PONDURANCE

Demystifying Modern MDR: Your Ultimate Guide To Managed Detection and Response

pondurance.com

The number of data breaches continues to escalate, **putting small businesses on high alert**

In 2021, organizations experienced a 68% increase in breaches, the highest number of breaches ever reported in a year, according to Identity Theft Resource Center. And in the first quarter of 2022, the number of publicly reported data breaches was up 14% over 2021.

The expanded attack surface has contributed to the increase in data breaches. Today's cyberattackers are no longer looking to steal only sensitive customer data such as Social Security numbers and credit card information. Ransomware has redefined "monetizable data." Now, any information that a business finds valuable, such as maintenance records on a fleet of trucks or a manufacturer's third-party supplier information, is monetizable and a potential target for attack.

To protect such data, many organizations 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 increasing threat of cyberattacks. Technological research and consulting firm Gartner projects that 50% of all organizations will use MDR services by 2025.†

But not all MDR providers are created equal. Businesses 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. Pondurance keeps it simple. We offer comprehensive 24/7 MDR and threat hunting, cybersecurity consulting, and digital forensics and incident response (DFIR) services.

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:

† *2021 Gartner Market Guide for Managed Detection and Response Services, Gartner, October 2021.*

PONDURANCE

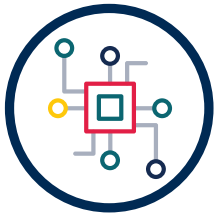
Exploring MDR's history

Cyberattacks have evolved over the years. The shift to working from home, the threat from nation-states and cybercriminals, the expanded attack surface, cryptocurrency as a payment method, and the abundance of data collected across every industry have all factored into the current cybersecurity landscape. Today's cyberattackers are using sophisticated assaults with greater frequency, and no organization is immune from a possible attack. Organizations face attacks from malware, ransomware, business email compromise, phishing, and more.

> MDR at its core is really about enabling organizations to benefit from what a provider can do for them, which includes triaging, detecting, and potentially responding to the threats. And that's really where modern MDR picks up ... really being able to reach into the environment and block threats, in addition to a number of other characteristics such as full visibility and the ability to do threat hunting continuously as well.
>
> *— Lyndon Brown, Chief Strategy Officer (ISC)2 webinar, May 2022*

To defend against cyberattackers, 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 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 has 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 to configure and operate. The customer remains on the hook to find capable talent and build processes.

- MDR began as a service to investigate alerts and incidents to better support internal teams with limited response capabilities. Today, modern MDR combines 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 organizations are at different stages of cybersecurity maturity. Your organization already may have technology and people in place, and modern 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 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*

PONDURANCE

An estimated **4.1 million people** work as cybersecurity professionals worldwide, including **1.14 million U.S. workers**, yet **the workforce must increase by 65% to defend against cyber threats.**

— *(ISC)2 2021 Cybersecurity Workforce Study*

Fighting cyberattackers with human defenders

Technology alone can't stop attackers. Modern MDR providers know that human attackers must be confronted by human defenders. Without experienced cyber professionals on your team to leverage security tools, 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 organizations are finding it difficult to hire, train, and retain professionals for in-house security teams. Small and medium-size 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 medium-size 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 hunters, and other security experts to seamlessly integrate with your existing team to detect and respond to cyber threats 24/7. We apply a guided yet collaborative approach to MDR at every step of the cybersecurity process. Our professionals respond to alerts in real time, offering recommendations for remediation with the context necessary to respond rapidly and even taking action on your behalf within established service legal agreements . We provide threat intelligence with insights into cyber activity worldwide and proactively hunt for threats around-the-clock to defend your organization against cyberattacks. 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 MDR providers like Pondurance help your 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 potential damage the attacker can cause.

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 services 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 digital forensics and incident response 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 privacy matters. We support the highest level of confidentiality and operational security regarding all matters.

