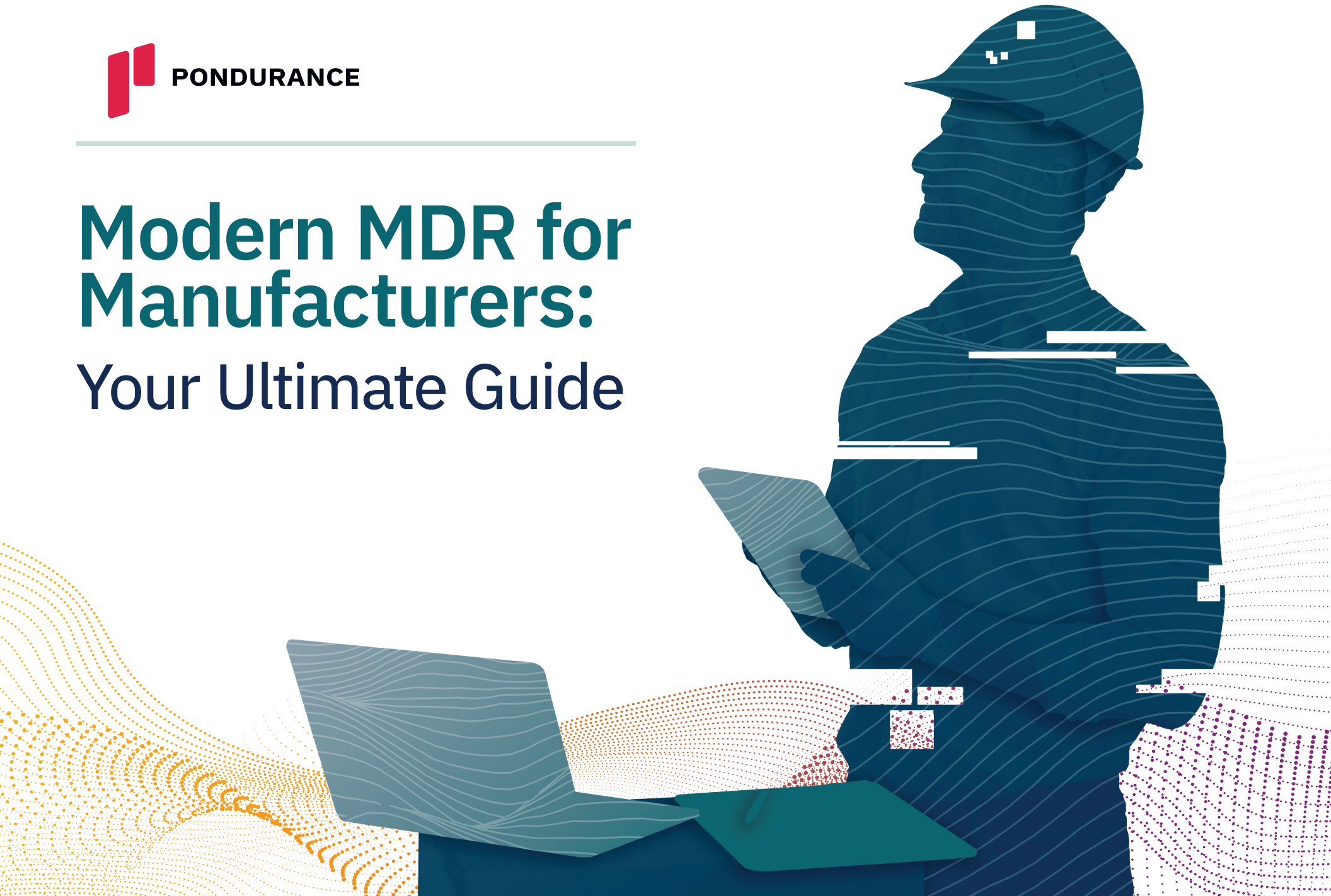
PONDURANCE

Modern MDR for Manufacturers:

Your Ultimate Guide



MODERN MDR FOR MANUFACTURERS: YOUR ULTIMATE GUIDE

Cyberattacks continue to occur at an alarming pace, which probably comes as no surprise to most manufacturers. In 2022, the manufacturing industry experienced 1,817 incidents and 262 breaches with confirmed data disclosures, according to Verizon's 2023 Data Breach Investigations Report. The report also found that hacking, malware, and social engineering attacks are the most prevalent attack patterns on manufacturers.

