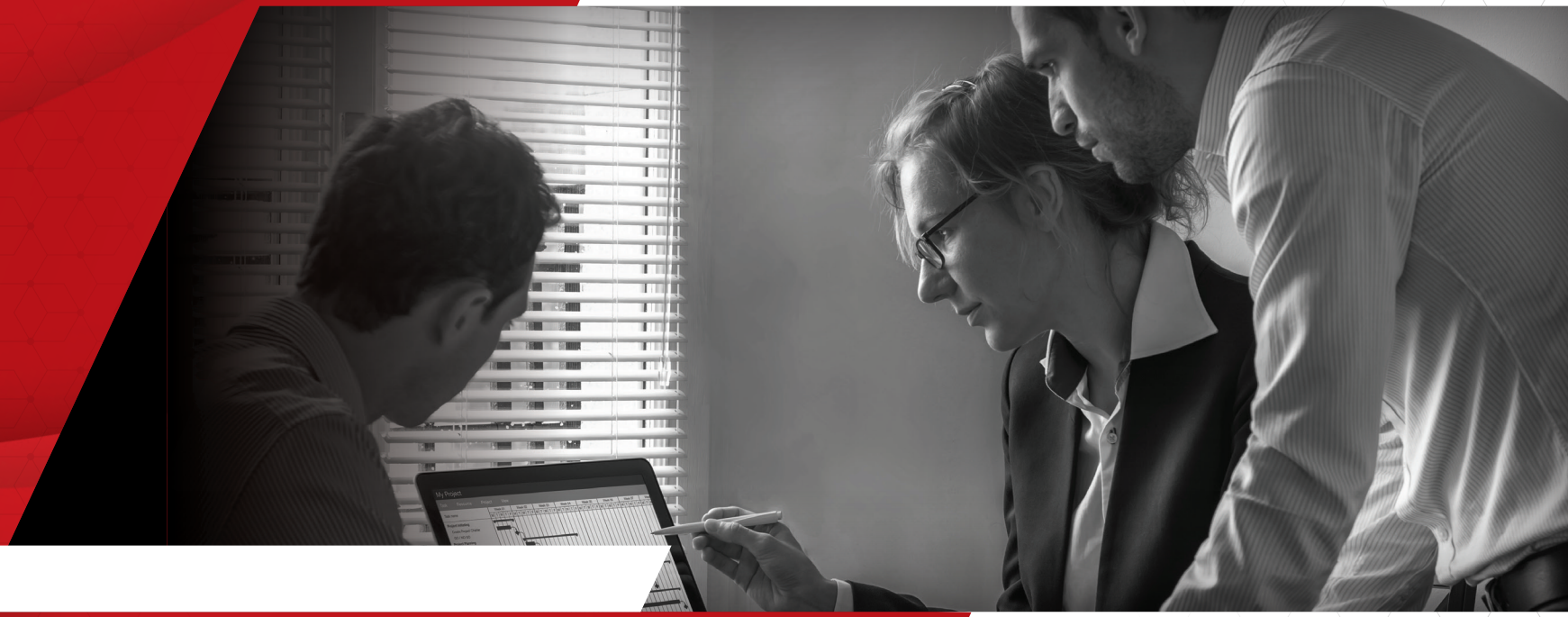
PONDURANCE



5 Things to Consider When Choosing an MDR Provider

pondurance.com

Cyber threats continue to grow and are more costly than ever

Managed Detection and Response is a growing category with Gartner projecting spend to reach $4B in the next 4 years. After reading this guide, you will have a better understanding of the challenges that are causing customers to turn to MDR service providers. This guide covers: the differences between SIEM, MSSP, & MDR, components of MDR, how to evaluate MDR vendors and Pondurance's approach to managed detection and closed-loop incident response.

41% of organizations are seeing **10,000 alerts every day.**

(Cisco[1])

Organizations face growing challenges when trying to protect themselves from cyber attacks.

