PONDURANCE

5 Things To Consider When Choosing an MDR Provider

pondurance.com

Cyberthreats Continue To Grow and Are More Costly Than Ever

Managed detection and response (MDR) is a growing category with Gartner projecting spend to reach $4 billion in the next four 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 Cyberattacks

CUSTOMER PAIN POINTS

Shortage of cybersecurity talent

Security professionals that are expensive to hire and hard to retain

Security technology that is expensive and hard to maintain

Difficulty managing multiple tools and investigating all alerts

Technology alone can't deter motivated attackers

New compliance and regulation requirements

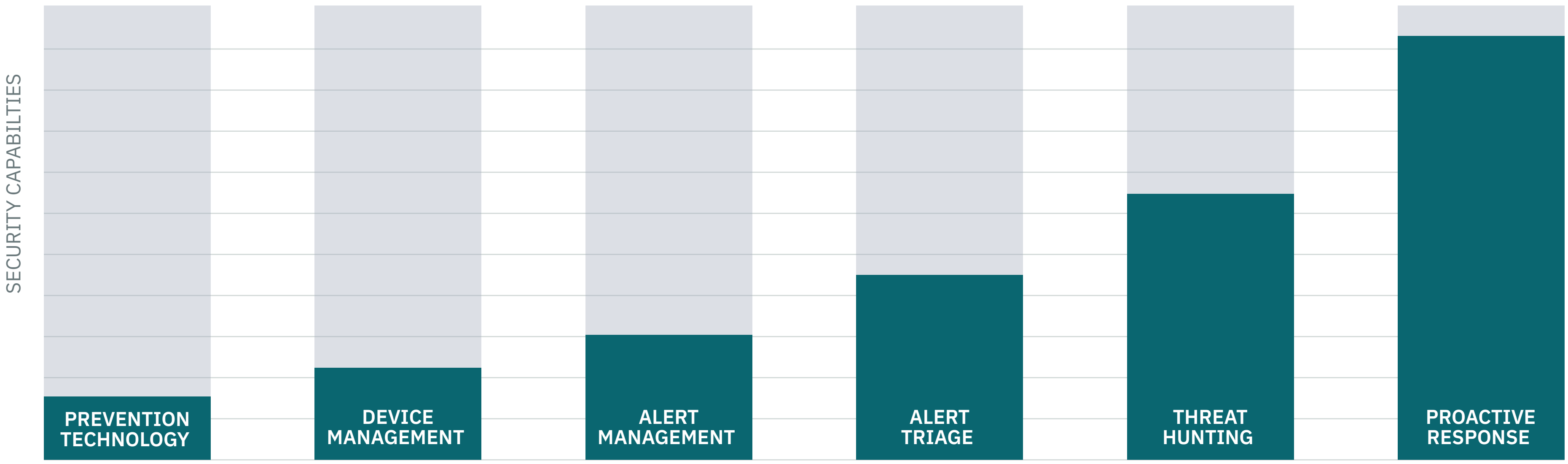
Undocumented processes in the event of an attack or breach

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.



PREVENTION TECHNOLOGY	DEVICE MANAGEMENT	ALERT MANAGEMENT	ALERT TRIAGE	THREAT HUNTING	PROACTIVE RESPONSE
VULNERABILITY PATCHING FIREWALL & ENDPOINT SECURITY	SECURITY RULE MANAGEMENT CONFIGURATION CONTROL	LOG AGGREGATION & RETENTION ENDPOINT AND NETWORK DETECTION	THREAT INVESTIGATION AND VALIDATION DETAILED VISIBILITY	INSIDER THREAT DETECTION DATA ANALYSIS & EXPLORATION	RISK-BASED STRATEGY ACTIVE BLOCKING INTEGRATED INCIDENT RESPONSE PREDICTIVE DETECTION

BY 2025, at least

75%

of IT organizations will face

ONE OR MORE ATTACKS.

Gartner[2]

50%

INCREASE in daily cyberattacks just in Q3 of 2020 alone.

Check Point Software Technologies[3]

Organizations Find It Expensive and Difficult To Build an Internal Security Operations Center (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.

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. SIEMs are difficult to maintain, have stale correlation rules, and are expensive from both a storage and management perspective.

What Is the Difference Between SIEM, MSSP, and 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: Provides remotely delivered, modern, 24/7 SOC capabilities to rapidly detect, analyze, investigate, and actively respond to threats.

