

Managed Detection & Response (MDR)

Warwick Ashford

July 10, 2023



Description: This KuppingerCole Leadership Compass provides an overview of the market for Managed Detection & Response services that manage a collection of cybersecurity technologies for a client organization to provide advanced cyber threat detection and response capabilities, including Security Operations Center as a Service (SOCaaS) offerings.

Contents

Contents.....	2
Figures	3
Introduction / Executive Summary	3
Highlights.....	5
Market Segment	5
Delivery Models	6
Required Capabilities.....	7
Leadership	9
Overall Leadership.....	9
Product Leadership.....	10
Innovation Leadership.....	12
Market Leadership	14
Correlated View.....	16
The Market/Product Matrix.....	16
The Product/Innovation Matrix	18
The Innovation/Market Matrix.....	19
Products and Vendors at a Glance	21
Product/Vendor evaluation	23
Arctic Wolf – Arctic Wolf Managed Detection and Response (MDR)	25
Cybereason – Cybereason Managed Detection and Response	29
eSentire – eSentire Managed Detection and Response.....	33
ESET – ESET PROTECT MDR	37
Expel – Expel Managed Detection and Response (MDR)	40
ForeNova Technologies – NovaMDR 360°	44
Fortinet – Fortinet Managed Detection and Response (MDR).....	47
IBM Security – Managed Detection and Response	51
Kroll – Kroll Responder	55
Proficio – ProSOC MDR	58

Red Canary – Red Canary MDR.....	62
ReliaQuest – ReliaQuest GreyMatter	65
SecurityHQ – Managed Detection and Response (MDR).....	69
Sophos – Sophos MDR	72
Tata Communications – Managed Detection and Response.....	76
Xcitium – Xcitium Managed (MDR) - Xcitium Complete (XDR).....	80
Vendors to Watch.....	84
Methodology.....	89
Types of Leadership	89
Product rating	90
Vendor rating	91
Rating scale for products and vendors.....	92
Inclusion and exclusion of vendors	93

Figures

Figure 1: The Overall Leaders in Managed Detection and Response (MDR).....	9
Figure 2: Product Leaders in Managed Detection and Response (MDR).....	10
Figure 3: The Innovation Leaders in Managed Detection and Response (MDR).....	12
Figure 4: The Market Leader in Managed Detection and Response (MDR).....	14
Figure 5: The Market/Product Matrix for Managed Detection and Response (MDR).....	16
Figure 6: The Product/Innovation Matrix for Managed Detection and Response (MDR)	18
Figure 7: The Innovation/Market Matrix for Managed Detection and Response (MDR).....	19

Introduction / Executive Summary

Industrialized cyber-criminal operations and increased nation state sponsored cyber espionage activities mean that most organizations are under continual cyber-attack, but the worldwide shortage of cybersecurity skills means many organizations are struggling to keep up with attackers, and security teams are often overwhelmed by the number of security alerts being generated by a multitude of security systems.

These and other related factors are driving the growth and evolution of the Managed Detection & Response (MDR) market for solutions that manage a collection of cybersecurity technologies or an integrated platform for a client organization to provide advanced cyber

threat detection and response capabilities, including Security Operations Center as a Service (SOCaaS) solutions.

MDR solutions are typically backed by teams of security experts that provide round-the-clock monitoring, analysis, and support, as well as advice on how to improve the client organization's cyber security posture. MDR solutions, therefore, go beyond traditional Managed Security Services (MSS) from Managed Security Service Providers (MSSPs), which typically focus on compliance reporting and helping customer organizations to meet security compliance requirements.

In previous Market Compass reports, KuppingerCole has focused on SOCaaS as a discrete market which emerged as a result of the evolution of MDR solutions by including coverage of all cloud environments, being built on cloud-based platforms, and including the services and guidance of human analysts. However, many standard MDR solutions now have these characteristics. Therefore, SOCaaS vendors have been included in this more in-depth Leadership Compass analysis of the broader MDR market.

All organizations, regardless of size, face similar cyber threats and therefore need advanced cybersecurity detection and response capabilities. Smaller organizations often lack the budget and skills to do this, while all organizations struggle to fill cybersecurity positions.

MDR solutions mean that even smaller organizations can tap into the benefits of having a large team of experts continually on call to detect and respond to incidents and help guide investments, strategies and processes without the cost and challenges of finding and retaining people with the necessary skills.

Where there is little or no in-house threat detection and response capability, MDR solutions help enterprises to outsource the majority of their security operation, including security related management of networks, endpoints, applications, websites, databases, and security logs. Many MDR services enable organizations to outsource their SOC completely if they do not have the resources to act on recommendations for containing threats, and in a growing number of cases, MDR services support automated response capabilities.

Where there is some in-house security capability, MDR can be used to supplement this whenever necessary to ensure that an organization has at its disposal all the cyber security skills and capabilities required to deal with high-risk threats and critical incidents. This is also relevant for very large organizations, given the volume of cyber-attacks and the skills gap in the market, making it challenging to develop long term security strategies, while keeping on top of daily cyber threats and incidents.

Even large organizations with in-house security teams find it challenging to manage SIEM, NDR, EDR, SOAR, and even IAM systems to deliver the required security outcomes. As a result, they are turning to MDR service providers to help with this, as well as provide rapid automatic containment capabilities for common threats. Some vendors report a growing demand for MDR services from the world's largest organizations due to the global lack of cybersecurity skills and high churn rates that make it challenging to run an in-house SOC and maintain the desired quality of service (QoS) levels.

The main aims of MDR are to:

- Strengthen organizations' ability to monitor and detect security threats and respond to security incidents 24/7.
- Continually improve overall security strategy and posture.
- Provide a comprehensive view across the security environment.
- Enable in-house security teams to focus on and manage strategic security initiatives.
- Increase value from existing security investments.

MDR solutions are also aimed at:

- Helping customer organizations deal with high volumes of security alerts.
- Reducing the time that it takes to identify and mitigate security incidents.
- Providing advanced analytics of threats and user behavior.
- Rationalizing, updating, and integrating/coordinating security tools.
- Improving visibility and governance of business IT environment across the whole enterprise.
- Providing tools and expertise to deliver or augment endpoint detection and response (EDR), eXtended Detection and Response (XDR) capabilities, and Security Orchestration, Automation, and Response (SOAR) capabilities.