The manufacturing industry is a prime target for cyberattackers, particularly those using ransomware, since manufacturers often pay the ransom when attacked. That's because even a small amount of downtime for a manufacturer can make an impact, causing production line stoppage and supply chain disruptions. In addition, many manufacturers use legacy systems that can't be properly patched or updated, leaving them vulnerable to an attack.

To combat these risks, many manufacturers are turning to managed detection and response (MDR) services, a category of security solutions that offers the technology, process, and humans 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. Manufacturers 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 modern MDR, cybersecurity consulting, and 24/7 incident response and threat hunting to help manufacturers like you stay safe from cyberattacks and disruption.

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

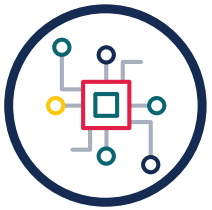
Exploring MDR's history

Cyberattacks have evolved over the years. Today's cyberattackers use sophisticated assaults with great frequency, and no organization is immune from a possible attack. Like other industries, manufacturing faces potential attacks from malware, ransomware, business email compromise, phishing, and more. At the same time, manufacturers have their own unique set of cybersecurity risks including the use of legacy systems with software vulnerabilities.

> 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.
>
> *— Pondurance, Chief Strategy Officer*

To defend against cyberattackers, manufacturers may consider a variety of security solutions including SIEM, managed security service providers (MSSPs), 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.



- **MSSPs** 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, MSSPs have become an "alert factory" with alerts being provided to internal security teams, with no additional support.

- **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 in the cyber environment to better support internal teams with limited response capabilities. Today, modern MDR combines advanced technology and experienced security professionals to capture, integrate, and analyze data. Security professionals perform full scope analysis of networks, endpoints, logs, and cloud environments and proactively respond to attacks. The best MDR is a modern one with a complete tool set and experts available to leverage it.

Simplifying the need for complex technology

Different manufacturers are at different stages of cybersecurity maturity. As IT and operational technology have converged, your business may have some cybersecurity technology and people already 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 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 manufacturers are finding it difficult to hire, train, and retain professionals for in-house security teams. All industries are having a difficult time keeping talent due to limited budgets and fewer opportunities for advancement, according to a Forrester study. External partners such as MDR providers fill the talent gaps. More than half of businesses in the Forrester 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 seamlessly integrate with your existing team to monitor and analyze data 24/7. We apply a humans-first approach to MDR at every step of the cybersecurity process. 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 manufacturers 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 manufacturers 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 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 preincident 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 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**.

– Modern MDR: How your organization can get the most business value from Managed Detection and Response, Aberdeen Strategy & Research, August 2022