CUSTOMER PAIN POINTS

Shortage of cyber security talent

Security professionals are expensive to hire and hard to retain

Security technology is expensive and hard to maintain

Difficult to manage multiple tools and investigate all alerts

Technology alone can't deter motivated attackers

New compliance and regulation requirements

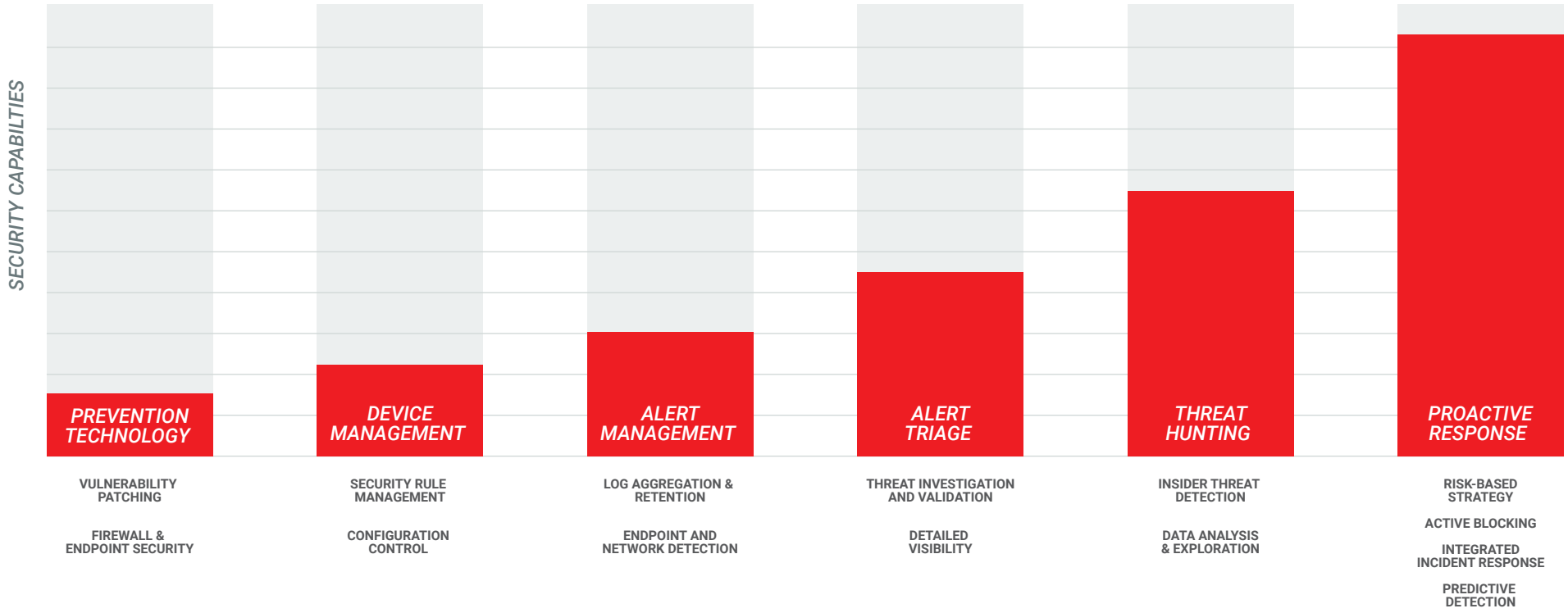
Undocumented processes in event of an attack or breach

Lack of visibility across the enterprise

Inability to quickly remediate or reduce attacker dwell time

Detection and Response Maturity Model

Organizations considering MDR have varying levels of maturity.



Organizations find it expensive and difficult to build an internal SOC.

As a result, they lack 24/7 detection and response capabilities.

Threat actors are getting smarter and circumventing prevention tools. Tools that were used in the past to detect phishing attacks or threats like ransomware are no longer sufficient. More often we are seeing insider threats, account takeovers and attacks entering through unpatched vulnerabilities.

BY 2025
AT LEAST 75%
OF IT ORGANIZATIONS
WILL FACE ONE
OR MORE ATTACKS

Gartner[2]

50%
INCREASE
in daily cyber
attacks just in 3Q20.

Check Point Software Technologies[3]

Traditional MSSPs or SIEMs do not provide the value organizations need.

Many MSSPs and SIEMs do not have detection and response capabilities, they only alert the security teams which causes a backlog of tickets to search through. Many customers spend more time triaging alerts from MSSPs than they can respond to. SIEM are difficult to maintain, have stale correlation rules and expensive from both a storage and management perspective.

What is the difference between SIEM, MSSP & MDR?

- **SIEM:** Security Information and Event Management technology supports threat detection, compliance and security incident management through collection and analysis of security events.

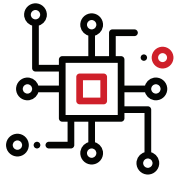
- **MSSP:** Managed Security Service Provider provides outsourced monitoring and management of security devices and systems.

- **MDR:** Provide customers with remotely delivered modern 24/7 SOC capabilities to rapidly detect, analyze, investigate, and actively respond to threats.

… so many are turning toward Managed Detection and Response (MDR) solutions.

Learn more about the differences between SIEM, MSSP, MDR and Pondurance MDR in our comparison chart.

