MarketUpdate

MDR market update 2023 ...a maturing market

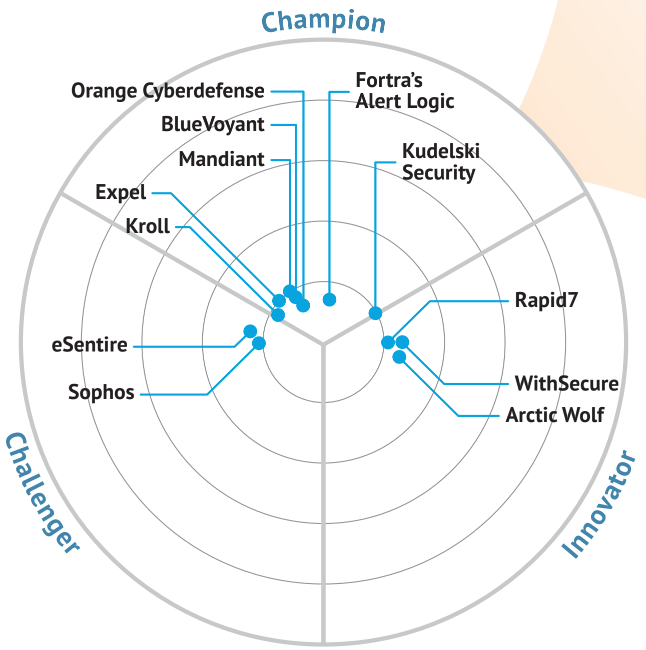
Introduction: a maturing market sector

In the nearly three years since the first market guide for MDR was published by Bloor Research, a great deal has changed. At that point, the market was extremely muddied. A whole host of vendors in the detection and response space were touting the services that they offered, many based on their own technology offerings that were largely focused on endpoint detection and response (EDR). They cited the complexity of detection and response technologies, the inability to hire and retain skilled security staff and the need for speed in tackling ever more sophisticated security incidents.

At that time, Bloor Research split the vendors into EDR vendors offering services on top of their offerings versus those that were pure-play, technology-agnostic versus managed service providers that were trying to break into the MDR market. Today, many of the EDR vendors have morphed into extended detection and response (XDR) vendors, extending the telemetry that they investigate beyond endpoints. Yet, many still base their services around their own technology.

This market guide focuses on technology-agnostic MDR providers. Those selected for this research are the most often cited by end users and rival providers as being the leading service providers in this market.

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.



Developments in the MDR market

Expanding telemetry

All the vendors included in this report have taken, or are moving towards, a multivendor approach to offer the best combination of technologies and to ensure that organisations can continue to benefit from investments that they have already made. Telemetry from multiple sources is key to provide visibility across the entire network and to expand available attack surface management. Most providers are focusing on expanding the integrations that they offer.

Endpoints are still important, more so given the increase in remote working over the past couple of years, but most have expanded to include more telemetry from the network in an XDR approach for detection and response. SIEM is seeing a resurgence alongside network feeds, providing good capabilities for detection when feeds are sent to such systems, although it is less suited for investigations. Inclusion of operational technology and internet of things devices are expanding.

Major focus on cloud services

Cloud services are growing massively in importance, with take up being driven by a number of factors, including the remote workforce. Expanding their cloud offerings is a key focus of development for most MDR providers and they are looking to support demand for hybrid and multicloud deployments among end user organisations. This is a recent development for some that had been focusing on providing MDR support for offerings from different cloud providers.

Expansion of identity management services

Managing identities and associated privileges is essential and getting more so. Credentials are a prime target for many attackers, especially in terms of social engineering attacks, with some providers beginning to offer managed security awareness services. The number of partnerships with identity management vendors is growing and is set to continue to do so.

