CLEARNETWORK

# MDR
# Evaluator's Guide

# Executive summary

Partnering with a third-party provider for managed security services is a smart way for small to mid-sized businesses with limited security resources to deploy a detection-based security strategy that meets their internal needs, compliance requirements and their budget. As the cyber threat landscape accelerates and evolves and the supply of cybersecurity talent fails to meet demand, many organizations are choosing to work with a managed detection and response (MDR) provider rather than trying to meet their own cybersecurity needs in-house.

The growing demand for MDR services has resulted in an explosion in the number of providers with a wide range of capabilities and available services. When evaluating potential MDR providers, it is important to look past the minimum (the ability to provide a 24x7 detection and response) to the specific services that the provider offers and other factors that can affect their quality of service.

The choice of an MDR provider has a significant impact on an organization's security and long-term profitability. Many organizations go out of business soon after becoming the victim of a cyberattack or data breach. When choosing an MDR provider, it is important to consider the following factors.

Elements to consider

# Alert Monitoring and False Positive Detection

The primary reason for partnering with an MDR provider is to simplify your organization's security operations. If an MDR provider can't make day-to-day security operations easier for your organization, then they're not worth the investment.

The average SOC sees 10,000 security events per day, and over 80% of these are false positives. Some MDR providers will simply aggregate all of the events for a customer's network and forward them on to the internal security team to sort out.

An MDR provider should evaluate every event produced by a network's security infrastructure and only escalate those indicating true threats to the internal security team. Accomplishing this requires adequate manpower and processes and procedures for investigating and evaluating the severity of security events. Look for an MDR provider that focuses on providing accurate analysis of the severity of an alert instead of quickly notifying you of any security event on the network.

## Elements to consider

# Cloud Visibility and Control

Over 96% of organizations have adopted cloud computing at some level, and 81% of public cloud users use multiple cloud providers. As businesses increasingly move sensitive data and critical business practices onto cloud-based infrastructure, the importance of securing the cloud is growing.

Achieving visibility and security for cloud-based resources is very different from on-premises deployments. The Cloud Shared Responsibility Model means that cloud service providers (CSPs) and cloud customers have responsibility for securing different levels of cloud infrastructure. In many cases, securing the portions of the cloud infrastructure that are the customer's responsibility requires understanding and properly using CSP-provided security controls and configuration settings.

As the cloud becomes an increasingly common part of businesses' network infrastructure, it is important to look for an MDR provider that provides complete security visibility and control in cloud environments. This should include seamless visibility into on-premises, public cloud, and private cloud environments, scanning for misconfigured cloud security settings, and the ability to enforce the organization's security policies procedures consistently across the entire network deployment.

Elements to consider

# Compliance Management and Reporting

The regulatory landscape for data protection has increased dramatically in recent years. These regulations include national, regional, and state-level regulations like the EU's General Data Privacy Regulation (GDPR) and the California Consumer Privacy Act as well as laws and standards designed to protect certain types of sensitive data or data in certain industries, including the Payment Card Industry Data Security Standard (PCI DSS) and the US's Health Information Portability and Accessibility Act (HIPAA).

Generally, compliance with data privacy laws requires demonstrating that certain security controls, policies, and procedures are in place within an organization. An MDR provider will provide many of the key functions necessary for compliance with most data protection regulations.

At a minimum, an MDR provider should provide the level of visibility and access to security data necessary to generate reports for compliance audits. However, some MDR providers go beyond this by providing pre-generated compliance reports that can be automatically populated based upon an organization's security data. As the compliance landscape grows more complex, an MDR provider that helps with compliance audits and reporting can generate significant time and cost savings for an organization.

Elements to consider

# Deployment, Configuration, and Onboarding

Organizations partner with an MDR provider to improve the security of their network. The longer that it takes to get an MDR provider's defenses and monitoring solutions in place, the longer that the customer is left vulnerable to attack.