Highlights

- Increasing cyber threats, alert overload, and the worldwide shortage of cybersecurity skills are among the top drivers for the ongoing evolution and growth of the Managed Detection & Response (MDR) market.
- MDR solutions include a wide range of cybersecurity services, ranging from simple alert triage to Security Operations Center as a Service (SOCaaS) to full MDR, including Incident Response.
- A key element of MDR is the focus on continual improvement of cybersecurity posture, going beyond traditional Managed Security Services from Managed Security Service Providers.
- MDR solutions that cater for all sizes of organizations provide the opportunity for even small companies to get the benefit of enterprise-level Security Operations Centers.
- Most MDR solutions now meet a range of use cases from assistance of in-house SOC's and security teams to full outsourcing of security operations.
- MDR solutions typically help organizations to maintain round-the-clock monitoring of IT assets and deal with large volumes of alerts across increasingly complex business IT environments.
- The Overall Leaders in Managed Detection and Response (in alphabetical order): Arctic Wolf, eSentire, ESET, IBM, Kroll, Proficio, ReliaQuest, and Sophos.

Market Segment

Adoption of MDR solutions has increased as organizations have increasingly come to understand that no level of technology investment will provide 100% protection against threats, and as the volume and complexity of the security challenges have become too great for internal security teams to manage. Evidence of the increased demand for MDR solutions

can be seen in the rapid growth in the market, with most vendors reporting significant growth in sales, particularly following the Covid-19 Pandemic.

Adoption of modern MDR solutions is being driven by:

- The rapidly increasing adoption of cloud services and the need to secure critical data in the cloud.
- The worldwide shortage of cybersecurity professionals leaves many organizations under-resourced.
- The growing number of cyber-attacks as the attack surface increases with digital transformation.
- The recognition of ransomware as a major cybersecurity threat.
- The increase in the number of data protection regulations and rising customer expectations in terms of privacy.
- The expansion of IT environments to include mobile, edge, and cloud computing.
- The adoption of home working/hybrid working post pandemic.
- The increase in data breach threats driven by nation state sponsored cyber-attacks.
- Increased cyber espionage, targeting both personal information, credentials, and IP.
- The rapid increase in the amount of data that organizations are producing.

The drivers listed above are the main reasons many organizations have already adopted MDR, and why the majority of those who have not committed to MDR are planning to evaluate it as an option. The adoption of MDR is typically in response to a security breach, regulatory requirements, mergers and acquisitions, and increased demand by the board for improved cyber security status reporting.

For many organizations, MDR is the only way they are able to consolidate all of their security threats, tools, and systems into a single point of control to address and resolve all alerts, monitor and respond to all indicators of potential compromise by analyzing all security data, and evaluate the effectiveness of existing controls to identify where and how this can be improved.

Many of the modern MDR solutions focus on the concept of continual improvement of security, which is one of the hallmarks of the SOCaaS model. Many MDR providers include some form of concierge or a white glove tailored solution in which the vendor and customer work in partnership, or they plan to add such a service in response to market demand.

This market segment continues to grow and evolve toward a model where MDR solution providers are taking on more areas of responsibility, including risk assessment in partnership with customer cybersecurity teams, threat detection, threat triage, threat containment, and even threat recovery and remediation in partnership with customer cybersecurity and IT teams. MDR solution providers are also increasingly managing EDR and providing SOAR-as-a-Service to reduce the burden of managing these complex systems.

Delivery Models

The MDR market is well established and mature, but it continues to grow and evolve to meet increased demand and changing business needs, business IT environments, and cyber-attack methods.

Consequently, MDR solutions are increasingly transitioning away from on-premises deployments to cloud-based services. However, an important requirement of this market is for vendors to fit in as much as possible with existing cybersecurity tools, systems, and controls. As a result, many MDR vendors are opting for flexible delivery models to best meet customer requirements.

While there are some vendors in this report that are entirely cloud-based services, most have some degree of flexibility to cater for customers whose tech stacks require some on-premises software, agents, and collectors. Some vendors even cater for customers in highly regulated industries by deploying the entire MDR solution on premises, including a dedicated SOC.

MDR solution delivery, therefore, can be on premises, in the cloud, or hybrid, but solutions that provide the most flexibility in deployment options and the best coverage of modern IT environments are the most likely to rank as leaders in this market segment report.

Required Capabilities

We are looking for MDR solutions that are designed to enable:

- Deployment and maintenance of tools which facilitate MDR capabilities across all customer environments: offices, data centers, remote workers and contractors, and cloud-based services.
- Rapid detection, investigation, analysis, and mitigation/containment of cyber risks and incidents.
- The elimination of false positives and prioritization of real threats.
- Continual improvement of security posture by identifying and remediating vulnerabilities.
- A consistently high level of visibility across all IT assets.
- Regular assessment of risks based on up-to-date threat intelligence.
- Advanced analysis of cyber threats and anomalous behavior.
- The collection, correlation, and analysis of all security data across the IT environment.
- The orchestration and automation of responses to threats.

We expect solutions to cover most of these capabilities, and in addition to delivering functionality to support them, must also meet our requirements for deployment and interoperability with other security tools.

This report, therefore, considers and rates the following capabilities to:

- Work well across on premises, cloud, and mobile IT environments.
- Integrate well with existing security technologies.
- Work across all the main operating systems.
- Deliver good security capabilities.
- Provide detection and response capabilities for remote/home working.
- Have a reasonable total cost of ownership.
- Be relatively quick and easy to implement.

Drilling into more detail, this report evaluates key capabilities to:

- Deploy and maintain detection and response tools.
- Monitor for anomalies, threats, attacks, and risks across the entire IT environment.

- Detect, analyze, and manage threats.
- Validate incidents.
- Provide Web Application Firewall functionality.
- Detect network intrusions.
- Scan, assess, report, and manage vulnerabilities.
- Manage logs.
- Provide threat intelligence for advanced detection and risk mitigation.
- Connect to cloud services, on-premises applications, and mobile applications.
- Support the Windows, Linux, and MacOS operating systems.
- Have a flexible, modern software architecture and deployment.
- Interoperate with a range of security solutions such as EDR, NDR, SIEM, SOAR, and DLP.
- Interoperate with email/web security solutions, and firewall systems and services.
- Detect and remediate threats on endpoints.
- Automate and orchestrate response activity on endpoints.
- Detect and remediate threats.
- Automate and orchestrate response activity on networks.
- Provide remote assistance response in the event of a breach.
- Provide clear and customizable playbooks on how to respond to various threat types.
- Provide clear escalation paths wherever threats cannot be resolved quickly.
- Provide dashboards for customers to view their organization's security status.
- Report regularly on security posture, threat hunting, emerging threats, and improvements
- Provide a content library of use cases for advanced threat protection and response playbooks.

