Economic Value from a Managed Detection and Response (MDR) Solution

CRITICALSTART®
They're good. We're better.

Overview

The pandemic has accelerated an organization's adoption of digital solutions. In fact, many organizations have adopted new business models and have shifted to more digital streams of revenue. In parallel, a high percentage of the workforce has moved remote. These factors broaden the attack surface available to malicious actors. As a result, the number of attacks has gone up significantly. This leaves many organizations with a very tough choice of spending either on top line activities like going digital or on resources to protect the organization. At Critical Start, we believe that you shouldn't have to make such unreasonable compromises. This white paper discusses how organizations can leverage an external MDR solution to help accelerate their business growth without compromising security. We focus on the factors influencing the costs of a Managed Detection and Response (MDR) solution and how an organization can benefit from a strong MDR partner.

Market Context

The Managed Detection and Response (MDR) is a relatively new market in cybersecurity but has gained significant traction over the past couple of years. Broadly, MDR solutions provide threat detection and response through a 24x7 security operations center (SOC) and technologies. Most industry analysts predict significant growth over the next few years. For example, Gartner (2020 Market Guide for MDR) predicts that by 2025, 50% of all organizations will be using threat monitoring, detection, and response functions. Reports and Data predicts that the global MDR market will grow to become a $4.6B by 2026, growing at a CAGR of 30.4%.

MDR solutions combine human expertise with advanced technologies to collect data, identify threats, and alert on security incidents. Additionally, they work with the organization's security team to respond and remediate key threats. These solutions adopt some of the latest technologies such as machine learning both for prevention, detection, and response.

Multiple factors drive the adoption of MDR solutions. Lack of cybersecurity talent has driven organizations to seek external experts to augment internal teams. According to the latest report from ISC2, there is at least 64% shortage of cybersecurity professionals. The US alone faces a shortage of 359,236 cybersecurity professionals today and globally, the shortage is close to 3M. This lack of talent has led to organizations seeking the assistance of external providers. The onset of the pandemic exacerbated this problem. Many organizations had to move their employees to a remote environment. In many instances, information security teams had less than 2 weeks to adopt to the new norms. As a result, there is a significant increase in the number of employees and end point devices. From an information security perspective, this has increased the threat surface rapidly. Additionally, as McKinsey recently pointed out, cybercrime has become more sophisticated and industrialized. While in the past the attackers exploited vulnerabilities for their own benefit, more recently, these attackers tend to lease ransomware to other intermediaries making it hard for organizations to detect attackers until very late in the attack cycle.

While the above factors drive adoption of MDR solutions, organizations need to evaluate their options on multiple vectors:

A. Integration with other security solutions

B. Coverage of threats

C. Overall cost of the solution

Adopting a MDR Solution – Integration with other security solutions

A strong MDR solution should help organizations reduce the Mean Time to Detection (MTTD) and Mean Time to Resolution (MTTR). To reduce MTTD and MTTR, MDR solutions should easily integrate with other security solutions in the organization. For example, integrations with Security Information and Event Management (SIEM), Endpoint Protection Platforms, network protection solutions, and other enterprise log sources should be quick, and standards based, ex. API connectivity. Additionally, the MDR solution should provide sufficient forensic and contextual information for incident remediation. Finally, the solution should also have a set of canned use cases that can be easily fine-tuned to an organization's environment and need. This will help the organization get a quick and effective start to monitoring their environment.

Overall Cost of the Solution

Focusing on just the price of the MDR solution being considered is one of the common pitfalls that organizations make. While it is true that the solution being considered must be priced commensurate to the value it delivers, very often, organizations don't account for the various cost factors that are either directly related or consequential to the kind of solution being considered. The following section lists some of the cost factors that need to be considered in the process.

Cost Factor A

Initial set up and Time to Value

Most organizations have at least the following characteristics when starting their MDR journey.

- **Multiple integrations to various security platforms such as Endpoint Detection and Response (EDR) solutions, firewall, VPN, directory services, and cloud security products.**
- **Baseline set of use cases for which they need immediate support**
- **Integration with a SIEM solution**

As the number of log sources or endpoints with which an organization needs to integrate increases, the time, effort, and cost of those integrations increase. An anecdotal observation is that an experienced MDR solution provider will take about 25% of the time an organization will take on its own. Moreover, in trying to get your full-time employees (FTEs) to provide that support, requires them to be removed from potentially more important security projects. An MDR provider comes with not just prior experience, but as in the case of Critical Start experts in specific areas and additional tools and technologies that have been built to ease such integrations and to reduce the time to value.

