PONDURANCE

5 MDR Considerations for Healthcare Organizations

pondurance.com

Cyber Threats Continue To Grow And Are More Profitable When Lives Are at Risk

Healthcare is one of the largest and fastest-growing industries, requiring around-the-clock cybersecurity support. As the industry continues to grow, healthcare providers will process more protected health information as a result of providing patient services. The road map to improve such care broadens the attack surface with complicated IT systems, HIPAA compliance requirements and legacy medical devices.

Managed detection and response (MDR) use within the healthcare industry is growing. Overall, Gartner estimates that 50% of organizations will use MDR services by 2025.[1] After reading this guide, you will have a better understanding of why healthcare organizations like yours are turning to MDR service providers for help. This guide covers:

- **The difference between SIEM, MSSP and MDR**
- **Components of MDR**
- **How to evaluate MDR vendors for your healthcare organization**
- **Pondurance's approach to managed detection and response**

50%

of organizations will use

MDR SERVICES BY 2025[1]

Gartner

PONDURANCE

If You Experience These Challenges When Trying To Protect Your Healthcare Organization From Cyberattacks, You're Not Alone

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 isn't enough to stop motivated attackers

HIPAA compliance and regulation requirements

Undocumented processes in the event of an attack or breach

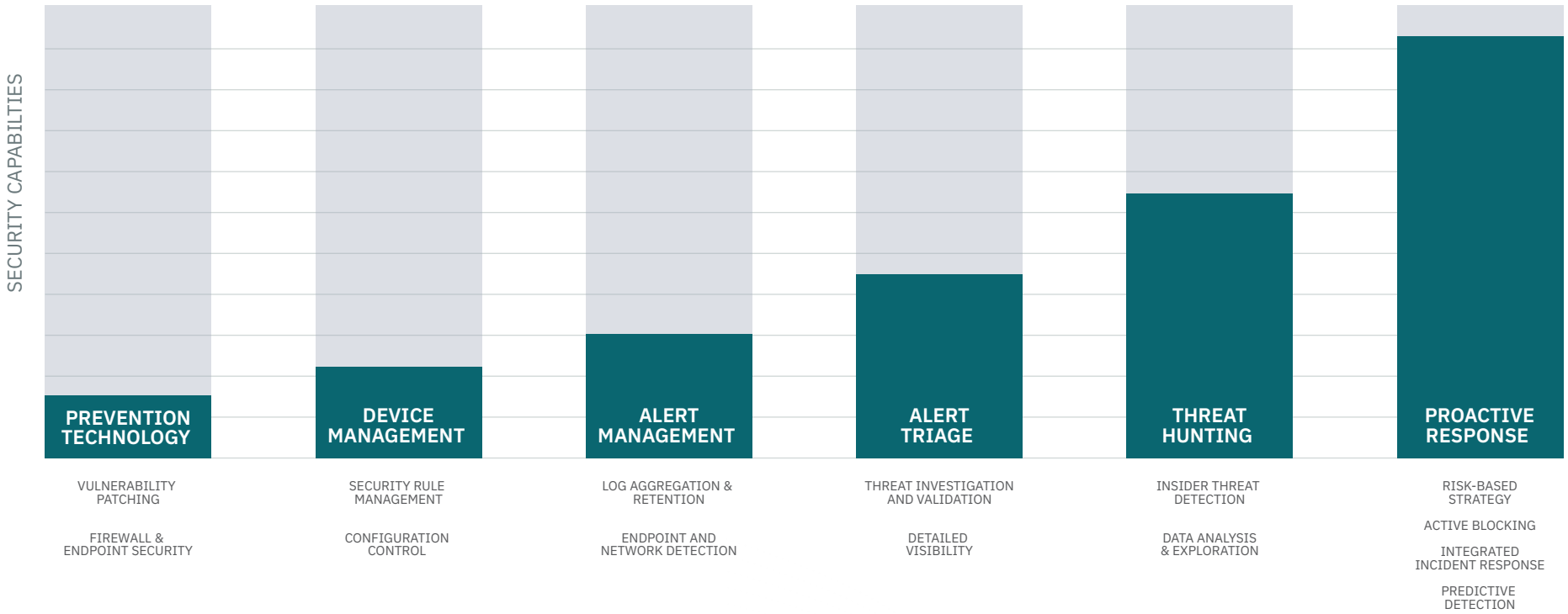
Lack of visibility across the enterprise

Inability to quickly remediate or reduce attacker dwell time

PONDURANCE

How Mature Are Your Security Operations?

