MDR Buyer's Guide

Selecting
a Managed
Detection
and Response
(MDR) Service

ARCTIC WOLF

MDR Buyer's Guide

In the era of digital transformation, many organizations find it a never-ending struggle to defend against rampant cybercrime. Preventative security is no match for today's threat actors, yet the advanced cybersecurity capabilities that organizations need are beyond the level of maturity that small-to-midsize enterprises (SMEs) possess.

At the same time, the expanding attack surface makes the IT environment increasingly vulnerable. Identifying and managing vulnerabilities has become exponentially more complex with more devices joining the corporate network, a mobile workforce connecting to the network from anywhere, and applications moving to the cloud.

Given the limited in-house resources, the cybersecurity skills gap, and the rapidly growing number and sophistication of threats, it doesn't surprise anyone that security teams can't keep up.

In this kind of reality, a data breach or network outage is all but inevitable. And the result is not only loss of productivity and revenue but also potential liability, regulatory noncompliance, and reputational damage. The ripple effects of these consequences can last for years.

Organizations are starting to recognize the inherent challenges that come with the lack of advanced technology and professional experts on staff. The question then becomes: What is the answer to the dilemma they face?

Table of Contents

MDR Buyer's Guide

LEVELING THE FIELD WITH MANAGED DETECTION AND RESPONSE

41%

The percentage of organizations seeing more than 10,000 alerts every day

— 2019 CISO Benchmark Study, Cisco

$11.7M

The cost of cybercrime to global organizations on average per year

— 2017 Cost of Cyber Crime Study, Ponemon Institute/ Accenture

$3.86M

The average cost per data breach or $148 per record

— 2018 Cost of a Data Breach Study, Ponemon Institute/IBM

As the threat landscape evolves, so must your defense strategy. But trying to stay ahead of the curve has become increasingly difficult.

Alert triage can simply overwhelm security teams, particularly those that are understaffed. Research shows teams only respond to approximately half the alerts they see on a daily basis[1]. And with 41% of organizations seeing more than 10,000 alerts every day[1], too often the doors are wide open for attackers.

These inadequate defenses come with a significant price tag that affects both the top and bottom lines. On average, cybercrime costs global organizations $11.7 million per year[2]. Additionally, the costs of data breaches continue to escalate — currently reaching $148 per record, or an average of $3.86 million per breach[3].

Managed detection and response (MDR) is an increasingly popular approach that addresses these security monitoring challenges, as it delivers real-time, 24x7 managed detection and response using a holistic, turnkey approach. As a cost-effective alternative to building an in- house security operations center (SOC), MDR protects against advanced threats and enables organizations of all sizes to follow cybersecurity best practices even within resource constraints.

Quick Reference

- **Endpoint Detection and Response (EDR):** A second-generation endpoint security solution focused on advanced threats, including continuous monitoring and response.
- **Intrusion Detection System (IDS):** A hardware or software appliance that provides real-time monitoring of network traffic and creates automatic alerts upon detection of indicators of compromise (IOCs).
- **Incident Response:** An organized, systematic approach to addressing the impacts of a security incident or data breach with the goal of limiting the damage to the infrastructure and the business.
- **Managed Detection and Response (MDR):** A comprehensive service for continuous monitoring, threat detection, and incident response provided by a third-party vendor.
- **Managed Service Provider (MSP):** An IT vendor that provides a service, software, or technology, such as remotely managing IT infrastructure, on a subscription basis.
- **Managed Security Service Provider (MSSP):** An MSP that provides 24x7 management, monitoring, and maintenance of security services, such as intrusion detection and endpoint protection, at a fixed subscription cost.
- **SIEM (Security Information and Event Management):** An integrated system that combines security information management and security event management to collect and correlate security events and alerts.
- **SOC (Security Operations Center):** A centralized approach that combines security technology, people, and processes to manage threats—from prevention and detection, to investigation and response.
- **Threat Hunting:** Proactive searches of data to identify stealthy threats that have evaded perimeter controls and are hiding on the network or endpoints.
- **Threat Intelligence:** Evidence-based data about current and potential threats, including context, indicators of compromise, mechanisms, and actionable information.

MDR Buyer's Guide

THE ADVANTAGES OF MDR SERVICES

25%

Percentage of organizations using MDR by 2024, compared to less than 5% in 2019

— Market Guide for Managed Detection and Response Services, Gartner

Gartner forecasts that 25% of organizations will use MDR by 2024, compared to less than 5% in 2019[4]. The market is growing in response to organizations' need to close the gaps in their ability to manage threats around the clock.