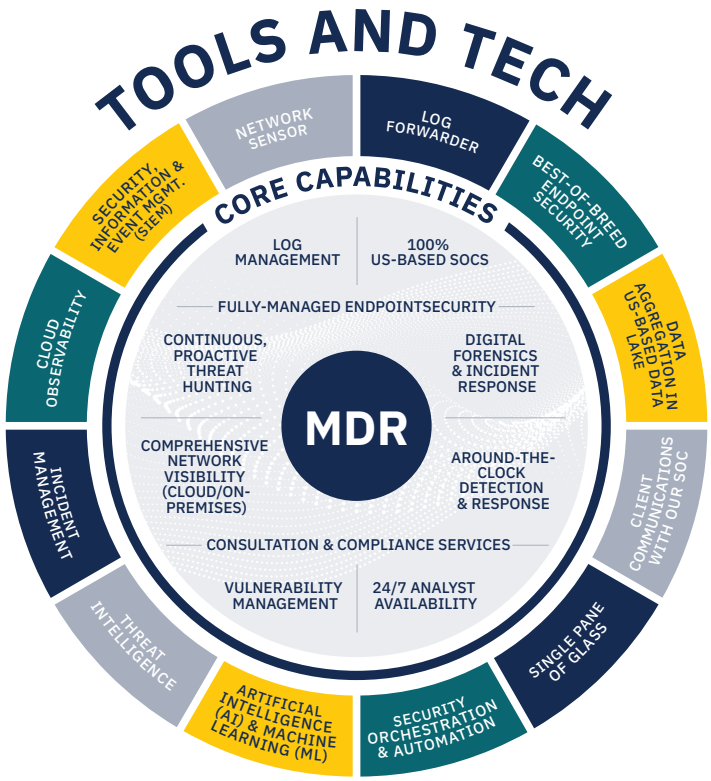
> Across all respondents, the total time to detect, investigate, and recover from a security incident ranged from 46 minutes to 46 weeks. *(median: 59 hours)*

— 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 organization is unique, with its own compliance requirements, staffing challenges, and security policies and procedures. Modern MDR 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 business, so we consult with you and customize our services to your organization's specific industry and operational needs and integrate any security tools that your organization has in place.

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, but heavily regulated industries are not the only ones that can benefit from comprehensive reporting. Most organizations perform more efficiently with the proper handling of incident logs and alerts. 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 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 organization against future cyber threats.

PONDURANCE

Knowing cybersecurity vs. compliance

Cybersecurity and compliance are not the same thing, and modern MDR providers know how to navigate the needs for both. Cybersecurity is about preventing cyberattackers from accessing your 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. Whether compliance is a concern for your particular organization can depend on your industry, size, location, or customers.

Many organizations must comply with more than one security standard, 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 organization's specific policies and skillfully progress through any compliance issues. We offer ongoing vulnerability management, including risk assessment and penetration testing, and our team of experts can keep you compliant to your specific industry's regulations, size, location, or customer needs.

> "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 compliance statutes that Pondurance commonly addresses include:

- **HIPAA** - This U.S. law regulates patient data for any healthcare entity operating within the United States.
- **23 NYCRR 500** - This New York Department of Financial Services law requires financial firms and related service providers to protect customers from loss of personal data.
- **Payment Card Industry Data Security Standard** - This standard regulates customer financial privacy and is a standard across the credit card industry.
- **California Consumer Privacy Act** - This personal data regulation applies to any entity using the data of California residents.
- **General Data Protection Regulation** - This personal data privacy compliance standard from the European Union (EU) requires that any organization holding EU citizen data must comply.

PONDURANCE

Understanding your industry

In today's cyber environment, threats pose a challenge for every industry — some more than others. 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*. Education, financial, manufacturing, energy, transportation, and agriculture industries also have seen their fair share of cyberattacks. No small, medium-size, or large business in any industry is exempt from a possible attack.

Modern MDR providers understand how to work within specific industries and tailor programs to fit those needs. They also are masters of threat intelligence across various industries, providing insights into the ever-changing threat landscape for their clients. Pondurance has significant experience in each of the above-named industries and more. That's important because every industry has unique privacy issues, compliance requirements, rules and regulations, and third-party vendor contracts that an organization must follow. Pondurance can tackle any cyber-related 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 data leaving the U.S. borders.

In addition, every supplier within the defense industrial base, including contractors and subcontractors, must undergo assessments to prove that they can sufficiently perform cybersecurity capabilities as specified in the Cybersecurity Maturity Model Certification (CMMC). As a registered provider organization for CMMC, Pondurance fully understands what your organization must do to become compliant and stay that way, and we closely work with you to make it happen.

[2]Cost of a Data Breach Report 2022, IBM Security, July 2022.

PONDURANCE

Tailoring to your needs and budget

Most likely, your organization has a set cybersecurity budget that you want to invest as wisely and cost effectively as possible. 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 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 "right size" 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 organization against cyber threats.

Continuing on the journey

Modern 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 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 business 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.