CONSIDER HOW MDR CAN HELP STEP UP YOUR HEALTHCARE SECURITY OPERATIONS MATURITY



PONDURANCE

The average cost of a healthcare organization breach is

$9.23 MILLION.[2]

IBM

HEALTHCARE DATA

is one of the **most common types of data exposed** in data breaches.[2]

IBM

Healthcare Organizations Like Yours Find It Expensive and Difficult To Build an Internal Security Operations Center (SOC)

AS A RESULT, MANY 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 outdated and legacy medical devices.

Healthcare facilities like yours continue to be prime targets for ransomware attacks, mainly due to the complex digital landscape, compliance requirements, and the valuable source of sensitive data processed. The average cost of a data breach for a healthcare organization is 218% more than organizations overall.[2] The ransom payments are only part of the total cost of the attack, while other contributors such as downtime, legal, public relations, and more have a significant impact on any healthcare organization's bottom line.

Could an MSSP or SIEM Help With Your Healthcare Organization's Challenges?

Many MSSPs and SIEMs do not have the detection and response capabilities that healthcare networks require. They only alert the security teams, which causes a backlog of tickets to search through, often creating false positives that lead to alert fatigue. Many healthcare IT and security professionals spend more time triaging alerts from MSSPs than they can respond to.

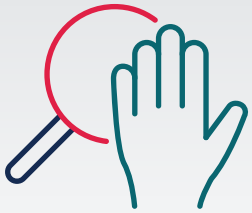
SIEMs are difficult to maintain, have stale correlation rules and are expensive from both a storage and management perspective.

What Is the Difference Between SIEM, MSSP, and MDR?

SIEM: Supports threat detection, compliance and security incident management through collection and analysis of security events.

MSSP: 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.

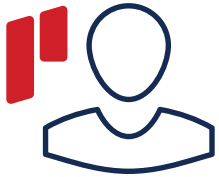


MDR MAY BE THE ANSWER FOR YOUR HEALTHCARE ORGANIZATION

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

PONDURANCE

What Should You Look For In An MDR?



PEOPLE	PROCESS	TECH
24/7 Security Analysts	Technology Management	Detection and Response Platform
Expert Human Intelligence	Detection and Response	Log Analysis, Network, and Cloud Analysis
Threat Hunters	Threat Intelligence	Endpoint Detection and Response
Incident Responders	Vulnerability Management	Forensics

Is Partnering With MDR Services Right for Your Healthcare 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 significantly enhance your security operations while leveraging your existing IT investments?
- **Fits with your policies:** Does the MDR provider's containment approach integrate with your organization's policies and procedures?
- **Monitor across your IT environments:** Can the provider detect and respond across your network, log, endpoint, and cloud infrastructure?
- **Custom reports including compliance:** Does the MDR provider offer custom reports including those needed for HIPAA 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? Will they work with you to respond to threats through instant triage and integrated services? Can the provider help minimize losses and prevent future incidents?
- **Experience with your industry:** Does the provider have experience with the healthcare 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 healthcare infrastructure. Find out whether the vendor specializes in the complex healthcare landscape, is able to integrate with your current technology stack, or is able to monitor your cloud environments.

The right MDR vendor will fit seamlessly into your healthcare organization and existing security protocols. The vendor must have decades of experience working with the complex IT landscape, medical devices and endpoints, and healthcare infrastructure so you can stay one step ahead of attackers.

Pondurance Approach to MDR

Human Experience, Intuition and Unwavering Curiosity Meet AI and Machine Learning

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
- Cloud

Asset and Vulnerability Data

Data Analysis

Global Threat Intelligence

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 You

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

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 network, log, endpoint, and cloud data and with proactive threat hunting, we reduce the time it takes you to respond to emerging cyber threats.

Pondurance MDR is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyberattacks. 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 you 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.

