment and provide 24/7/365 Managed Security Services.**

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.

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. **The right MDR understands the limited budgets a hospital or healthcare organization may have and focuses on the most efficient and effective methods to reduce overall risk.**

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 desire to proactively improve security posture to reduce risk of a patient data breach, HIPAA readiness, a hospital 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."[5]

- 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 **Healthcare Managed Detection and Response 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 healthcare 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 and provide visibility to clinical boards on ROI spends.

Strengthen Threat Detection and **Response Capabilities**

A modern HDO cybersecurity program provides security leaders visibility throughout their environment to identify attacks and respond. Healthcare organizations need to protect against operational disruption and risk to patients. 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, look for an MDR provider that is 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.[6]

$4.87m

The average cost of a breach with a lifecycle over **200 days**.[6]

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. **MITRE Health** Cyber provides healthcare specific resources to protect against ransomware.	the MITRE ATT&CK® framework is a leading method for healthcare 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 Machine Learning (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.

Monitoring and Response

WHY IT WORKS

24/7/365 Security Monitoring for security events conducted by expert-led 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

Trained security analysts monitoring the network ensure threat actors are identified and responded to fast to prevent disruptions to patient care and access to patient data. 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.

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

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 longer a threat actor is on the network, the higher the likelihood there is for a financially impactful ransomware breach. The playbooks should be organized according to the MDR provider's alert triage and workflow integration with the in-house security team.

Endpoint Detection and Response (EDR) for real-time endpoint monitoring, mitigation, and remediation capabilities. Healthcare often has more end-points than they can manage from an expanding attack surface and hybrid workforce. EDR solutions should leverage technology from leaders in the EDR space, to automate and orchestrate response activity on endpoints.

EDR technology captures data from endpoints on the healthcare 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.

Response Continued

Vulnerability Management (VM) for identifying, prioritizing, and remediating the most critical vulnerabilities that could be exploited by attackers. VM gives complete visibility of assets, software, and accounts across the environment, and takes a risk-based approach to ranking vulnerabilities. Prioritization is instant, and takes into account business context, asset criticality, and threat intelligence for the highest level of accuracy. Teams can then focus on maximizing impact and minimizing resource usage, with product-certified experts providing remediation guidance.

WHY IT WORKS

Healthcare organizations are uniquely vulnerable to attacks due to unprotected devices, legacy systems, and complex attack surfaces. VM provides the tools and expertise to quickly address security gaps before threat actors can exploit them. Product-certified engineers monitor for threats and take over day-to-day operations, relieving the load on internal teams and improving security posture with effective patch and risk management.

A NOTE ON EDR VS. MDR SERVICES

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.

Firewall (FW) management for managing and monitoring firewall deployments in order to protect network traffic and prevent unauthorized access. Proper firewall management assures segregation of legacy and advance systems, maximizes investments and maintains the uptime of critical devices with continuous optimization based on the organization's specific needs. HIPAA compliance is maintained by controlling access to protected health information (PHI).

Managed firewall accelerates rule changes and policy enhancements based on asset criticality. Network traffic and vulnerability data are analyzed to detect potential threats, and firewall engineers respond with real-time configuration updates and containment measures. HIPAA-compliant logging tracks all systems that interact with ePHI, while network segmentation and encryption control access.

Mature the **Healthcare Security Program**

Healthcare security leaders need in-depth insights to quantify and map their security risks to organizational priorities and 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 deprioritized.

A healthcare-focused 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 HDO 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.**

Extend the Hospital or Clinic **In-House Security Team**

One of the universally identified issues in every security team is the difficulty hiring and retaining security talent—hospitals and clinics 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, organizations 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!

On average, it takes over 100 days to fill healthcare cybersecurity job positions (almost three times as high as the national average for other industries) which can lead to burnout on the cybersecurity team.[7]

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.**

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

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.

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.

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

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)

Sufficient Levels of Assigned Staffing to ensure that the in-house team can focus on other important security initiatives.

HOW IT HELPS THE IN-HOUSE TEAM

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.**

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.

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

Hospital boards and clinic leadership 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, working within a hospital or clinic team's budget constraints.
- **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.[8]

Some key attributes to look for in an MDR service provider to realize better ROI from security investments include:

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.

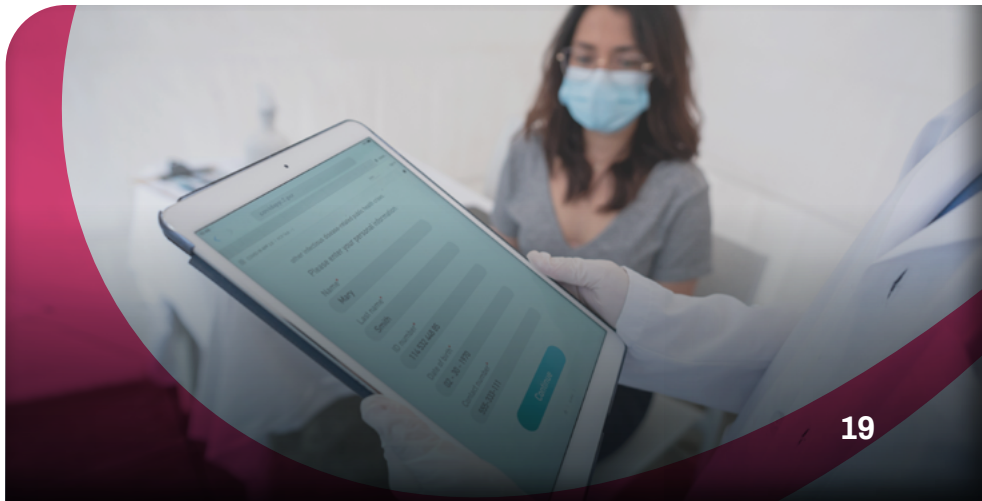
WHY IT IMPROVES ROI

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 to fit the healthcare organization's requirements and budgets, with the flexibility to expand as a hospital or clinic grows—especially into the cloud	Organizations grow and staffing talent will shift. An MDR service provider should **make it easy and cost effective** for the healthcare security team to add and subtract technologies and assets as the organizational needs or budget's 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 the healthcare organization a way 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 for healthcare organizations based on the security and business outcomes that are most critical to an organization. By taking a holistic view of security outcomes, a healthcare 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 hospitals, clinics and other healthcare organizations.
- 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. 2021 Cost of a Data Breach Report, IBM: https://www.ibm.com/security/data-breach
2. Why hospitals, health systems are facing a cybersecurity talent shortage, November 2020: https://www.beckershospitalreview.com/cybersecurity/why-hospitals-health-systems-are-facing-a-cybersecurity-talent-shortage.html
3. Managed Detection and Response, Enterprise Management Associates, July 2020: https://www.ibm.com/downloads/cas/YNKDLKBD
4. Now Tech: Managed Detection And Response Services Providers, Q4 2020, Forrester, December 16, 2020: https://www.forrester.com/report/Now-Tech-Managed-Detection-And-Response-Services-Providers-Q4-2020/RES161762
5. Market Guide for Managed Detection and Response Services, Gartner, August 2020: https://www.gartner.com/en/documents/3989507/market-guide-for-manageddetection-and-response-services
6. 6 2021 Cost of a Data Breach Report, IBM: https://www.ibm.com/security/data-breach
7. 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-skillsgap/
8. 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-areWorking-Despite-an-Average-of-18.4-Million-Annual-Spend