MDR enables companies to expand capabilities beyond in-house resources. The advantages of MDR services include:

- **Better technology:** MDR providers use advanced technology and a comprehensive suite of tools.
- **An integrated approach:** A framework that integrates threat detection and vulnerability assessment enables you to more efficiently manage risks from both known and unknown threats.
- **Greater expertise:** MDR vendors employ seasoned cybersecurity specialists who have needed expertise, have a wide range of skills, serve as dedicated teams, and understand clients' particular business needs.
- **Cost-savings:** The technology and 24x7 staffing of a SOC are cost-prohibitive for many organizations, while using an MDR service acts as a force multiplier that is easy on a budget.

MDR vs. MSSP vs. EDR

Managed detection and response takes a different approach from managed security services. Managed security service providers (MSSPs) focus primarily on functions such as managing vulnerabilities, monitoring network traffic, and remotely managing devices (like firewalls for example). The capabilities of legacy MSSPs are typically limited to known threats and don't include mitigation.

MDR also differs from endpoint protection and response (EDR) because EDR solutions don't provide visibility into the network or cloud. Additionally, managing EDR agents still requires human resources — the already overworked and understaffed IT teams. And while many threats do enter the environment through endpoints such as workstations and mobile devices, relying largely on an EDR solution leaves other entry points exposed.

An MDR provider gives you contextual understanding of your environment and digs deeper into the nuanced details that make your environment vulnerable to threats. Unlike MSSPs or EDR providers, managed detection and response is a holistic approach that helps you monitor and understand your overall security posture while also improving compliance and reducing your risks.

> "Managed detection and response enables companies to expand capabilities beyond in-house resources. The advantages of MDR services include: Better technology, an integrated approach, greater expertise, and cost-savings.

MDR Buyer's Guide

KEY MDR FEATURES AND CAPABILITIES

Specific capabilities range from vendor to vendor. However, look for these five key features when exploring the market:

24x7, Real-Time Threat Detection

Cybercriminals don't keep office hours. A security incident can unfold at any time. You need a 24x7 team of security analysts and engineers who monitor and triage alerts, and actively respond to indicators of compromise when they occur. You can't afford to wait for a report delivered to you hours or days later.

Threat Intelligence Integration

To reduce the risk of advanced threats, you need the latest threat intelligence from multiple sources. MDR solutions that integrate threat intelligence, as well as behavior analytics, are much better positioned to analyze data in the right context and to detect advanced, unknown threats.

Incident Response

The longer your dwell time, the more expensive your remediation becomes. The mean time to identify (MTTI) a breach is 197 days — but companies that identify a breach in fewer than 100 days can save $1 million[3]. MDR providers include different degrees of incident response as part of their base fee, along with crisis support.

Threat Hunting

Defenses based on point-in-time scanning or signatures can no longer keep up with today's stealthy threats like fileless malware. Proactive threat hunting goes beyond scanning files when they enter your environment. Instead, it relies on a combination of automated tools and human analysts to track activity and identify suspicious behavior even as a threat evades perimeter or endpoint controls.

Advanced Analytics

Through leveraging machine learning, threat intelligence, and big data, advanced analytics is a critical MDR component that enables real-time threat detection. Top providers invest heavily in analytics platforms and other tools to analyze data in context, as well as correlate events across the entire environment.

MDR Buyer's Guide

TOP CRITERIA FOR EVALUATING MDR VENDORS

Technology Stack Capabilities

While some providers employ EDR agents provided by an outside vendor, others offer a comprehensive, proprietary technology stack for SIEM. Using network sensors deployed on customers' premises, the provider's stack should include tools such as network traffic analysis and endpoint activity monitoring.

When researching MDR providers, ensure their technology stack fits within your IT and security technology, such as your point tools, and that you won't need to make an additional investment.

Ability to Monitor On-Premises and Cloud Assets

You need visibility into, and protection of, your entire environment—both on-premises and in the cloud. Many providers, however, only specialize in one or the other. As the adoption of IaaS and SaaS grows, monitoring those environments becomes more critical.

Although public cloud providers offer various native security features, you can't rely on those capabilities to keep your cloud secure.

