MarketUpdate

Managed detection and response services

Introduction

The term MDR may be relatively new, but there are many signs that it is here to stay. It provides the antidote to security risks that many organisations need right now and will for some time to come. The stakes are high in terms of keeping things secure given the relentless attacks and the lack of skilled staff to deal with them. Through MDR, organisations can go from just keeping the lights on to proactively keeping attackers at bay.

This second MDR update provides insight into how various leading vendors in this market are positioned and discusses the trends being seen in this fast-growing market.

Focus on outcomes

This can be a sea change for organisations. MDR is not a one-time fix. Whilst organisations that take such services will in all probability see immediate results by being better able to see right across their environment to detect threats faster and to respond in a more efficient manner that best suits their needs, with the help of experts, they will also be in a position to more easily achieve their long-term goals.

Through the use of MDR services, they will be better able to achieve the outcomes that they desire. One of these is the ability to reduce the likelihood of attacks being successful, which is a measurable outcome in the immediate term. But, over time, they will help to realise the ultimate goal of greater cyber resiliency and a more robust, hardened security posture. This will appeal to any executive that realises that security is as great and as important a risk as all other the organisation faces, enabling security teams to prove their effectiveness in terms of business operations as a whole.

Market trends

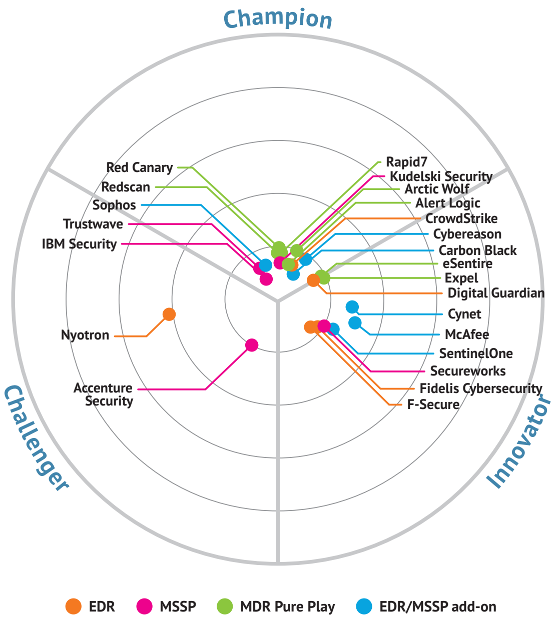
The market for security services continues to gain pace, with managed security services and MDR in particular showing growth. Even the pandemic is failing to dent this market, after some initial jitters.

Rapid expansion

Many MDR service providers are reporting high numbers in terms of new customer wins, both in terms of enterprises and small and medium firms. High growth rates are not unusual in new technology segments, but they are being reported by vendors across the board, from those new into the market to those that have been in this space for a while, even before the MDR moniker was invented.

Seizing on the strong growth opportunities, investors are flocking to this market. Over the past 18 months or so, many vendors have seen large cash injections to enable them to expand and further develop their offerings. Three vendors have been acquired, two by private equity and one by another large technology vendor.

Figure 1: The highest scoring companies are nearest the centre. The analyst then defines a benchmark score for a domain leading company from their overall ratings and all those above that are in the champions segment. Those that remain are placed in the Innovator or Challenger segments, depending on their innovation score. The exact position in each segment is calculated based on their combined innovation and overall score. It is important to note that colour coded products have been scored relative to other products with the same colour coding.



To meet the growing demand, the majority of the market players are expanding their geographical footprint. In many cases, this is through ambitious partner programmes to allow them to better serve customers on a local basis. Local partners understand the market in which they operate and the threat landscape, providing insights specific to a particular sector that are relevant to a particular region. They can provide coverage that is tailored to a specific business through interactions with internal teams in order to better understand their environment and objectives, often providing support in the local language used by the business. For those that need it, local experts from the service provider can more easily be parachuted in to work alongside an organisation's security team or can help with rapid set up of services. Many smaller businesses in particular are benefiting from this trend, helping them to withstand the targeted attacks that they are facing.

This is a trend that will continue, although some expansion plans have been put on hold until the current pandemic is brought under control. Europe is a region that has seen particular interest and this is likely to continue as vendors renew their expansion plans.

Further development of service offerings

Over the past few months, what constitutes the MDR market has become clearer. It is all about telemetry. In IT terms, telemetry refers to data that is collected from multiple points to give a complete view of network activity. By gaining a complete view, organisations will be better able to effectively manage threats and make more informed decisions regarding what actions to take.