An anecdotal observation is that an experienced MDR solution provider will take about 25% of the time an organization will take on its own.

Once the integrations are up and running, an MDR solution like Critical Start will provide a baseline set of use cases that have proven to be effective in multiple customer environments. This collective body of knowledge ensures that most common and critical use cases and immediate threats are addressed quickly. It also ensures that the organization realizes value from the MDR solution very quickly.

Cost Factor B

Amount of data stored from log sources

Another challenge that many organizations face is the number of false positives they encounter when detecting threats. These false positives result in two opposing challenges. First, the cost (time and resources) spent in analyzing these false positives are high. Second, the same time and effort could easily have directed towards serving other starved areas within the organization. With a solution such as Critical Start, the MDR will ensure that only the relevant logs are consumed and analyzed. This helps in multiple ways. First, the noisy logs that typically cause false positives are vastly reduced, and only relevant logs and events are analyzed. This improves the quality of security event detection and remediation. Another important and often overlooked benefit is the cost of storage of the logs. For example, at Critical Start we have observed that we can filter out noisy logs and process just the relevant ones, a realize a saving of up to 75% in storage costs.

Cost Factor C

Personnel expenses

One of the biggest benefits of leveraging an MDR solution rather than taking a Do-it-Yourself (DIY) approach is the potential savings in personnel expenses. This should not be perceived as a reduced headcount, but as a more efficient deployment of talented cybersecurity professionals who are in real short supply. Very often, these expenses take multiple forms as explained below.

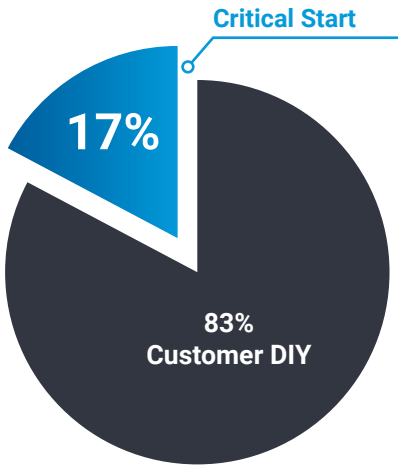
1. Higher attrition

When seasoned security professionals must detect and resolve low priority security events, over a period of time, they seek better opportunities. With a shrinking talent pool and significant demand, it is matter of time before such talented personnel are lost to attrition. On the other hand, such talented professionals are also in very high demand under current market conditions. With any attrition, one needs to consider the cost of talent search and the higher cost of employment.

2. Cross-product talent

If the organization has multiple security products, endpoint platforms and log sources to connect to, the kind of talent that is required is typically very expensive and hard to find. Given limited resources, organizations make compromises by either hiring fewer analysts or taking longer to integrate and monitor their alerts. This results in fewer threats being addressed.