Identities are also a key attack vector in the cloud, with less exploitation of cloud services themselves than identity. DevOps and Kubernetes deployments are mainstream, with Expel estimating that some 70% of organisations are using Kubernetes. There is a pressing need to monitor what is going on inside containers in order to limit threats. Many service providers are adopting a zero trust approach where no entitlements greater than needed are granted and can be provided on an as-needed basis, then removed once the task for which they are granted has been completed.

Much greater emphasis on incident response

Yes perhaps one of the most important developments being seen in the MDR market is the development of more robust incident response capabilities. This is an area that many felt was lacking, with threat detection having been a greater area of focus. Response is seen as the hardest part for end user organisations and is an area where they are looking for more help.

MDR providers are responding by ramping up their capabilities. This includes increasing automation, especially for mundane tasks. Many MDR providers are expanding their playbook offerings, which offer a guided response for different types of incidents, including steps that should be followed.

However, human expertise is still essential, so organisations looking to take MDR services should look closely at what the provider offers and their level of in-house expertise. Intelligence is key, both in terms of threat intelligence from a wide range of sources, which can greatly help to inform threat hunting activities, as well as that intelligence gathered through detections and previous experience. Most services have machine learning and advanced analytics built into their offerings. Those that provide visibility into ongoing investigations via interactive dashboards are particularly popular.

Many providers are developing a strong knowledge of attacker groups and the tools, techniques and processes that they use through adversary research and intelligence. Knowledge at a local or regional level is sought after in some jurisdictions, with georestrictions very important in some geographies, as is a local touch. Accordingly, those service providers without a strong international presence are looking at expansion into new regions.

More providers catering for the midmarket

Another key area of development in the MDR services market is a greater focus on the midmarket, where very high levels of growth are being seen. Many are tailoring their services to the needs of this market sector, with some bringing out special offerings on a SaaS basis that remove some of the pain in onboarding and ongoing management of such services for smaller organisations that often have fewer capabilities themselves than larger enterprises. Some are offering to manage entire security operation centres on behalf of their customers. Many cite the increasing uptake of MDR capabilities from Microsoft, which is seeing growth that is fourfold and uptake is high in the midmarket. In particular, Office 365 is seen as a particular risk and many organisations are looking for help with their deployments of Microsoft Defender.

More focus on risk management

Digital risk management and resilience is another area where developments are being seen. In part, this is driven by the expansion of digital footprints from external sources and the need for greater visibility of third-party risk as supply chain attacks continue to grow. Organisations are increasingly deploying more network and collaboration tools, which must be effectively controlled to manage overall risk. There is a corresponding increase in the offer of more ancillary services, including offensive security such as red teaming, pen testing and in terms of vulnerability assessments and management. Overall, there is increasing demand for more end-to-end MDR.

Vendor landscape: MDR is a very dynamic growth area

The MDR service providers included in this report are all seeing high levels of growth as threat detection and response is coming to be seen as a must-have by the majority of organisations. Several are valued at more than $1 billion. There have been a flurry of acquisitions: Alert Logic was acquired by HelpSystems in April 2022, which has now been renamed Fortra, Redscan by Kroll in March 2021, Mandiant by Google for $4.5 billion in September 2022 and Sophos by Thoma Bravo in February 2020. In July 2022, F-Secure split out its enterprise business to form WithSecure. Two of the providers featured here, Orange Cybersecurity and Rapid7, are public companies. Some have received substantial funding over the past couple of years, including Arctic Wolf, BlueVoyant and Expel. This dynamism is expected to continue for the foreseeable future.

Summary and conclusions

MDR services can vastly help organisations to improve their security postures, shield them from threats and mitigate incidents that occur. The service provider will monitor feeds from an organisation’s technology estate, including the use of external services such as those in the cloud. Whilst automation is on the rise, especially for mundane tasks, the expertise of the provider’s staff is essential for providing the best outcomes. Any of the vendors included here is a viable choice, although offerings vary.

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

This document is copyright **©2023 Bloor**. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research. 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**