Many MDR services have endpoint detection and response (EDR) at their core and some providers started out as EDR vendors. Endpoints remain critical to providing telemetry since they have become so widespread and diverse in nature. And the importance of EDR is not diminishing, especially with the rise of remote working that often involves the use of poorly protected endpoint devices. They are also important to attackers, who routinely use phishing as their preferred route into the network.

But one trend being seen is the growth of eXtended detection and response (XDR) capabilities. Many EDR vendors are embracing this trend by expanding their offerings beyond telemetry from endpoint devices to sources from the network, cloud services and beyond to support hybrid environments that are a reality for most organisations. This will benefit all customers, whether they are using services based on the EDR of their choice, or pure play service providers or MSSPs that partner with EDR/XDR vendors in the provision of their services.

With such expansion of telemetry capabilities, customers will benefit from the greater visibility that is provided over their environments from the enriched number of data feeds, augmented by threat intelligence and the expertise of the service provider's defenders to enable more prioritised and efficient action to be taken.

Threat hunting is an essential component of MDR and the majority of providers are now offering this. Threat hunting came into existence some ten years ago, driven by the need to improve detection capabilities by identifying gaps that existing controls cannot and plugging them before they can be exploited. It goes beyond threat detection alone to proactively try to identify threats at the earliest possible stage of an attack or compromise.

Threat hunting requires a mix of human expertise and automation, combining the use of machine learning and behavioural analysis that are often included in EDR/XDR and user and entity behaviour analytics (UEBA) technologies, along with telemetry from a range of other sources to find indicators of compromise and to understand the tactics, techniques and procedures used by attackers. This is generally done in combination with the use of threat intelligence gleaned from internal network and external sources, which is invaluable in helping security teams to hypothesise where attackers may be found.

But automation alone is not enough. Rather, threat hunters must be trained to think offensively, creating hypotheses on the basis of security alerts, risk assessments, penetration tests and external intelligence. They will then test those hypotheses through investigation and offensive activities, including simulating attacks according to type to determine how a potential attack might happen. Artificial intelligence, especially in the form of machine learning, is not capable of thinking creatively at the expert level required to defeat attacks. Humans will take the analysis presented through automation techniques to uncover relationships in data sets, routing out nefarious data that might otherwise go undetected.

A development being seen among MDR providers is the use of security frameworks in services that they offer such as threat hunting, penetration testing and red teaming. In particular, vendors are embracing the MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework, which is a comprehensive matrix of behaviours employed by attackers when attempting to compromise a network.

According to Anomali, using a framework such as MITRE enables analysts and defenders to test controls and their efficacy, ensure that different techniques used by attackers are accounted for, understand gaps in visibility or protection, validate the configuration of tools and systems, demonstrate where attackers are likely to be successful versus where success is unlikely, and provide hard evidence of exactly what is detected or mitigated and what is not. This helps considerably in helping to prioritise actions to reduce the likelihood of any attack being successful and thus mitigate risk.

Whilst meeting compliance objectives is not always a key factor in the decision to sign up for MDR services, it is one of the largely unsung benefits. Vendors are increasingly offering programmes within their services to help organisations meet the regulatory challenges that they face, including PCI DSS, GDPR, ISO 27001, SOC2, vertical and regional regulations or standards. This shows the growing maturity and professionalism of MDR services and expands the benefits of using such services even further.

Metrics

The top-level criteria used for the Bullseye evaluation are:

- Stability and risk
- Support and location
- Value
- Innovation
- Awareness
- Adoption

Summary

The market for MDR services is fast growing, but there are signs that it is reaching a greater maturity. There are services available to cater to the needs of any organisation, whatever its size or line of business, including those that have offerings specific to needs of particular vertical sectors, such as government or industrial environments. The pace and sophistication of attacks are not diminishing and impact all organisations. The use of MDR services will be of benefit to all.

About the author

FRAN HOWARTH
Practice Leader, Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including ***Silicon***, ***Computer Weekly***, ***Computer Reseller News***, ***IT-Analysis*** and ***Computing Magazine***. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of ***InfoToday***.

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of Mutable business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.

Bloor Research International Ltd
20–22 Wenlock Road
LONDON N1 7GU
United Kingdom

tel: **+44 (0)1494 291 992**
web: **www.Bloorresearch.com**
email: **info@Bloorresearch.com**