… SO MANY ARE TURNING TOWARD 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
24/7	Technology Management	Detection and Response Platform
Expert Human Intelligence	Detection	Log Analysis
Security Analysts	Response	Network Analysis
Threat Hunters	Threat Intelligence	Endpoint Detection and Response
Incident Responders	Vulnerability Management	Forensics

Key Areas When Evaluating an MDR Provider

How do you know if adding MDR services is the right move for your organization? Gartner suggests that you consider an MDR provider if you need remotely delivered, modern, 24/7 SOC functions and there are no existing internal capabilities or if you need to accelerate or augment existing capabilities. You should also consider an 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 and Cloud Assets:** Can the provider support your on-premises and cloud environments?
- **Custom Reports Including Compliance:** Does the MDR provider offer 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? Does the provider offer real-time alerts? Are the alerts reviewed by experts to alert you only when action is needed to stop an attack?
- **Incident Response and Remediation:** Does the MDR provider offer incident response capabilities? Can the provider help minimize losses and prevent future incidents?
- **Experience With Your Industry:** Does the provider have experience with your industry? Does the provider work with other organizations that are similar in size to yours?

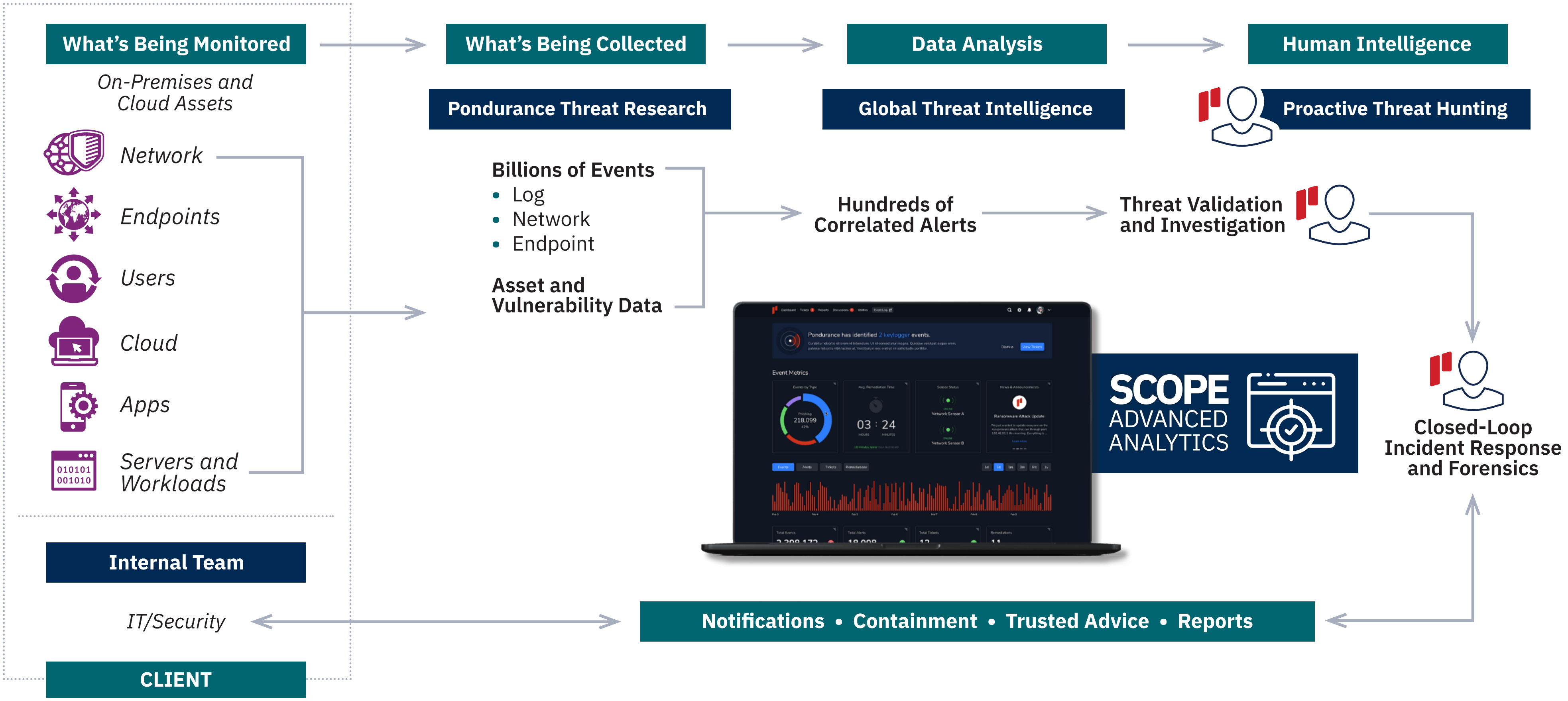
When you are looking for a new vendor, you want to find the one that works best for your organization. Find out whether the vendor specializes in your industry, is able to integrate with your current technology stack, or is able to monitor your cloud environments.

