PONDURANCE

Modern Managed Detection and Response for Healthcare Providers: Your Ultimate Guide

pondurance.com

The number of data breaches continues to escalate, putting the healthcare industry on high alert

In 2022, for the 12th year in a row, the healthcare industry experienced the highest average cost of a data breach at $10.1 million, according to IBM Security's Cost of a Data Breach Report 2022. That's an increase of 9.4% over the $9.23 million amount reported in 2021. In healthcare, an operational shutdown is a life or death scenario, making a healthcare organization much more likely to pay the ransom immediately if hit with an attack. An escalation in frequency and severity of cyberattacks, an expanded attack surface, and the complexity of regulatory compliance have contributed to the increase in healthcare data breaches.

To protect their data, many healthcare organizations like yours are turning to managed detection and response (MDR) services, a category of security solutions that offers the technology, process, and expertise needed to defend against the threat of cyberattacks. Cyberattacks and threats have motivated 70% of healthcare organizations to prioritize privacy and cybersecurity, an increase from 40% in 2021, according to a commissioned survey by Xtelligent Healthcare Media.

But not all MDR providers are created equal. Healthcare organizations looking for an MDR provider in the evolving cyber landscape are having to sort through the confusion to find the right MDR provider for their needs.

After reading this guide, you will have a better understanding of available MDR services and how those options may align with your needs. The guide covers:

PONDURANCE

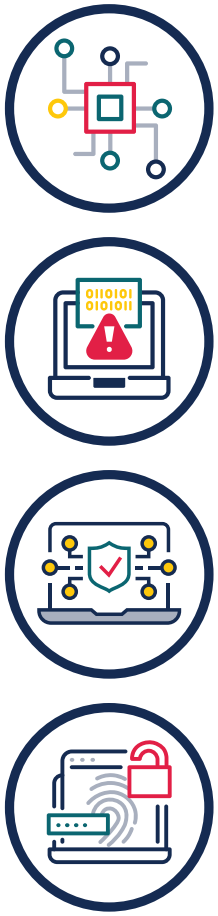
Exploring MDR's history

Cyberattacks on the healthcare industry have evolved over the years. Providers are offering more digital technology options for patients, facing constant threats, and suffering from internal staffing and budget shortages. Today's cyberattackers are using sophisticated assaults with greater frequency to get their hands on sensitive data that healthcare organizations store. In particular, healthcare providers are challenged with attacks from insider threats, ransomware, business email compromise, and more.

> "You need a dedicated and strong security competency that never sleeps, never takes a vacation. And I think the key is to find a partner that will sit with you at the table, work with you, respond with you, learn with you, and grow with you."
>
> *— Ron Pelletier, Founder and Chief Customer Officer, Cybersecurity Trends at Midsize Healthcare Provider Organizations*

To defend against cyberattackers, healthcare organizations may consider a variety of security solutions, including security information and event management (SIEM), managed security service providers (MSSP), extended detection and response (XDR), and managed detection and response (MDR):

- SIEM collects log data and forwards the data to a centralized management and analysis system. It stores the data for posterity, correlates data, and provides alerts, but because it's technology only, it's outdated as a solution.
- MSSP provide alerts and manage firewalls and devices designed to keep attackers out at the perimeter. It involves technology, people, and some processes, but it's not designed to compete with today's sophisticated cyberattackers. Over time, MSSP have become an "alert factory" with alerts being provided to internal security teams, with no additional support with investigation or response.
- XDR delivers detection and response by connecting network, log, and endpoint visibility. However, the platform can be complicated to deploy and requires considerable time and energy from capable cybersecurity experts to configure and operate it.
- MDR began as a service to investigate alerts and incidents to better support internal teams with limited response capabilities. Modern MDR combines advanced technology and experienced security professionals to combat today's threat environment and provide closed-loop incident response. Security professionals perform full scope analysis of networks, endpoints, logs, and cloud environments and proactively respond to threats. The best MDR is a modern one with a complete tool set, experts available to leverage it, and a close partnership with your team to investigate and respond to incidents.