Core Components of MDR



PEOPLE	PROCESS	TECH
24 X 7	TECHNOLOGY MANAGEMENT	DETECTION AND RESPONSE PLATFORM
EXPERT HUMAN INTELLIGENCE	DETECTION	LOG ANALYSIS
SECURITY ANALYSTS	RESPONSE	NETWORK ANALYSIS
THREAT HUNTERS	THREAT INTELLIGENCE	ENDPOINT DETECTION & RESPONSE
INCIDENT RESPONDERS	VULNERABILITY MANAGEMENT	FORENSICS

Key areas when evaluating MDR provider

How do you know if adding MDR services is the right move for your organization? Gartner suggests that you consider a MDR provider if you need remotely delivered modern 24 x 7 SOC functions and there are no existing internal capabilities or if you need to accelerate or augment existing capabilities. You should also consider a MDR provider if there is no one in-house to respond to threats that require immediate attention. We recommend the following criteria when evaluating MDR vendors:

- **Technology Stack:** What tools are you using now? Can your MDR provider make you better while leveraging some of your existing investments?
- **Fits with Your Policies:** Does the MDR provider's containment approach integrate with your organization's policies and procedures?
- **Monitor On-Premises & Cloud Assets:** Can they support your on-premises and cloud environments?
- **Custom Reports Including Compliance:** MDR providers should provide custom reports including those needed for compliance
- **Real-Time Alerts Backed by Human Intelligence:** Does the MDR provider have a fully managed and monitored log? Can they provide real-time alerts? Are the alerts reviewed by experts to only alert you when action is needed to stop an attack?
- **Incident Response and Remediation:** Does the MDR provider offer incident response capabilities? Can they help minimize losses and prevent future incidents?
- **Experience with Your Industry:** Do they have experience with your industry? Do they work with other organizations that are similar in size to yours?

When you are looking for a new vendor, you want to find the one that works best for your organization. Whether they specialize in your industry, are able to integrate with your current technology stack or are able to monitor your cloud environments.

The right MDR vendor will fit into your organization and current security protocols. They will actively hunt for and identify threats across your endpoints, networks and access management tools.

Pondurance's approach to MDR

Artificial Intelligence and Machine Learning
Meets Human Experience, Intuition and Unwavering Curiosity

What's Being Monitored

On-premises and cloud assets

- Network
- Endpoints
- Users
- Cloud
- Apps
- Servers & Workloads

Internal Team

IT/Security

CLIENT

What's Being Collected

Global Threat Intelligence

Billions of Events
- Log
- Network
- Endpoint

Asset and Vulnerability Data

Data Analysis

Pondurance Threat Research

Hundreds of Correlated Alerts

SCOPE ADVANCED ANALYTICS

Human Intelligence

Proactive Threat Hunting

Threat Validation and Investigation

Closed-Loop Incident Response and Forensics

Notifications • Containment • Trusted Advice • Reports

How Pondurance Can Help

Our mission is to ensure that every organization is able to detect and respond to cyber threats – regardless of size, industry or current in-house capabilities. We combine our advanced platform with decades of human intelligence to decrease risk to your mission.

CLOSED-LOOP MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 US-Based SOC services powered by analysts, threat hunters and incident responders who utilize our advanced cloud-native platform to provide you with continuous cyber risk reduction. By integrating 360 degree visibility across log, endpoint and network data and with proactive threat hunting we reduce the time it takes to respond to emerging cyber threats.

Pondurance MDR is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyber threats. Human attackers must be confronted by human defenders.

INCIDENT RESPONSE

When every minute counts, organizations need specialized cyber security experts to help them respond to a compromise, minimize losses, and prevent future incidents.

Pondurance delivers digital forensics and incident response (DFIR) services with an experienced team capable of guiding you and your organization every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis and helping to quickly restore your normal operations.

SECURITY CONSULTANCY SERVICES

Our specialized consultancy services will help you assess systems, controls, programs and teams to uncover and manage vulnerabilities. Our suite of services ranges from penetration testing to red team exercises, along with compliance program assessments for highly regulated industries. We provide security incident response and business continuity planning to put you in the best position to defend against and respond to cyber attacks.

About Pondurance

Pondurance delivers world-class managed detection and response services to industries facing today's most pressing and dynamic cyber security 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.

Sources:

1. Cisco, 2019 Cisco Benchmark Report, 2019.
2. Gartner, Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware, Jan 2021.
3. Check Point, Global Surges in Ransomware Attacks, Oct 2020.

pondurance.com

500 N. Meridian St., Ste 500 Indianapolis, IN 46204

PONDURANCE