Additional capabilities considered by this report include:

- Regular automated threat hunting.
- Regular manual threat hunting.
- Asset discovery.
- External vulnerability scanning (in addition to internal).
- Automatic application of product updates without delay after release.
- Regulatory compliance reporting.
- On-premises issue resolution.
- On-premises consultation.

Innovative capabilities considered by this report include:

- User behavior analytics
- Attacker behavior analytics.
- Integration with third-party behavior analytics.
- Applied AI/ML for detection, reporting, and blocking of anomalous or suspicious activity.
- A single management console to provide visibility and control over users, applications, and data across the enterprise IT environment.
- Collection of telemetry from Operational Technology (OT) environments and Internet of Things (IoT) devices, including those in medical (IoMT) and industrial (IIoT) environments.
- Deployment and operation of Distributed Deception Platforms for customers.
- Mobile app to access dashboards, status reports etc.

Leadership

Selecting a vendor of a product or service must not be based only on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help to identify vendors that should be further evaluated. However, a thorough selection process should also include a subsequent detailed analysis and a Proof of Concept or pilot phase, based on the specific criteria of the customer.

Based on our research, we have created various Leadership ratings. The Overall Leadership rating, shown in Figure 1, provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership



Figure 1: The Overall Leaders in Managed Detection and Response (MDR)

Overall Leaders are (in alphabetical order):

- Arctic Wolf
- eSentire
- ESET
- IBM
- Kroll
- Proficio
- ReliaQuest
- Sophos

Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.

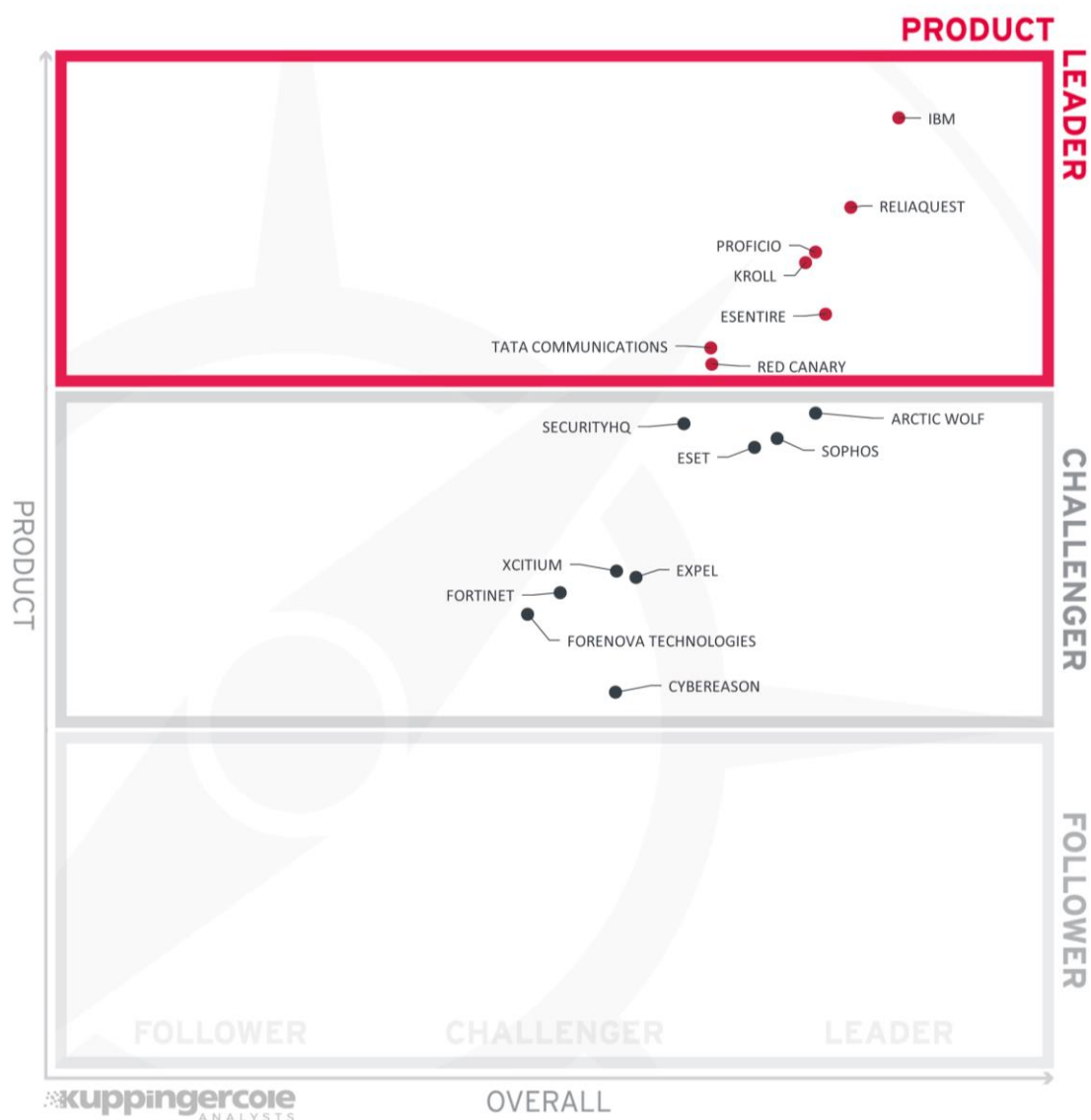


Figure 2: Product Leaders in Managed Detection and Response (MDR)

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

MDR is an important market segment that continues to grow and evolve in response to the rising demand for round-the-clock security monitoring and analysis of increasingly complex business IT environments.

To be rated as MDR service leaders, vendors must meet most of the key capabilities defined in chapter 1. eSentire, IBM, Kroll, Proficio, Red Canary, ReliaQuest, and Tata Communications (in alphabetical order) lead the field with the most comprehensive offerings.

The remaining vendors covered in this report are all challengers in the MDR market. With attention to the areas identified as challenges, these services have the potential of moving up to become product leaders.

Product Leaders (in alphabetical order):

- eSentire
- IBM
- Kroll
- Proficio
- Red Canary
- ReliaQuest
- Tata Communications

Innovation Leadership

Innovation from our perspective is a key capability in all IT market segments. Customers require innovation in order to meet evolving and emerging business requirements. Innovation is not about delivering a constant flow of new releases and upgrades. An innovative approach is being able to provide customer-focused upgrades, as well as other cutting-edge features, while maintaining compatibility with previous versions.

