A BUYER'S GUIDE
Five critical criteria for evaluating managed detection and response providers
Introduction

The threat landscape is increasingly complex and dynamic. Threat actors are well-funded, resolute and innovative in creating new tools and techniques to advance their mission. Organizations quickly learn that technology alone will not stop determined adversaries. But when organizations try to outsource managed security, vendors often don’t meet expectations:

• Legacy managed security solutions designed to provide cost-effective compliance and device management can detract from risk mitigation efforts because they often overemphasize alert management.

• When an organization enhances or upgrades its security infrastructure, outsourcing costs can increase dramatically based on the additional number of sites, personnel and endpoints.

• Most managed security providers play the role of tier one analysts focused on alert validation and notification, rather than decreasing attacker dwell time — the amount of time an actor remains in your environment.

• The detection capabilities of legacy managed security solutions are primarily limited to identifying known threats that attempt to enter the network, but once the network perimeter is breached, ongoing attacker activities often go largely undetected.

The emerging managed detection and response (MDR) service market addresses the need for realtime threat detection and response. But when each vendor takes a different approach to creating and delivering services, you need to determine how their approaches will protect your organization.

This Buyer’s Guide helps you identify and evaluate the most critical capabilities of MDR service providers and includes a checklist of pertinent questions to assess a prospective vendor’s approach. By applying this guidance, you can make better security investment decisions that effectively defend your organization against cyber threats.

$3.92 MILLION
The average cost of a breach

2019 Ponemon
Cost of a Data Breach Study
Capability #1

Threat Intelligence is the Foundation for Detection

Real-time threat detection starts with thinking like an attacker. What is their motivation? Who are their targets? What infrastructure will they need to carry out their attack? What capabilities will they need to acquire?

An effective MDR vendor has a varied set of intelligence sources that are operationalized into comprehensive, actor-specific playbooks that inform detection, investigation and response activities. Threat Intelligence sources should include:

- **Adversary intelligence** from hundreds of threat researchers embedded deep within the adversary’s development ecosystem that provide insight into the earliest stages of threat initiation.

- **Victim intelligence** gained from over a decade on the front lines investigating the world’s most consequential breaches.

- **Machine intelligence** derived from analysis of global detection technology, that provides real-time visibility into attack telemetry and proliferation.

- **Geo-political analysis** by experts from diverse domains who rigorously track and analyze the financial and political dimensions of thousands of cyber threats worldwide.

Comprehensive, actor-specific playbooks provide extensive insight into the identities, motivations, intentions and methods of adversaries to accelerate detection, investigation and response. For example, watching an adversary acquire new tools and infrastructure enables the creation of pre-emptive defenses against attacks before they launch. Rather than reactively responding to alerts, effective MDR vendors proactively hunt for covert activity using hunt scenarios from attacker playbooks specific to your industry. The intelligence in these playbooks should also inform investigation activities to help determine the scope, tools and techniques and anticipated path of threat actor operations in your environment.

Ask These Questions When Evaluating the Threat Intelligence Your MDR Vendor Uses

- What intelligence sources does your vendor use beyond simple data feeds?
- How quickly can they apply intelligence gained from recent breaches to your environment?
- Can they tell you who is targeting your industry? And how?
- How frequently do they update the attacker playbooks for your specific industry?

---

*Know your enemy, know his sword*

Miyamoto Musashi
Capability #2
Hunting is an Iterative Process

Passively waiting for signs of intrusion won’t keep you safe. Today’s increasingly sophisticated attackers bypass legacy security controls, then continuously alter their techniques to evade detection. To detect emerging threats, organizations must move from reactive alert monitoring to proactively hunting for the unknown. Hunting isn’t about searching for indicators of compromise (IOCs). By definition, IOCs are known. Expert hunters think differently — they systematically combine knowledge, intuition and automation to proactively search for covert signs of an active or attempted compromise.

Expert hunters create attacker playbooks containing dynamic hunt scenarios developed through their extensive knowledge of attacker tools, techniques and procedures (TTPs). Using these hunt scenarios, they sift through massive amounts of data to identify patterns of anomalous behavior. Continuous exposure and response to critical cyber attacks gives expert hunters a finely-honed intuition regarding attacker behavior, tactics and targets. When they discover anomalous activity, they can quickly form and test hypotheses around the attacker’s next moves to formulate a definitive response.

To keep pace with the velocity of change seen in the threat landscape, hunting must be viewed as a continuous, iterative process of discovery and development. As hunters refine their understanding of adversaries and attack techniques, they must develop automated hunting processes to systematically apply and scale their efforts.

Ask These Questions When Evaluating an MDR Vendor’s Hunting Capabilities

- How do their hunting techniques extend beyond searching for known IOCs?
- How often do they hunt for threats?
- What automated hunting techniques can they frequently, reliably and systematically apply?
- In what ways do their hunting techniques inform product detection capabilities?
Capability #3

Hunting Drives Technology Innovation

Gartner’s definition of MDR providers includes the delivery of services using the vendor’s curated technology stack to free customers from the burden of selecting and maintaining protection technology. MDR providers should also use what they learn from protecting their customers’ environments to improve the technologies they deploy.