Deploying and configuring an MDR's security infrastructure to protect the customer's unique network can take some time; however, it is important that the process is completed as quickly as possible. This includes everything from the initial consultation and signing through to "turning everything on" and providing full service to the customer.

While an MDR provider may give sample deployment timelines, it is possible that "unforeseen issues" could delay deployment. When evaluating an MDR provider, look for one willing to provide customer testimonials and references regarding how quickly they are able to onboard a new customer.

Elements to consider

# Flexibility and Scalability

The cyber threat landscape is rapidly evolving and so is the average business network. An example of this is the rapid adoption of cloud computing and deployment of Internet of Things (IoT) devices in business contexts. Over a third of businesses currently use IoT devices, and the number is increasing.

When choosing an MDR provider, it is important to plan not just for the organization's current network environment but for the future as well. While an organization may not currently be using the cloud or IoT, digital transformation efforts may cause this to change in the future. An organization's network may also grow and evolve in other ways, such as expanding the number of employees or opening up satellite locations. When choosing an MDR provider, it is important to look for one that can secure the business as it grows and evolves.

Evaluating the flexibility and scalability of an MDR provider requires visibility into their pricing models and history. It is better to know up front if MDR solution pricing is based upon headcount or number of locations than to be surprised when the need for growth arrives. If an MDR provider can provide customer testimonials and references regarding how the provider helped them throughout the growth and evolution of their business, this is a good sign for the future.

Elements to consider

# Incident Detection and Response

Detecting and responding to potential security events is a core part of an MDR provider's duties. The longer that an attacker remains undetected within an organization's network, the greater the cost and impact of the cyberattack. The fastest cyber threats can expand their foothold on an organization's network within 18 minutes of the initial compromise. If an organization can detect and respond to an incident within this window, the impact is dramatically reduced.

A core feature of an MDR provider is 24x7 detection and response. This SOC is responsible for continuously monitoring security events within an organization's network infrastructure, triaging them to eliminate false positives, and responding promptly to remediate any real threats.

An MDR provider's ability to respond rapidly to potential security events requires having the necessary security expertise on-hand and a plan in place before an incident happens. An effective provider will work with the customer during the onboarding process to determine an incident response plan and establish communication channels and procedures for use during a potential incident.

When evaluating a potential MDR provider, it is important to get hard data regarding their ability to detect and respond to incidents. The MDR provider should be able to provide data on their average detection and response time for security incidents and a sample procedure for how they respond to incidents. Requesting and reviewing this data is important to determining if a provider can meet an organization's security needs.

Elements to consider

# Provider Security Infrastructure

The complexity of the average business network is expanding rapidly. 96% of organizations have started using the cloud for business operations, and over two-thirds are currently using business IoT devices or plan to in the near future. As the complexity of an organization's network infrastructure increases, organizations must deploy a greater range of security solutions to achieve comprehensive security and visibility.

Protecting all of these different platforms against a rapidly evolving landscape of cyber threats requires an MDR provider with broad threat detection capabilities. Reliance on a single security product increases the probability that the MDR provider will miss some threats to the organization's network. By using several different products and cross-correlating their results, a provider can provide more comprehensive threat detection and protection and decrease the probability of false positive detections wasting analysts' time.

When evaluating a potential MDR provider, it is important to request information regarding their security infrastructure and determine how well it meets the organization's security needs. At a minimum, an MDR provider's general capabilities should include automated asset detection and vulnerability scanning, intrusion detection or prevention systems, and alert correlation and analysis via a security event and information management (SIEM) solution. More specifically, the provider should be able to monitor, manage, and protect assets across an organization's entire network infrastructure.

## Elements to consider

# SOAR Capabilities

Cybercriminals are increasingly leveraging automation in their attacks, allowing them to target more organizations and more rapidly move through the stages of an attack. A reliance on manual threat detection and response leaves an organization less capable of defending against these threats. By embracing automation, organizations can measurably improve their resiliency against attack, including a 23% improvement in threat detection and a 15% better response.