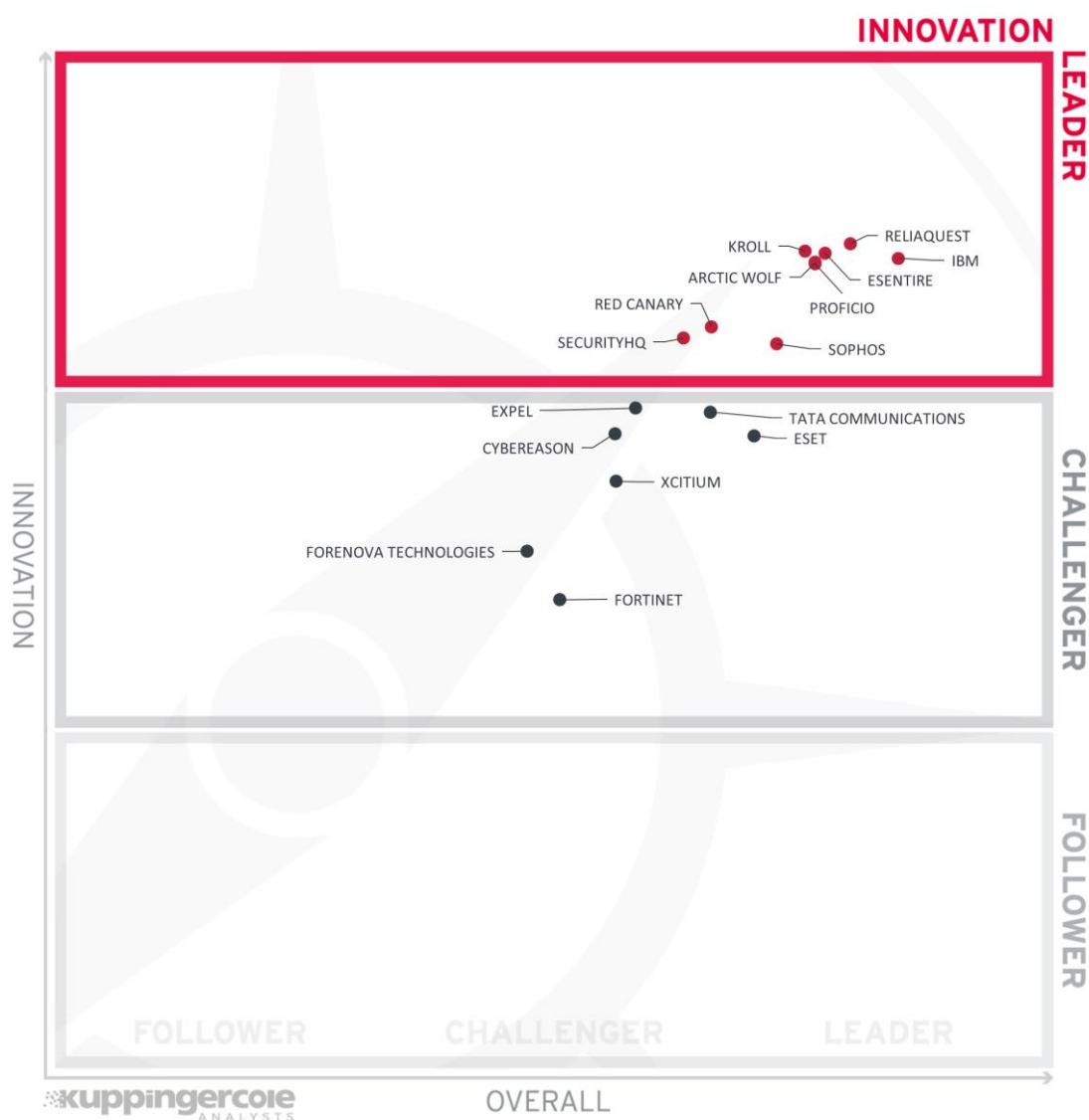


Figure 3: The Innovation Leaders in Managed Detection and Response (MDR)

Arctic Wolf, eSentire, IBM, Kroll, Proficio, Red Canary, ReliaQuest, Sophos, and SecurityHQ are the leaders in MDR innovation. Cybereason, ESET, Expel, and Tata Communications are strong challengers, followed by ForeNova Technologies, Fortinet, and Xcitium. Innovation leaders and challengers are listed in alphabetical order.

Innovation in MDR is characterized by continual expansion of automated capabilities, the inclusion of user and attacker behavior analytics, the use of machine learning and deep learning, the availability of recently investigated incidents that are similar to current incidents, context about recent events in the customer organization's environment, global context based on customer events, detection of steganography used for malware control and/or data exfiltration, validation that a threat has been neutralized, and support for activity recording.

Planned innovation in the MDR market segment will focus on risk analysis and situational intelligence on customer infrastructure to steer strategic security investments, increased support for automation, self-service log onboarding, cyber resilience scoring, support for federated data analytics, tighter integration with cloud-native security controls and exposure management tools, and a greater focus on OT and IoT environments.

Innovation Leaders (in alphabetical order):

- Arctic Wolf
- eSentire
- IBM
- Kroll
- Proficio
- Red Canary
- ReliaQuest
- SecurityHQ
- Sophos

Market Leadership

Lastly, we analyze Market Leadership. This is an amalgamation of the number of customers, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