The right MDR vendor will fit into your organization and current security protocols. The vendor 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

Meet Human Experience, Intuition, and Unwavering Curiosity



What's Being Monitored

On-Premises and Cloud Assets

- *Network*
- *Endpoints*
- *Users*
- *Cloud*
- *Apps*
- *Servers and Workloads*

Internal Team

IT/Security

CLIENT

What's Being Collected

Pondurance Threat Research

Billions of Events
- Log
- Network
- Endpoint

Asset and Vulnerability Data

Data Analysis

Global Threat Intelligence

Hundreds of Correlated Alerts

Human Intelligence

Proactive Threat Hunting

Threat Validation and Investigation

Closed-Loop Incident Response and Forensics

SCOPE ADVANCED ANALYTICS

Notifications • Containment • Trusted Advice • Reports

How Pondurance Can Help

Our mission is to ensure that every organization is able to detect and respond to cyberthreats — 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 U.S.-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 cyberthreats.

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

INCIDENT RESPONSE

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

Pondurance delivers digital forensics and incident response 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

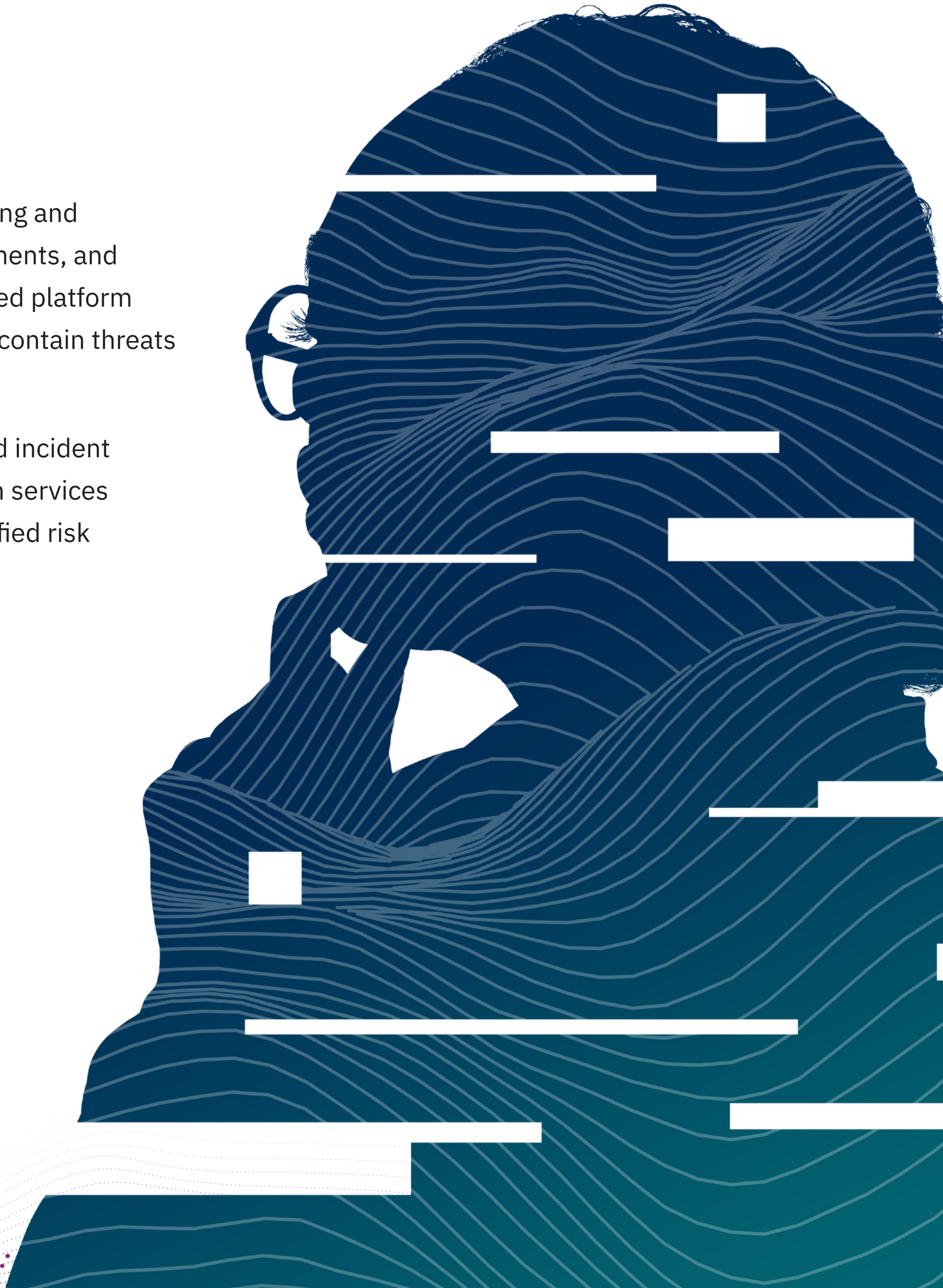
Our specialized consultancy services will help you assess systems, controls, programs, and teams to uncover and manage vulnerabilities. Our suite of services ranges from penetration testing to red team exercises, along with compliance program assessments for highly regulated industries. We provide security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

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.



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