Common Framework for Known and Unknown Threats

Many malware campaigns and other attacks exploit vulnerabilities that have had patches for months — and sometimes years. These tactics are successful because it's common for organizations to lack strong policies for managing vulnerabilities.

Some vendors offer a common framework that helps you identify these known vulnerabilities and prioritize patching, while at the same time the MDR solution continuously monitors for new threats that emerge in the wild. The added benefit is that you only need to work with one vendor to ensure you're covered in both areas.

4

Important Questions to Ask Vendors: Threat Hunting

What kinds of threats and suspicious activities does the solution monitor? Does it cover both known and unknown threats?

How does the vendor proactively hunt for threats?

Which sources of threat intelligence does the vendor use?

Which detection strategies does the vendor use to identify anomalies and find indicators of compromise?

MDR Buyer's Guide

TOP CRITERIA FOR EVALUATING MDR VENDORS (CONTINUED)

24x7 Eyes-on-Glass Monitoring

Threats can hit your organization at any time, and 24x7 live monitoring is a critical factor that determines your ability to detect and respond to a security incident quickly and effectively. Yet not all vendors offer around-the-clock staffing.

A vendor who doesn't have 24x7 eyes-on-glass monitoring leaves you with blind spots and a limited ability to detect malicious activity.

Real-Time Alerts, Time to Remediation, and Time to Respond

Reducing your time to respond and your time to remediation is critical during a security incident.

Weigh the response capabilities of prospective MDR providers —are they effectively monitoring, triaging, and investigating alerts in real time? Do they use a mix of human and artificial intelligence to shorten the time between detection and response?

Incident Response and Remediation Capabilities

Attackers can cause large amounts of damage in a short amount of time. Fast threat containment and remediation is crucial to minimizing the impact on your business.

You need an MDR partner with an experienced incident response team who can take immediate steps to facilitate a speedy remediation.

6

Important Questions to Ask Vendors: Process

Will you need to change your infrastructure or deploy new technology? Do you need to adapt to the MDR vendor's technology stack?

Does the vendor monitor and provide security around your existing applications and those you plan to use in the future?

Which types of updates and reports do they provide and how frequently?

Which log sources does the vendor collect and retain?

Can you directly search your log information?

How does the vendor's security experts engage/communicate with your in-house team?

MDR Buyer's Guide

TOP CRITERIA FOR EVALUATING MDR VENDORS (CONTINUED)

Compliance Reporting And Custom Reports

Regulatory compliance is a major concern for select industries, and MDR solutions need to adapt to this new regulatory environment.

Choose an MDR partner who offers reporting on policies for your compliance regime (PCI, DSS, HIPAA) and areas such as data privacy and network mapping— you'll not only simplify compliance, but also reduce audit costs.

Predictable Pricing

It's difficult to budget for security if your MDR provider charges based on log volume. Imagine the costs when an incident requires sifting through a large collection of activity data.

A fixed recurring price that's based on your attack surface rather than log volume simplifies your pricing structure while helping with cost control.

Consistent Relationships with Dedicated Advisers

If you have to work with a different analyst every time you have an issue or a question, your security expert doesn't really have the complete understanding of your business and operations. Conversely, when a vendor provides a dedicated team of experts and a single point of contact, you can build a trust-based, consistent relationship.

A consistent team is the foundation for having the MDR service be an extension of your internal team.