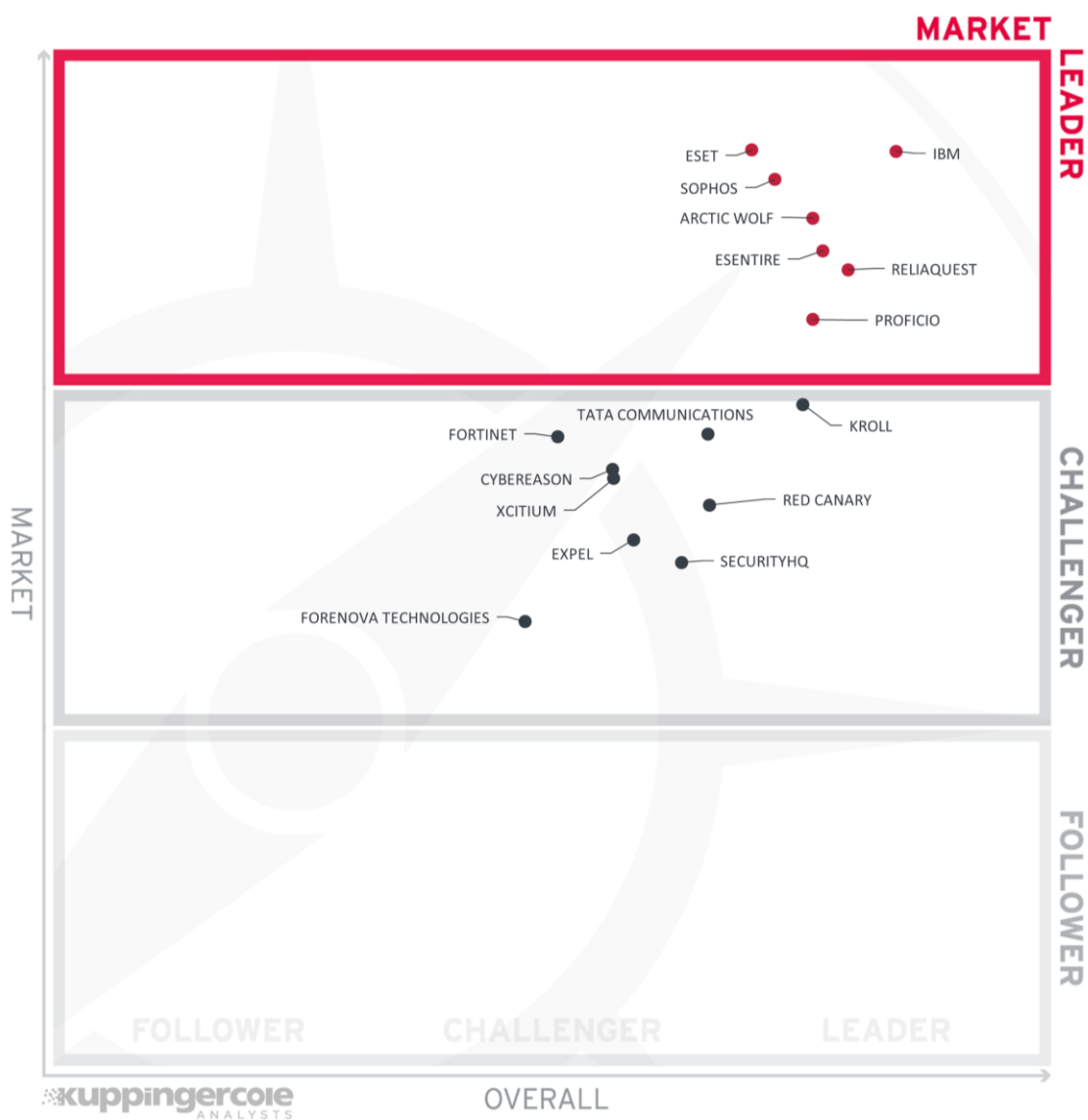


Figure 4: The Market Leader in Managed Detection and Response (MDR)

The MDR market is large and growing, driven by increased targeting of sensitive data by malicious actors, the need to prevent data breaches, increasing demand for compliance with data protection regulations, the lack of available security talent, and an increasing attack surface. Market Leadership is determined by combining the scores for a wide variety of market-related factors detailed above.

The MDR Market leaders are, in alphabetical order, Arctic Wolf, eSentire, ESET, IBM, Proficio, ReliaQuest, and Sophos. The challengers need to improve across all the determining factors, such as, expanding the size and global distribution of their customer base to move up into the leadership category.

Market Leaders (in alphabetical order):

- Arctic Wolf
- eSentire
- ESET
- IBM
- Proficio
- ReliaQuest
- Sophos

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking for a product leader and for a vendor that delivers a solution that is both feature rich and continually improved. This would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

The Market/Product Matrix



Figure 5: The Market/Product Matrix for Managed Detection and Response (MDR)

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

All vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

eSentire, IBM, Proficio, and ReliaQuest are the Market Champions in the top right corner. This means that product strength correlates closely with the market position.

Arctic Wolf, ESET, and Sophos are in the top center square, indicating that these MDR providers have a strong market position that they could capitalize on by improving their MDR service offerings in terms of features and functionality to bring them more in line with the Market Champions.

Kroll, Red Canary, and Tata Communications are in the center right square, indicating that they have relatively strong service offerings, which are not yet matched by the size and geographical spread of their customer bases. These vendors could move up by improving these two areas.

All the vendors in the center square have the opportunity to improve their MDR service offerings and grow their customer bases.

The Product/Innovation Matrix

This matrix illustrates the correlation between Product Leadership and Innovation Leadership. It is clear that technological innovation drives product success, which means there is typically a close relationship between innovation and product strength.



Figure 6: The Product/Innovation Matrix for Managed Detection and Response (MDR)

Vendors below the line are more innovative, while vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The Technology leaders are eSentire, IBM, Kroll, Proficio, Red Canary and ReliaQuest. With a bit more focus on innovation, Tata Communications could become a Technology Leader, as could Arctic Wolf, SecurityHQ, and Sophos by strengthening their overall service offerings.

Vendors in the center square all have the opportunity to align innovation with overall strength. Cybereason and Expel would benefit from focusing on increasing overall service strength, while ESET, ForeNova Technologies, and Fortinet would benefit from focusing more on innovation.

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.



Figure 7: The Innovation/Market Matrix for Managed Detection and Response (MDR)

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate despite having less market share, and thus the biggest potential for improving their market position.

The Big Ones in the first edition of the MDR Leadership Compass are: Arctic Wolf, eSentire, IBM, Proficio, ReliaQuest, and Sophos. ESET is in the top center square, indicating that it has the ability to capitalize on its market position by paying more attention to innovation. Kroll, Red Canary, and SecurityHQ, in the center right box, have sufficient innovation in their offerings to drive further market share growth.

All the vendors in the center square have the potential to drive market growth by increasing their efforts in terms of innovation.

Products and Vendors at a Glance

This section provides an overview of the various products analyzed within this KuppingerCole Leadership Compass on Managed Detection and Response (MDR) solutions. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These help to identify highly innovative, but specialized vendors or local players that provide strong product features, but do not have a global presence and large customer base yet, for example.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
Arctic Wolf	Positive	Positive	Positive	Neutral	Strong Positive
Cybereason	Neutral	Positive	Positive	Neutral	Neutral
eSentire	Strong Positive	Strong Positive	Positive	Positive	Positive
ESET	Positive	Positive	Strong Positive	Neutral	Strong Positive
Expel	Neutral	Positive	Positive	Positive	Positive
ForeNova	Neutral	Positive	Positive	Neutral	Neutral
Fortinet	Neutral	Positive	Positive	Positive	Neutral
IBM	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Kroll	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
Proficio	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
Red Canary	Positive	Positive	Strong Positive	Positive	Positive
ReliaQuest	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
SecurityHQ	Positive	Strong Positive	Positive	Positive	Positive
Sophos	Positive	Strong Positive	Strong Positive	Positive	Positive
Tata Communications	Strong Positive	Strong Positive	Positive	Positive	Positive
Xcitium	Neutral	Positive	Strong Positive	Weak	Positive

