Gartner Now Recommends What Pondurance Has Provided From the Start

PONDURANCE

In the *Gartner 2023 Marketing Guide for Managed Detection and Response Services,* Gartner states that: "Misnamed technology-centric offerings and vendor-delivered service wrappers (VDSW), that fail to deliver human-driven managed detection and response (MDR) services, are causing challenges for buyers looking to identify and select an outcome-driven provider."

Pondurance agrees. As an MDR services provider, we have always believed that human intelligence is the foundation of any comprehensive cybersecurity solution. Technology alone can't stop attacks. You need both technology and people to defend against today's cybercriminals — and Pondurance is staffed with exceptional humans who know how to leverage cutting-edge technology.

GARTNER SAYS	PONDURANCE AGREES
Gartner recommends that a security and risk management leader responsible for security operations should:	Pondurance uses humans, technology, and best practices to comply with Gartner recommendations as follows:
Use MDR services to obtain 24/7, remotely delivered, human-led security operations capabilities when there are no existing internal capabilities, or when the organization needs to accelerate or augment existing security operations capabilities.	Our analysts, threat responders, security experts, and technology can function as your full security operations team or seamlessly integrate with your existing team to provide dynamic detection and prevention controls. We provide the 24/7, eyes-on-glass monitoring you need and can integrate any technology that your organization already has in place to maximize your current cybersecurity investments.
Assess how the MDR provider's containment approach and incident reporting can integrate with your organization and whether actions can be performed on your behalf to align with business requirements as well as compliance/legal policy/government regulation.	We identify, contain, and respond to threats and, when necessary, guide you through remediation. From the moment a threat is detected, our experienced team springs into action with a coordinated incident response (IR) plan aligned with your business requirements and regulations. Our in-house IR capabilities effectively bring continuity of response, minimize damage, reduce recovery time, and keep costs under control.
Attain the maximum benefit from MDR services by preparing response workflow processes and integrating existing ticket management systems to ensure a business-centric response.	Our Scope platform provides a seamless user interface, assuring that your internal team has 24/7 access to the Pondurance team. You have complete visibility and access to your data, and together we can establish the workflows and processes that align with your business goals.
Investigate whether the MDR provider's service is able to align with your business-driven requirements and provide actionable findings that internal teams can successfully react to, rather than settling for regurgitated technology outputs with no added analysis.	Our risk-based approach focuses on the areas most important and critical to your business. We provide 360-degree visibility across your networks, endpoints, devices, logs, and cloud infrastructure for a broad and in-depth view of your cyber environment. Our experts proactively hunt for and detect signs of malicious activity, provide malware prevention, and respond to real-time alerts with confirmation, context, collaboration, and active response measures.

CONTACT US FOR A RISK ASSESSMENT and to see how Pondurance MDR can help you mature your cybersecurity program.

READ THE GUIDE HERE

pondurance.com