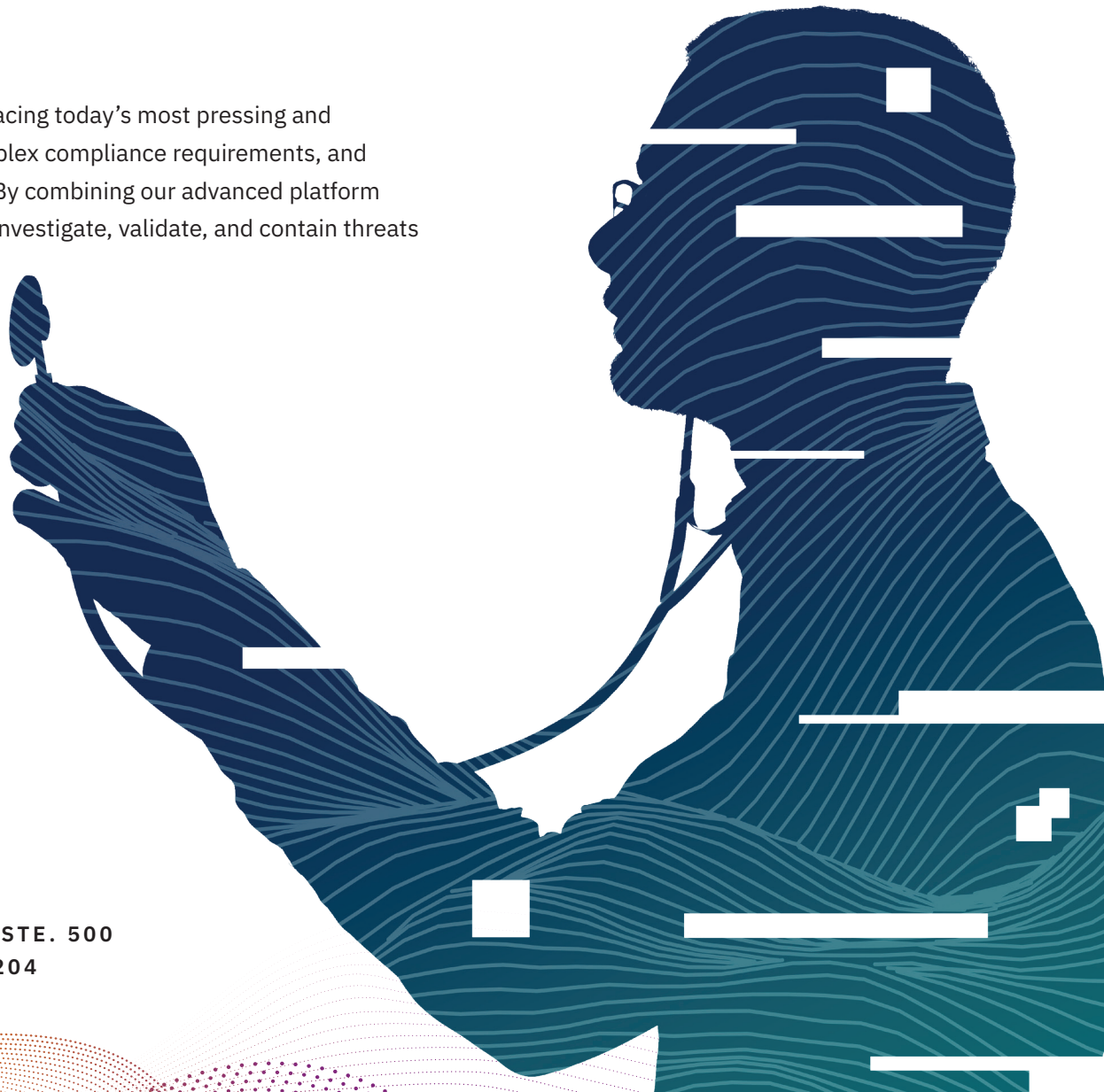
PONDURANCE

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

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



Sources:
1. Market Guide for Managed Detection and Response Services, Gartner, Oct 2021.
2. Cost of a Data Breach Report 2021, IBM, 2021.

pondurance.com

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