Table 1: Comparative overview of the ratings for the product capabilities

In Table 2 there is an overview which contains four additional ratings for each vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Arctic Wolf	Strong Positive	Positive	Strong Positive	Positive
Cybereason	Positive	Positive	Positive	Positive
eSentire	Strong Positive	Strong Positive	Positive	Strong Positive
ESET	Positive	Strong Positive	Strong Positive	Strong Positive
Expel	Positive	Neutral	Neutral	Neutral
ForeNova	Neutral	Neutral	Weak	Positive
Fortinet	Neutral	Positive	Strong Positive	Strong Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Kroll	Strong Positive	Neutral	Positive	Strong Positive
Proficio	Strong Positive	Strong Positive	Neutral	Strong Positive
Red Canary	Positive	Positive	Neutral	Positive
ReliaQuest	Strong Positive	Strong Positive	Positive	Strong Positive
SecurityHQ	Strong Positive	Neutral	Neutral	Neutral
Sophos	Positive	Strong Positive	Strong Positive	Strong Positive
Tata Communications	Positive	Positive	Strong Positive	Positive
Xcitium	Neutral	Positive	Neutral	Strong Positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC Managed Detection and Response, we look at the following eight categories:

- **Coverage:** Effective detection relies on comprehensive monitoring of the IT environment. This metric reflects the breadth of the solutions coverage in terms of monitoring and analysis of data movement across applications, systems, endpoints, protocols, groups, and locations. It also includes integrations with other security products such as DLP and EPDR.
- **Cloud Support:** A measurement of the degree to which solutions provide monitoring and analysis of cloud environments, including service providers, applications, infrastructures, and data stores. It also includes cloud security posture management, workload protection and vulnerability scanning.
- **Detection:** An evaluation of threat detection coverage and capabilities across modern IT environments. It includes the average detection times, behavior analytics, integrations with intrusion detection and prevention systems, and the capability to detect certain types of malicious tactics, techniques, and procedures.
- **Response:** This category looks at a solution's ability to respond to threat detections, including blocking capabilities, rapid incident validation, response times, post-remediation support, and activity recording.
- **Automation:** An in-depth look at a solution's automation capabilities in terms of threat containment actions, including process termination, host isolation, port blocking, and file quarantining. It also looks at solution's SOAR capabilities and integrations and provision of incident response playbooks.
- **Threat intelligence:** This is a measure of a solution's threat intelligence and threat hunting capabilities, including provision of automated threat hunting, type and number of intelligence sources, and support for threat intelligence exchange.
- **Insider threat detection:** This metric reflects a solutions ability to detect and block insider threats, including the detection of phishing attacks aimed at tricking employees into revealing their credentials which would give insider access, the abuse of privileged credentials, and the use of user behavior analytics.
- **Admin support:** An evaluation of the administrative support provided by the solution in terms of initial setup, incident response, language support, and professional support services. It includes the ability of the solution to provide full SOC services, to work as an extension of internal teams, to assist in developing security and governance policies, to provide dedicated analyst teams, and to provide continual improvement guidance.

Arctic Wolf – Arctic Wolf Managed Detection and Response (MDR)

Arctic Wolf was founded in 2012 and is a private US cybersecurity company which specializes in security operations. Arctic Wolf is headquartered in Eden Prairie, Minneapolis, with SOC's in Eden Prairie, San Antonio, and Pleasant Grove in the US, Waterloo in Canada, and Frankfurt in Germany. Arctic Wolf has customers around the world with the majority in North America, followed by EMEA, and caters to all sizes of organization.

Arctic Wolf MDR is a vendor-neutral concierge-style service, providing at least two named security experts per customer, that is offered via channel partners only. Pricing is based on users, appliances, servers, and the assets required to support the service. Once a contract price is agreed, it is an all-inclusive fixed price, regardless of log/data quantity.

Arctic Wolf offers rapid deployment times and flexible on-premises, cloud, and hybrid deployment models, depending on the customers' requirements. The solution is based on the Arctic Wolf Platform built on open XDR architecture, includes vulnerability management, security awareness training, continuous improvement, and covers all major operating systems and browsers. In addition to MDR, Arctic Wolf offers managed risk, managed security awareness, and incident response services.

The solution provides round-the-clock monitoring and analysis of all business IT environments, including Edge computing, and provides detection and response services across all environments, including medical and industrial IoT devices, and remote workers.

Arctic Wolf MDR includes prebuilt integrations with 13 common third-party EPDR products, 20 NDR products, and one third-party behavior analytics solution (Microsoft Advanced Threat Analytics). Integrations are possible with any third-party tools or systems that can export data in the SYSLOG format, can export data directly into an S3 bucket, or can export data via Cloud Watch in AWS.

The solution provides good support for cloud computing with monitoring and analysis of cloud applications and cloud data stores, with detection and response services across all cloud services and applications, and the ability to identify data loss across cloud infrastructure. Arctic Wolf MDR includes cloud security posture management, cloud workload protection, vulnerability scanning of customer multi-cloud environments, and detection of business email compromise (BEC) attacks.

Arctic Wolf is able to detect threats across the entire IT estate and perform network-based detections that include full packet capture and inspection, as well as identify a wide range of malicious activity, including ransomware and evasive malware. The solution also includes attacker behavior analytics.

Focusing on response, the solution is able to disrupt threats automatically, while attack blocking capabilities include the disruption of malicious network communications but not account suspensions. The solution includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced. It also supports activity recording for forensic analysis.

Arctic Wolf MDR is able to execute predefined containment actions automatically, including host isolation. However, these do not include the termination of processes or network sessions, the blocking of communications by port and IP, quarantining of files, sinkholing, or preventing registry changes. The solution can provide its own SOAR capabilities and comes with a prebuilt integration with one third-party SOAR solution (ServiceNow).

The solution includes the support of a dedicated threat hunting team, automated threat hunting, and regular reporting on threat hunting findings. Arctic Wolf MDR uses threat data from customer deployments, Arctic Wolf's threat intelligence team, and a select number of commercial and open-source intelligence feeds, and includes connectors with seven third-party intelligence sources.

The solution is able to capture East-West traffic for insider threat detection, and it can detect and respond to phishing attacks, insider threats, and abuse of privileged access. It also includes user behavior analytics.

Arctic Wolf offers a service for assistance with initial setup, an expert team for assisting in incident analysis and remediation, and guided remediation as part of standard service. In-person incident response services are available at an additional cost. Support services and documentation are available only in English and German. On-site support is available only in North America. The updated customer portal brings all information and services together.