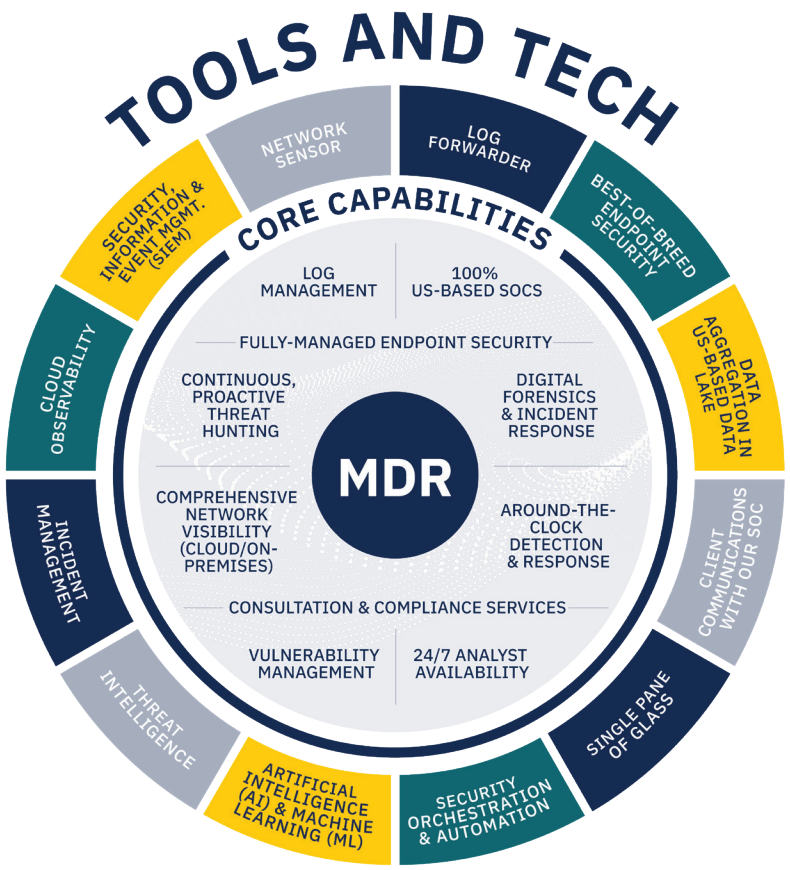
> **94%** of manufacturing organizations with a standalone policy and **93%** of those with a wider insurance policy that covers cyber got [encrypted] data back. In comparison, only **53%** of those without a policy were able to get encrypted data back.

— Sophos, The State of Ransomware in Manufacturing and Production 2023

Customizing solutions for today and tomorrow

Your business is unique, with its own legacy systems, 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 manufacturer, so we consult with you and customize our services to your operational needs and integrate any security tools that you already have 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.



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

- **Reporting.** Security incident reporting is important for compliance, but heavily regulated industries are not the only ones that can benefit from comprehensive reporting. Most businesses 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 business 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 business against future cyber threats.

PONDURANCE

Understanding your industry

In today's cyber environment, threats pose a challenge for every industry — and manufacturing is no exception. The manufacturing industry experienced the fourth-largest number of cyber incidents, with the public administration, information, and finance industries comprising the top three spots, according to the Verizon report. As much as 96% of cyberattackers who targeted manufacturers were financially motivated, meaning they wanted a big payout.

Such motivation makes manufacturing an especially popular target for ransomware attacks because manufacturers often pay the ransom to minimize any disruption to their operations. After all, a successful cyberattack can both halt production and interrupt the supply chain, causing negative repercussions for the manufacturer and its customers down the line.

In addition, manufacturers are easy targets because their attack surfaces are typically large with multiple entry points into their networks. Many manufacturers work with legacy systems that provide ease of use but were not designed with cybersecurity in mind, making them vulnerable to attacks.

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

Pondurance has significant experience in the manufacturing industry, protecting the expanded attack surface and dealing with the multitude of cyber-related challenges that affect manufacturing. We can tackle any cybersecurity issue that arises with the confidence that comes from having been there and done that.

Tailoring to your needs and budget

Most likely, your manufacturing business 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 — that is, if you can even find workers during the talent shortage — and purchasing the technology tools needed to make it work.

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 you face, 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 CrowdStrike, SentinelOne, or Microsoft Defender. Or we can seamlessly work with your existing technology, integrating your data into the Pondurance tech stack, to maximize your cybersecurity investment, 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 business against cyber threats.

Continuing on the journey

Modern MDR has come a long way from its cybersecurity origins, and it continues to evolve. As a modern MDR provider, Pondurance offers MDR services, incident response, and cybersecurity consulting to protect your business from cyberattacks and disruption. 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 you need as your cybersecurity posture matures in the years ahead.

PONDURANCE

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 customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

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

PONDURANCE

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