Simplifying the adoption of complex technology

Different healthcare organizations are at different stages of cybersecurity maturity. Your healthcare organization may already have technology and people in place, and modern managed detection and response (MDR) providers like Pondurance build on what you have or bring what you need to provide a customized approach to your cybersecurity. At Pondurance, we believe you shouldn't have to throw out your existing tools or be locked into only one approach. We integrate your existing infrastructure and controls into our own monitoring and response platform.

As technology has advanced over the years, security tools have become increasingly tough to deploy, operate, and maintain. Many of the complex tools even require specialized certifications to properly use them. When you use Pondurance's powerful platform to protect against cyberattacks, the technology burden lifts from the shoulders of your IT or cybersecurity team and lands squarely on our shoulders. However, your in-house team still has access to the same technology and visibility as our analysts, and you retain access to your data at all times.

> **58% of respondents** report the top pressure driving current investments in detection and response is increasingly complex enterprise computing infrastructure.
>
> — Modern MDR: How your organization can get the most business value from Managed Detection and Response, Aberdeen Strategy & Research, August 2022

> Security overall is a scarcity business because there just aren't enough people available to cover all of the needs out there. Organizations are thinking about rightsizing their programs. They don't want to be a technology company; they don't want to put all of their investment in security, nor do they need to be, to be as secure as they should be. So I think it's very smart for organizations to have value-driven partnerships with third parties that can be there at their side.

— Ron Pelletier, Founder and Chief Customer Officer,
Cybersecurity Trends at Midsize Healthcare Provider Organizations

Fighting cyberattackers with human defenders

Technology alone can't stop attackers. Modern managed detection and response (MDR) providers know that human attackers must be confronted by human defenders. The healthcare industry relies heavily on technology, and specifically operational technology and internet-connected devices, to function properly. Without experienced cyber professionals on your team to leverage security tools and manage risk, attackers will work around your defenses. Though technology is important, Pondurance believes people are the foundation of any comprehensive cybersecurity solution.

As you probably know, there's a global cybersecurity talent shortage, and healthcare organizations are finding it difficult to hire, train, and retain professionals for in-house security teams. Across all industries, small and midsize businesses have a particularly difficult time keeping talent due to limited budgets and fewer opportunities for advancement, according to a commissioned study conducted by Forrester Consulting on behalf of Pondurance (July 2022). External partners such as MDR providers fill the talent gaps for these small and midsize businesses. More than half of businesses in the Forrester Consulting study rely on external partners for close collaboration during cybersecurity incidents, and 53% use external partners to keep their security operations centers (SOCs) operational.

Pondurance is fully staffed with seasoned analysts, threat responders, and other security experts to work as an extension of your existing team to monitor and analyze data 24/7. We apply a humans-first approach to MDR. Our professionals respond to real-time alerts with context, collaboration, remediation, and recommendations. We provide threat intelligence with insights into cyber activity worldwide and proactively hunt for threats around-the-clock to defend your healthcare organization against cyberattacks and mitigate the risk of your operational environment. Pondurance delivers proactive security services backed by authentic human intelligence.

PONDURANCE

Bringing the ‘R’ to MDR

Once a threat is identified in the cyber landscape, every minute counts. Modern managed detection and response (MDR) providers like Pondurance help your healthcare organization immediately respond to the cyber threat to minimize damage and reduce recovery time and costs. After all, the longer a cyberattacker dwells in your network, the more opportunity the attacker has to access sensitive protected health information (PHI), infiltrate financial accounts, and introduce malicious malware.

Pondurance rapidly takes action against an attack with predefined parameters and a 24/7 team of incident responders, incident handlers, and forensic and malware specialists who can coordinate a full incident response from the moment the threat is identified. We combine our industry-leading MDR platform with our experienced team to provide:

- **Identification** – Identify and detect an incident as soon as possible
- **Containment** – Stop the incident and reduce the impact
- **Eradication** – Eliminate the threat and prevent recurrence
- **Recovery** – Return to normal operations and conduct a post-breach investigation

Not only can Pondurance stop the incident, but we also can compile detailed forensic reports to document what happened and openly communicate with your insurance providers and attorneys:

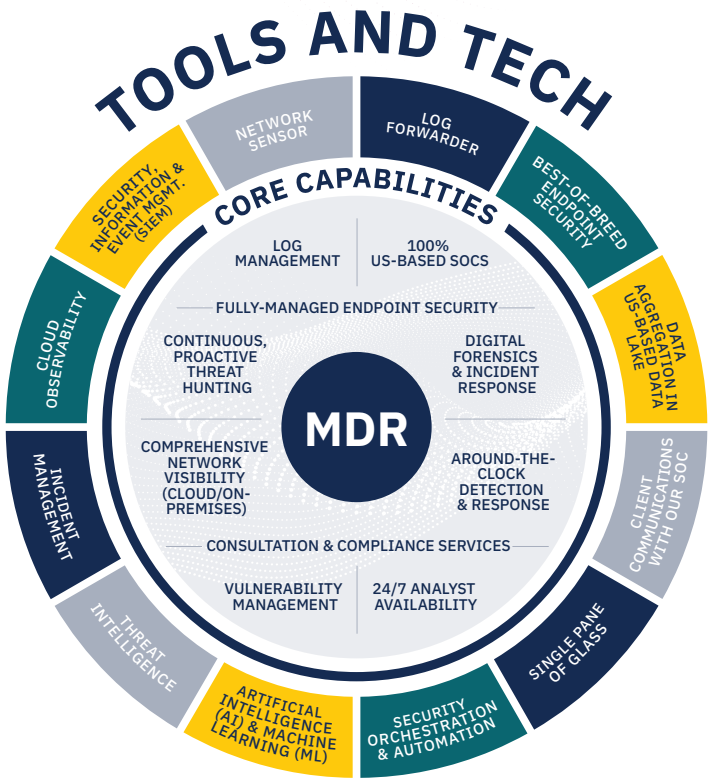
- **Insurance brokers and carriers** – Pondurance works as a go-to provider for incident response and digital forensics engagements. We specialize in building pre-incident relationships to facilitate a rapid, on-target response and reduce the cost of incidents.
- **Attorneys** – Pondurance partners with leading law firms and in-house attorneys who specialize in cybersecurity and HIPAA privacy matters. We support the highest level of confidentiality and operational security regarding all matters.

> “Across all respondents, the total time to detect, investigate, and recover from a security incident ranged from 46 minutes to 46 weeks. *(median: 59 hours)*”
>
> — Modern MDR: How your organization can get the most business value from Managed Detection and Response, Aberdeen Strategy & Research, August 2022

Customizing solutions for today and tomorrow

Your healthcare organization is unique, with its own compliance requirements, staffing challenges, vulnerability issues, and security policies and procedures. Modern managed detection and response providers need to allow for flexibility in their solutions and the ability to adapt and meet your changing needs. Pondurance understands that no one cybersecurity package fits every healthcare organization, so we consult with you and customize our services to your organization's specific operational needs from assessment to implementation and through the life of your partnership with us.

We meet you where you are in your cybersecurity journey. Then, as your cybersecurity needs mature over time, our services adapt to continue keeping you safe from an attack and in compliance.



As part of our customized solutions, we offer comprehensive reporting and risk assessment:

- **Reporting.** Security reporting is important for compliance in the heavily regulated healthcare industry. Pondurance's experts provide custom logging and reporting — with fine-grained visibility and alerting for all relevant systems including networks, endpoints, and the cloud — to precisely document processes and cybersecurity incidents as they happen.
- **Risk assessment.** To stay protected against attack, your healthcare organization needs to know its cybersecurity posture. Performing periodic risk assessments is a great way to identify the areas where you are at risk and know the full extent of your vulnerabilities. A risk assessment can ensure that you're properly allocating your cybersecurity resources and have a thorough incident response plan in place. Pondurance can conduct a risk assessment to uncover your security weaknesses and build a solid solution to defend your healthcare organization against future cyber threats.

PONDURANCE

Knowing cybersecurity vs. compliance

Cybersecurity and compliance are not the same thing, and modern managed detection and response providers know how to navigate the needs for both. Cybersecurity is about preventing cyberattackers from accessing your healthcare organization's data and infrastructure and minimizing the damage of an attack. Compliance involves conforming to industry regulations, government rules, security frameworks, and third-party contracts.