Customers can use the service to outsource their SOC entirely or Arctic Wolf analysts are able to work as an extension of the internal SOC or security teams. The solution includes regular risk assessment reporting, and assistance in developing security and governance policies. There is also a dedicated analyst or team allocated to each customer and continual strategic and security improvement planning is included as part of the standard subscription.

Arctic Wolf MDR is suitable for all sizes of business, particularly small and medium enterprises looking for a personalized, concierge-style managed detection and response service with a focus on BEC attacks and optimizing security operations.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Strong Positive



Table 3: Arctic Wolf's rating

Strengths

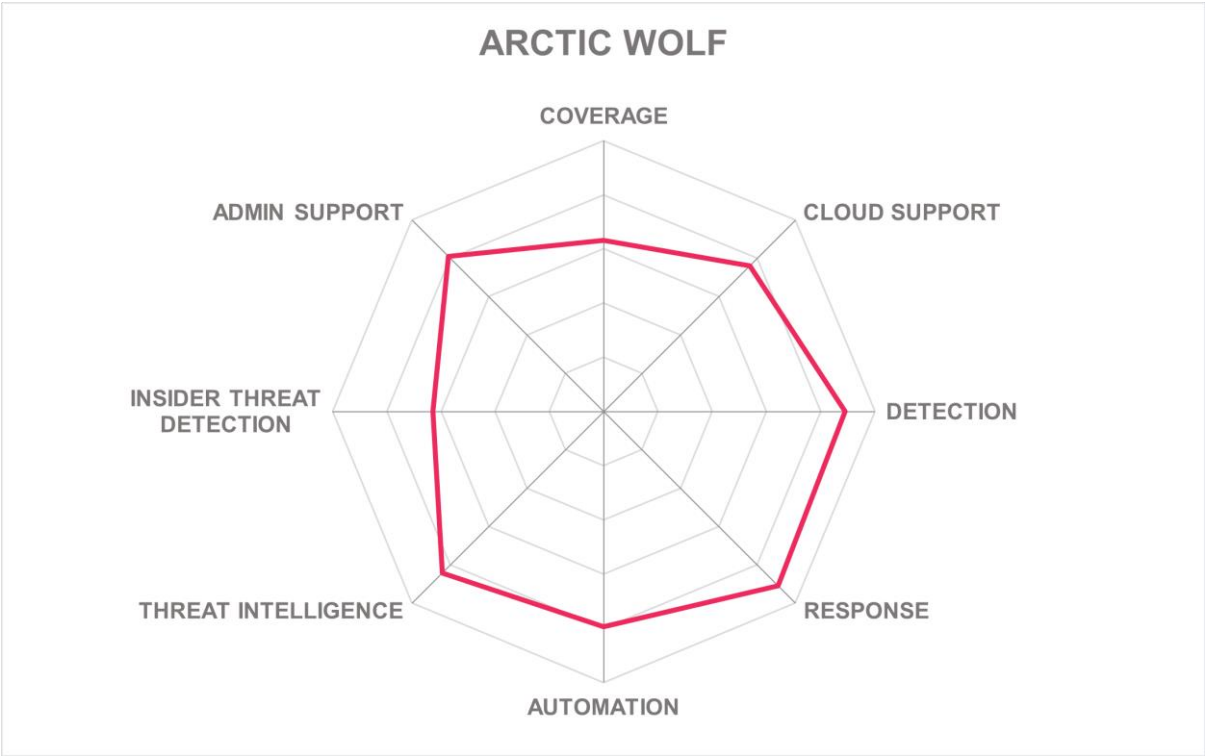
- Personalized, concierge-style service.
- Security operations focus and expertise.
- Simple pricing model via channel partners.
- Flexible and rapid deployment model.
- Comprehensive coverage of all business IT environments.
- Unified customer portal.
- Good detection capability for insider threats.
- Focus on BEC attacks.
- A mobile app to support cyber defenders wherever they are.

Challenges

- Providing integrations with third-party behavior analytics, SIEM and NDR products would help customers get greater ROI out of existing investments.
- Adding the ability to suspend accounts would bolster the solution's response capabilities.
- Expanding the number of automated containment actions would boost the solutions response capabilities.
- Prebuilt integrations with third-party SOAR solutions would help customers get greater ROI out of existing investments.
- Providing support services and documentation in more than two languages may help to open up new markets or grow existing ones.

Leader in





Cybereason – Cybereason Managed Detection and Response

Cybereason is a private American cybersecurity technology company founded in 2012 and headquartered in Boston, Massachusetts, with three global SOCs for North America, EMEA, and Japan. Most customers fall into the mid-market category, with the largest number of customers in the APAC region, followed by EMEA.

Cybereason uses a simple pricing model based on per endpoint, per year and depends on the subscription size. Customers have the choice of either on-premises or cloud-based deployment and the choice of two packages: MDR Essentials for more mature organizations and MDR Complete for organizations that want full functionality and support.

Cybereason MDR is based on the company's Open XDR Defense Platform, which includes a detection engine to provide full network visibility and contextualization. The solution focuses on augmenting internal skills and driving effectiveness and efficiency through its technology and malicious operations approach, which groups indicators of malicious activity into "MalOps" which are assigned severity scores to speed up triage and remediation processes. Every MalOp is also aligned to the MITRE ATT&CK framework to help improve customer security posture.

The solution covers all major operating systems and web browsers, with the exception of Opera, and provides 24-hour monitoring and analysis of most business IT systems and environments, except internet traffic, cloud data stores, and Edge computing environments. The solution provides detection and response services across all environments, including medical and industrial IoT devices, and remote workers.

Cybereason MDR includes integrations with three third-party NDR products (Darktrace, FireEye Network Security, and Vectra Cognito) and four SIEM products (Microsoft Sentinel, IBM QRadar, Rapid7, and Splunk) but none with EPDR and behavior analytics products.

While the solution provides monitoring and analysis of cloud applications and provides detection and response across cloud services and applications, as already noted, it does not monitor cloud data stores. It can identify data loss across cloud infrastructure, but it does not include cloud security posture management, cloud workload protection, or vulnerability scanning of customer multi-cloud environments.

Looking at detection capabilities, Cybereason MDR can detect threats across the entire IT estate, but network-based detections do not include full packet capture and inspection. The solution can detect a wide range of malicious activity, including ransomware and evasive malware. The solution also includes attacker behavior analytics and scores highly in MITRE ATT&CK testing in terms of protection and visibility.

Cybereason MDR is able to disrupt threats automatically, while attack-blocking capabilities include the disruption of malicious network communications and account suspensions. The solution includes post-remediation support to validate that a threat has been neutralized and to verify that it has not resurfaced as well as supporting activity recording for forensic analysis. Response processes are also supported by the Cybereason MDR app for iOS and Android, which is part of the MDR Complete package and enables cyber defenders to see what is happening in the IT environment, initiate automated responses, and communicate with Cybereason SOC analysts.