5

Important Questions to Ask Vendors: Service Offering

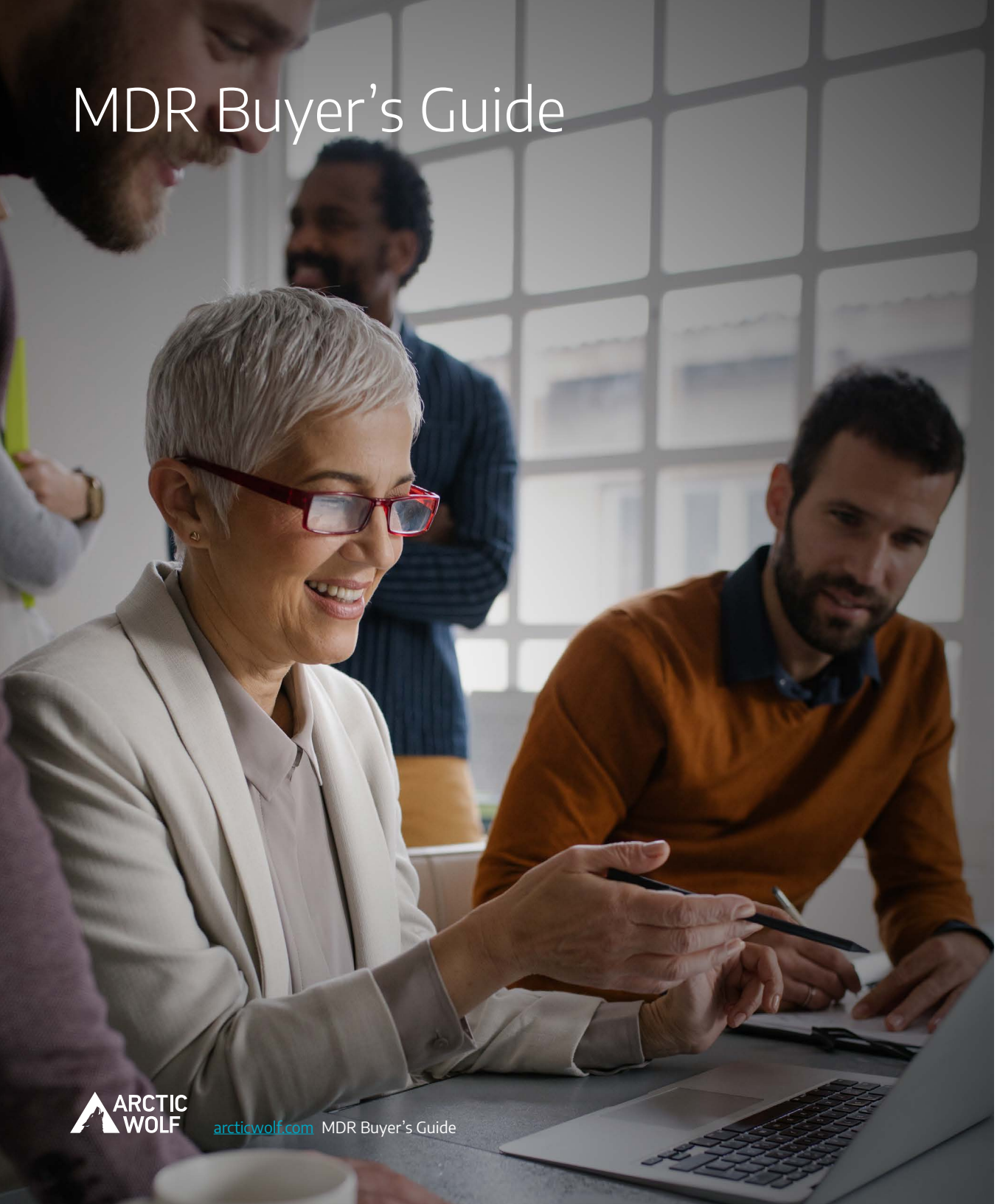
Does the vendor also offer risk management services on the same incident framework?

Will you receive a dedicated point of contact/support?

How do the vendor's services scale/tailor to your needs?

Are both cloud and on-premise infrastructure security monitored? What cloud assets?

What is the vendor's pricing model? Is it a fixed subscription price or based on log volume?



FINAL THOUGHTS

Whether your organization doesn't yet have internal detection and response capabilities or just needs more flexible technology choices, a managed detection and response service can help you keep up with the changing threat landscape. But, not all MDR providers are the same. It's important to ensure the service fits your organization's specific needs, size, existing security capabilities, and maturity level.

A trusted MDR provider is not just about technology and expertise. Find a partner who will get to know your business deeply and will build a long-lasting relationship with your internal team. An effective approach to threat detection and response requires both trust and collaboration.

About Arctic Wolf: Arctic Wolf Networks delivers the industry-leading security operations center (SOC)-as-a-service that redefines the economics of cybersecurity. The Arctic Wolf Managed Detection and Response and Managed Risk services are anchored by Concierge SecurityTeams™ who provide custom threat hunting, alerting, and reporting. Arctic Wolf's purpose-built, cloud-based service offers 24×7 monitoring, vulnerability assessment, threat detection, and response. For more information about Arctic Wolf, visit arcticwolf.com.

1. 2019 CISO Benchmark Study, Cisco
2. 2017 Cost of Cyber Crime Study, Ponemon Institute/Accenture
3. 2018 Cost of a Data Breach Study, Ponemon Institute/IBM
4. Market Guide for Managed Detection and Response Services, Gartner