Healthcare organizations must comply with multiple security standards, and keeping track of the security log, data storage, and audit requirements demands in-depth knowledge and competency. Pondurance's experienced professionals can readily implement your healthcare organization's specific policies and skillfully progress through any compliance issues. We offer comprehensive assessments to determine gaps in compliance with industry regulations like HIPAA, as well as other vulnerabilities in your systems with mitigation plans accompanying those results.

> "Compliance is what you have to do, but security is what you should do."
>
> *— Dustin Hutchison, Vice President Services and Chief Information Security Officer*

Legislatures enact new cyber laws and legal requirements each year. A few of the many healthcare compliance statutes that Pondurance commonly addresses include:

- **HIPAA** - This law regulates the flow of healthcare information and ensures that all protected health information (PHI) is kept confidential and private.
- HIPAA Safe Harbor Act - This law encourages the adoption of cybersecurity best practices against cyberattacks and decreases the length and extent of a data breach audit if best practices were used.
- **21st Century Cures Act** - This law improves the flow of healthcare data between providers, patients, and developers of health IT and promotes patient access to electronic PHI.

Understanding your industry

Cyberattacks pose a serious threat to hospitals, physician practices, ambulatory care facilities, and medical businesses of every size. Many healthcare organizations know firsthand that a cyberattack can cost millions of dollars, wreaking havoc on the bottom line. More importantly, a cyberattack at a healthcare organization can risk patient safety and cost lives.

Modern managed detection and response providers understand how to work within various industries and tailor programs to fit those industry needs. They also are masters of threat intelligence, providing insights into the ever-changing threat landscape for their clients.

Pondurance has significant experience and expertise in the healthcare industry, defending against the increased number of cyberattacks and threats, protecting the expanded attack surface, navigating the complexities of regulatory compliance, and dealing with the multitude of other cyber-related challenges that affect healthcare organizations. We can tackle any cybersecurity or privacy issue that arises with the confidence that comes from having been there and done that. And since our SOCs are all based in the United States, you will never have to worry about your sensitive patient data leaving the U.S. borders.

Tailoring to your needs and budget

Most likely, your healthcare organization has a set cybersecurity budget that you want to invest as wisely and cost effectively as possible. Ninety-two percent of midsize healthcare providers surveyed by Xtelligent Healthcare Media are either currently outsourcing or plan to outsource this year. Managed detection and response (MDR) services can fit your budget. Using an MDR provider is a more economical option than hiring a full security team. And, during the current talent shortage, finding talent with the expertise needed to maximize your investment in security tools can be difficult.

First and foremost, Pondurance knows the healthcare industry and listens to your cybersecurity needs. We find out what's important to you and what existing technology systems and controls you have in place. We help you prioritize your budget based on the specific cyber risks your organization faces, to maximize efficiency, minimize complexity, and ensure we rightsize your services from the outset.

Then, Pondurance tailors a customized package of security services to meet your specific needs across multiple vectors, including endpoints, networks, logs, and the cloud. One size fits all is not an option. We can put technology to work from preferred vendors such as SentinelOne, CrowdStrike, or Blackberry Cylance. Or we can seamlessly work with your existing technology, integrating your data into the Pondurance tech stack, to maximize your cybersecurity investments, so there's no need to rip and replace what you already have. We'll never ask you to agree to or pay for more security services than you actually need to protect your healthcare organization against cyber threats.

Continuing on the journey

Modern managed detection and response (MDR) has come a long way from its humble origins, and it continues to evolve. As a modern MDR provider, Pondurance offers MDR services, incident response, and cybersecurity consulting to protect your healthcare organization from cyberattacks and compliance issues. We integrate with your existing technology and staff the human defenders you need to stay safe and proactively respond to cyber threats. And Pondurance will continue to offer the customization, flexibility, and service your organization needs as your cybersecurity posture matures in the years ahead.

PONDURANCE

PONDURANCE

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204

About Pondurance

Pondurance delivers world-class MDR services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to clients seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.