Security Orchestration, Automation, and Response (SOAR) is a crucial capability to look for when evaluating MDR providers. SOAR allows an organization to automatically collect and aggregate security data from multiple sources to determine if the network is under attack. For low-level security events, an organization can pre-program responses that the system can take automatically to respond to the potential incident. For example, detection of malware on the network could result in automatic blacklisting of associated domain names and IP addresses, ensuring that other instances of the malware are incapable of communicating with their command and control infrastructure.

As the cyber threat landscape grows and accelerates, protecting against common threats requires the ability to make strategic use of automation. An MDR provider should provide centralized visibility into an organization's security infrastructure and the ability to define automatic responses to common threats. This has the twin advantages of speeding up the organization's responses to common threats and relieving pressure on the organization's security team caused by low-level security events.

## Elements to consider

# Threat Intelligence

About 10 million new malware variants are detected each month. Most cybersecurity solutions, like antivirus, work by matching potential threats to signatures derived from known malware variants. Protecting against the latest threats to enterprise networks requires knowledge of which threats are currently active. In order to provide comprehensive threat detection and protection to an organization's network an MDR provider needs access to reliable and relevant threat intelligence.

Ideally, an MDR provider will have real-time access to a variety of internal and external sources of threat intelligence. Continuous access to threat intelligence feeds from external services allows an MDR provider to learn about and protect against new, widespread threats in real-time. By combining and cross-correlating data from multiple external sources, an MDR provider can achieve a high level of visibility into the current global threat landscape.

However, the ability of an MDR provider to generate threat intelligence in-house can be invaluable. An organization's MDR provider has the greatest visibility into their client's network and is most familiar with the types of threats that their customers might experience. More targeted threats aimed at particular organizations or industries may not appear on external threat intelligence feeds. Access to an in-house team of cybersecurity experts that process their customers' data to generate threat intelligence can allow an MDR provider to offer more personalized and comprehensive protection than a provider that is completely reliant upon external feeds.

## Elements to consider

# Transparency and Availability

Organizations outsource security to an MDR provider if they do not have the resources or desire to manage these functions in-house. However, just because an organization chooses to outsource their security monitoring to a third-party provider does not mean that they should not have visibility and control over their own cyber defenses. An MDR provider should be transparent regarding how they protect the client's network infrastructure and should be available for and responsive to questions regarding alerts and event data passed on to the customer's internal security team.

When working with an MDR provider, an organization is not just paying for their provider to protect their organization against cyber threats. A good MDR provider also acts as a resource and source of cybersecurity knowledge for their customers. A healthy relationship with open communication between the MDR provider and their customer makes everyone's job easier.

An MDR provider should provide customers with the expertise and guidance that they need to make cybersecurity decisions. This includes everything from design and reviews of cybersecurity and network architecture to help with understanding and achieving relevant data protection regulations. When evaluating an MDR provider, it is important to find out how they communicate with their clients and how a customer can access the data and logs generated by the MDR provider in the course of protecting the customer's network.

# Common Mistakes When Evaluating an MDR Provider

Selecting an MDR provider should be the beginning of a close and long-term relationship between the customer and the service provider. When evaluating different options, it is important not to make any of these common mistakes.

## Falling Prey to Sticker Shock

When evaluating a potential MDR provider, some organizations may experience "sticker shock" due to the cost of protection and consider performing some or all of the provided duties in-house. Before making this decision, it is important to fully consider the value of the benefits provided by the MDR provider.

With an average cost per cyberattack of over $1 million, an effective cybersecurity defense and threat hunting program can generate significant financial savings to an organization in the long term. A relationship with an MDR provider also removes the need to find and retain highly-skilled cybersecurity professionals for an in-house SOC and incident response team. Finally, partnering with an MDR provider allows an organization to reap the benefits of sharing the cost for specialized security products, threat intelligence feeds, etc. with the MDR's other customers.