Legacy managed security providers typically spend their time correlating logs from hundreds of products limited to signature-based detection. They don’t tell you anything you don’t already know. An effective MDR provider correlates information from multiple layers of detection analytics, systematic analyst-driven hunting processes and supplementary network and endpoint evidence to reveal anomalous activity at each stage of the attack lifecycle.

By using a consistent technology stack for every customer, MDR providers can build up large datasets on alerts, context and investigative decisions. These analyst decisions become another source of knowledge that can be applied to continually improve the efficacy of the associated technology products. When analyst hunting activities identify changes in attacker TTPs, such insights should be swiftly translated into new product detection capabilities and indicators of compromise (IOCs).

Ask These Questions to Evaluate an MDR Provider’s Detection Analytics

• How does the vendor maintain cyber security domain expertise?
• How extensive are the connections between product development and the vendor’s frontline security experts?
• How quickly can they transform changes in the threat landscape into product detection capabilities?

Median dwell time 2019

2020 M-Trends Report
Capability #4
Incident Investigation Provides Answers, not Alerts

Because traditional managed security providers lack a proprietary technology stack, they use the alerts generated by an organization’s existing security products. Their services focus on rapid alert validation and notification, limiting the vendor’s role to a tier one analyst who simply passes alerts to the client. This typically leaves organizations with an overwhelming number of notifications and no understanding of the probable identity or motivations of threat actors.

Because most providers prioritize speed of reporting, the burden of investigation lies with the client organization. Instead of focusing on higher-order activities that ultimately reduce attacker dwell time, security teams still spend an inordinate amount of time running down false positives.

In contrast, effective MDR vendors provide answers, not alerts. They fundamentally reject a log-based approach as the starting point for real-time threat detection and response. Although device alerting is still useful as supplementary evidence, effective MDR providers rely on a proprietary technology stack that supports the entire security operations workflow, from analyst-driven, intelligence-based detection to investigation to response.

MDR vendors use an intelligence-led approach that combines analyst-driven detection with correlated incidents from a proprietary technology stack to drive targeted investigations. MDR vendors employ extensive knowledge of threat group behavior with rigorous investigation methods to discover signs of intrusion, learn how attackers are operating and assess their capabilities. Throughout an investigation, outcome-oriented MDR vendors continually update Investigation reports to include the context needed for organizations to fully understand the scope of the attack, information to help assess risk and definitive remediation recommendations.

Ask These Questions When Evaluating How Your Vendor Investigates Incidents

- What kinds of information do they provide in addition to reporting alerts?
- How effectively do their reports convey the context around likely threats and any correlated activity?
- What sort of evidence is provided to establish the identity, methodology and attack timeline of suspected threat actors?
Capability #5
Rapid, Definitive Remediation and Response

No matter how good your security is, experiencing a breach is inevitable. Response and remediation services are critical to reducing dwell time during priority incidents. Outcome-oriented MDR providers must offer a full spectrum of response capabilities to match the scope of different attacks to the specific needs of a target organization.

After a breach, every second counts. Organizations need on-call incident response that can quickly contain affected computer systems and disable known operational capabilities of the threat actor. On-call incident response experts should swiftly validate potential incidents, provide appropriate context, investigate as much as is feasible about scope and severity, make recommendations and guide or inform methodical remediation. After the investigation, orchestration tools should be employed to automate and accelerate response activities, further reducing dwell time and risk.

Lastly, when organizations have disclosure duties, loss and exposure can be minimized if they have both as complete a picture of the compromise as possible and the ability to pull in additional response resources.

Ask These Questions When Evaluating Remediation and Response

• What range of response services do they offer?
• What types of remediation recommendations do they provide beyond “wiping the box?”
• How will their analysts collaborate with your internal team?
• How frequently is the vendor called on to respond to consequential breaches? How long after your initial call will they begin their investigation?
Summary

The legacy of compliance-oriented security services and alert-driven detection has been quickly outpaced by increasingly sophisticated adversaries using constantly evolving methods of attack. To keep up, companies need to go beyond legacy detection solutions and enlist MDR providers that evolve just as quickly.

As new MDR vendors compete for mindshare and dollars with similar-sounding offerings, it can be difficult to distinguish which ones provide definitive detection and response capabilities. The five criteria outlined in this guide provide customers with a way to understand and evaluate MDR options.

True MDR providers blend technology with human expertise in tracking and spotting novel TTPs to investigate, remediate and respond to threats. Organizations should understand the importance of focusing on intelligence-driven hunting, analytics, investigation and response using purpose-built technology.

Organizations should consider outsourcing security functions to a trusted MDR provider with solutions tailored to their needs. And every dollar spent on such services should translate directly into reduced business risk.

Make sure your MDR provider is up to the challenge.

By 2024, **25% of organizations will be using MDR services**, up from less than 5% today.

*Gartner Market Guide for Managed Detection and Response Services*
*July 2019*
About FireEye Managed Detection and Response Services

FireEye Managed Defense is a managed detection and response (MDR) service that leverages the full power of FireEye to relentlessly protect our customers from impactful cyber attacks.

To learn more about FireEye, visit: www.FireEye.com