

# Standing Apart from the Crowd – Pondurance Top 5 Strengths



## Modular pricing and flexible deployment options



Pondurance is able to meet our clients where they are with modular and flexible deployment and pricing options, not just solely based on your size or user count. We can help fill specific gaps in your environment (log, network, or endpoint monitoring and response) or cover everything. We look at client asset inventory to produce a licensing level that is both cost-efficient and security-conscious.

No nickel and diming. Our costs are all inclusive of project management for implementation, 24/7 monitoring, an enterprise cloud-based SIEM tool (for log/network), and ongoing tuning, dashboards, and custom parsing as needed throughout the contract.

## Full access, ownership, and observability – SIEM as a Service



Along with our Gartner recommended 24/7 Managed Detection and Response (MDR) service, Pondurance also provides the added bonus of a fully hosted, managed, and administered SIEM. We architect this backend SIEM ourselves and give all clients their own subtenant access, mimicking the same functionality many clients would typically have to purchase themselves. This hosted SIEM provides clients real-time observability, log aggregation, dashboarding, and querying within seconds, as well as archival access to logs for as long as needed for compliance. Contractually, clients own all the data they send for monitoring for the duration of the term, giving full transparency and peace of mind.

## Award-nominated in-house IR team available in minutes



Nominated by Advizen for three years in a row as a top 10 global incident response (IR) team, Pondurance's in-house incident responders are best in class. When clients first come to us, many times they're in a tough spot and need assistance containing an active incident. Pondurance springs into action to contain and forensically investigate, in close conjunction with our legal and insurance partners, and provide continuous monitoring after the fact. We are currently on the panels for many top insurance partners and have relationships spanning breach coaches, e-discovery, and more. Our MDR clients can be assured that we have the ability to pivot to an IR investigation at a moment's notice, typically within minutes, should it be deemed necessary. Pondurance has been doing IR for 10-plus years. It has never been an afterthought or bolt-on solution.

## Fully managed and MITRE vetted EDR



Instead of reinventing the wheel with a homegrown endpoint agent like our competitors, we partner with best-in-class MITRE vetted solutions like SentinelOne, CrowdStrike, and Defender to provide 24/7 managed endpoint detection and response (EDR). According to IDC, a large percentage of incidents involving EDR tools were due to misconfiguration leading to bad policies, alerts that didn't get followed up on, and incidents spreading within the network. Let Pondurance analysts do all the hard work to deploy, manage, and monitor EDR on your behalf. When something goes wrong in the middle of the night, you can wake up the next day with full containment and peace of mind. To top it all off, we add 360-degree correlation across logs, network, and cloud from a single source.

## Personalized communication, onboarding, and alerting aligned to your needs



Communicate with actual human beings in real time, not a robot. Have custom needs or requests throughout the contract? Reach out directly in Pondurance's proprietary SCOPE portal to speak with a U.S.-based analyst any time of day. Have a new data source you want to add? Reach out and we will work with you. Not all clients have the same needs, so we don't treat them that way. During onboarding, we will work to understand your specific environment, risks, assets, and standard operating procedures in order to act as a true partner and extension of your security team.