## Failing to Plan Ahead

When shopping for an MDR provider, many organizations may focus on finding one that meets the organization's current security needs. However, the organization's network will likely grow over time and may expand to include new platforms and technologies like Internet of Things (IoT) devices and cloud computing.
When evaluating a potential MDR provider, it is important to compare their current capabilities to the organization's future goals and to learn how they typically adapt and evolve to address changes in how their customers do business. This information is vital to determining if the provider is a good fit for a long-term relationship.

## Geographic Limitations

The role of an MDR provider includes providing a 24x7 detection and response to protect an organization's network and cloud against attack. With round-the-clock protection, it doesn't matter as much if the provider is local or operates within the same time zone as the customer.
When evaluating a potential MDR provider, the focus should be on the services that the provider offers, not their location. In most cases, a national service provider can protect an organization's network from anywhere while providing storage of logs and any other data in the region of their choice (i.e. to comply with potential regulatory and legal guidelines).

## Service Lock-In

Partnering with an MDR provider can allow an organization to achieve a high level of security very quickly and with limited security infrastructure or knowledge on the part of the client. This can help an organization ensure that it is protected against cyberattacks while it focuses its resources on its core business needs.

While this may be desirable in the short term, in the long term an organization may wish to move some or all of their security monitoring and protection in-house. However, some MDR providers may be unwilling to support this, forcing the customer to rebuild their cybersecurity infrastructure from scratch.

When evaluating a potential MDR provider, it is a good idea to check to see if they provide a range of flexible service offerings. If so, this allows a customer to customize their security to meet their needs, instead of being locked into the terms of their initial relationship with their provider.

# Why Choose Clearnetwork?

| | |
|---|---|
| Alert Monitoring and False Positive Detection | • Clearnetwork makes it a priority to only show you valid threats, not waste your valuable time with false positives. |
| Cloud Visibility and Control | • Clearnetwork natively monitors<br>◦ AWS and Microsoft Azure public clouds<br>◦ Windows and Linux endpoints in the cloud and on prem<br>◦ Virtual on-premises IT on VMware / Hyper-V<br>◦ Physical IT infrastructure in your data center<br>◦ Other on-premises facilities (offices, retail stores, etc.)<br>◦ Cloud applications like Office 365 and G-Suite |
| Compliance Management and Reporting | • Clearnetwork provides “audit ready” reports for PCI-DSS, HIPAA, NIST, ISO-27001, NERC-CIP, SOX, SOC2 and more!<br>• C-Suite reports<br>• Configurable/custom reports |
| Deployment, Configuration, and Onboarding | • Clearnetwork MDR can be deployed in less than an hour<br>• Asset discovery<br>◦ API-powered asset discovery<br>◦ Network asset discovery<br>◦ Software and services discovery |
| Flexibility and Scalability | Clearnetwork MDR pricing is based on the monthly data ingestion capacity. All the essential security capabilities are included in the service and scale with each data |

| | |
|---|---|
| Incident Detection and Response | • 24x7 detection and response with human analysis<br>• Bi-monthly vulnerability assessments<br>• Regular Asset Discovery scans<br>• When a threat is identified our analysts immediately escalate it to your IT team with a complete action plan.<br>• We will call you for serious threats, and send a ticket/email for normal non-priority threats. With select devices/applications like Cisco Umbrella, Palo Alto Firewalls, Carbon Black Next Gen-AV and several others, we can even respond to threats directly for you. |
| Provider Security Infrastructure | • Platform based upon Alienvault<br>• Use Cisco Umbrella, Palo Alto Firewalls, Carbon Black Next Gen-AV and several others |
| SOAR Capabilities | • Clearnetwork analysts utilize SOAR as an essential part of their tech stack. This enables us to integrate the capabilities of disparate security and network systems into automated workflows that enable a fast response |
| Threat Intelligence | Clearnetwork receives continuous threat intelligence updates both internally and from multiple high-end sources. These dedicated teams spend countless hours researching and analyzing the different types of attacks, emerging threats, vulnerabilities, and exploits—so you don't have to. |
| Transparency and Availability | With read-only access to our system, and regular reports and calls from our analysts, you always know what we are doing. |