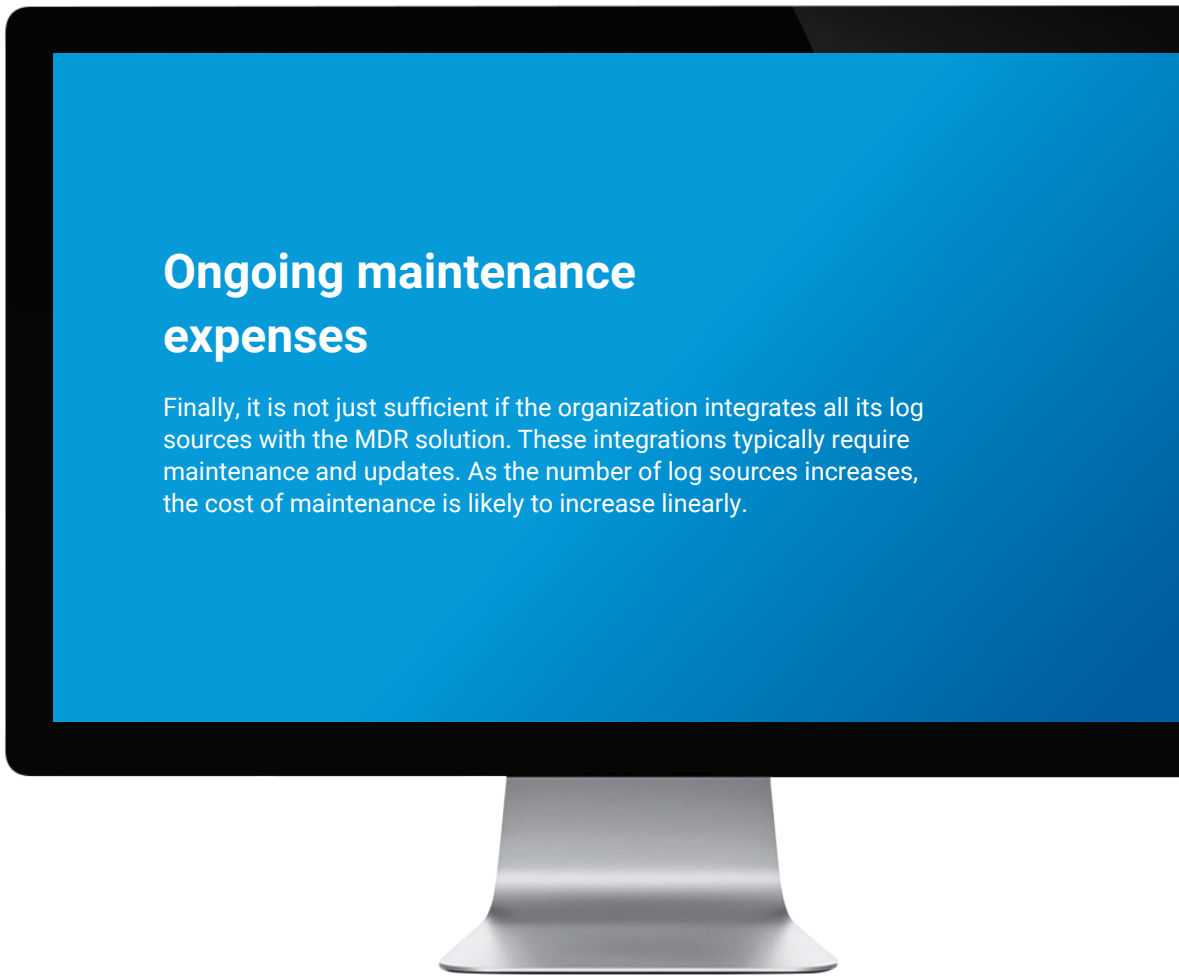
3. Personnel Costs



Anecdotally, we have observed that customers spend only 1/8th the cost of building their own SOC when they leverage Critical Start.

Training expenses

It is not sufficient to just hire strong security analysts and professionals, but an organization must invest in their ongoing training and upskill programs. Given the dynamic nature of the threat landscape, these trainings are mandatory. However, these trainings come at a cost. Organizations face challenges providing such training sessions, If they decide to provide training, they incur a monetary cost and an opportunity cost for the duration of the training. Typically, we have observed that an average security analyst needs to spend at least 120 hours a year in training and upskill activities. One of the biggest advantages that an MDR such as Critical Start provides is the availability of trained professionals and their regular re-training. During these sessions, 24x7 monitoring of an organization's security events continue given the broad talent pool at their disposal.



Putting it all Together

As one can see from the various cost factors above, organizations face various challenging decisions when look at avenues to protect themselves from relentless cyber attacks. While trying to build their own SOC may sound like a very valid idea, it has multiple short and long term quantitative and qualitative drawbacks.

In the short turn, the organization will run into challenges of hiring the right talent and retaining them. Once they have hired the right people, they must ensure that these new team is able to set up the monitoring ecosystem. Some if the costs incurred have been described in the section above. Beyond the costs we have discussed here, customers forgo the economies of scale and scope that a MDR solution will provide.

An assessment of the total costs shows that customer save significantly by going with Critical Start and can realize complete payback within a year of commencement. This is shown in the graph below.

Conclusion

In conclusion, Managed Detection and Response solutions offer both tangible and intangible benefits. We reviewed the clear tangible benefits that an organization can realize with each of these cost levers at a high level. Each of these levers should be studied in greater detail in conjunction with an organization's needs. For example, a startup organization in a rapidly evolving industry like fintech may choose to start with a MDR solution initially while augmenting this capability with internal staff as growth accelerates. On the other hand, an organization in a different vertical where technology is not their core competence and key revenue generator may choose to pick an external MDR solution for the long term. One of the key intangible benefits is the ability to leverage network effects that a solution such as Critical Start provides. Combining advanced machine learning (ML) and artificial intelligence (AI) techniques with deep human expertise, Critical Start helps customers secure any organization's digital journey and growth.

Visit www.criticalstart.com for more information.