The solution provides a range of automated actions, including terminating processes, isolating hosts, quarantining files, and preventing registry changes, but it does not include terminating network processes, blocking communications by port and IP, or sinkholing. The solution does not offer any out-of-the-box integrations with common SOAR products.

Cybereason MDR includes automated threat hunting and the support of a dedicated threat hunting team that proactively hunts threats and provides regular reporting on threat hunting findings. The solution applies threat data from customer deployments, and a few select commercial and open-source threat intelligence feeds. It includes a connector to only one external threat intelligence source.

The solution includes user behavior analytics and can detect and respond to insider threats, phishing attacks, and abuse of privileged access, but does not capture East-West traffic for insider threat detection.

Cybereason offers a service for assistance with initial setup and an expert team for assisting in incident analysis and remediation, but incident handling is not part of standard service support. Incident response services can be purchased in advance or added when necessary. Support services and documentation are available only in English and Japanese. There are also no on-site support services in any region.

Customers can use the service to outsource their SOC entirely or Cybereason SOC analysts are able to work as an extension of the internal SOC or security teams. There is no dedicated analyst or team allocated to each customer, but Cybereason MDR does include a “white glove” onboarding process. The solution includes regular risk assessment reporting and assistance in developing security policies. There is no assistance in developing governance policies and the offering does not include strategic, continual improvement planning.

Cybereason MDR caters to enterprises of all sizes, except for very small businesses, and can scale easily as an organization grows. It is best suited to mid-market organizations looking to get more value out of existing cybersecurity tools and to augment internal security teams to make them more efficient and effective.

Security	Neutral
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Neutral



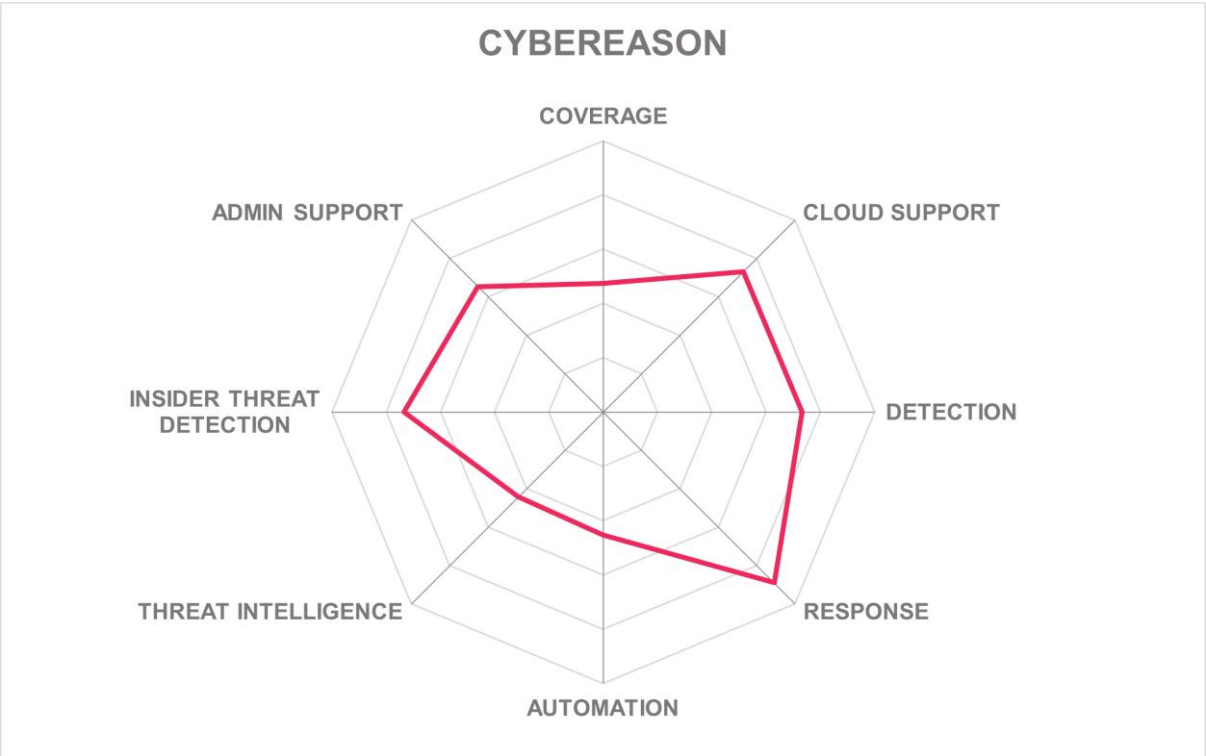
Table 4: Cybereason's rating

Strengths

- Choice of cloud-based or on-premises deployment.
- Proactive and automated threat hunting capability.
- Outcomes-based approach.
- MDR Complete offers fast detection, triage, and remediation.
- Alignment of incidents to the MITRE ATT&CK framework
- Mobile app to support cyber defenders wherever they are.

Challenges

- Coverage of internet traffic, cloud data stores, and Edge computing environments would bolster solution's detection capabilities.
- Prebuilt integrations with third-party EPDR and behavior analytics products would help customers get greater ROI from existing investments.
- Monitoring and analysis of cloud data stores would bolster solution's detection capabilities and support for cloud computing.
- Expanding cloud support and protections would make this offering more attractive to organizations heavily invested in cloud-based services.
- The solution would benefit from more automated capabilities and integration with third-party SOAR products.
- Collecting and correlating external threat intelligence from a wider range of sources could improve threat detection capabilities.
- Expanding the number of languages for support and documentation could help open up new markets or grow existing ones.



eSentire – eSentire Managed Detection and Response

eSentire is a private Canadian MDR company founded in 2001, with its headquarters and a SOC in Waterloo, Ontario, and an additional SOC in Cork, Ireland. The company has customers around the world with most customers in North America, followed by EMEA, and services all sizes of organization, with most falling into the medium and mid-market enterprise segments.

Launched in 2008, eSentire MDR combines its proprietary, open cloud-native XDR Platform, multi-signal threat intelligence, and teams of round-the-clock SOC analysts and threat hunters. The eSentire XDR Platform ingests network, cloud, log, endpoint and identity threat signals, and correlates indicators of compromise to detect and respond to threats automatically. The platform “learns” from positive SOC investigations, adding more than 200 IoCs (indicators of compromise) to its global block list every day to improve customer automated defenses. The open architecture means that the platform can connect to hundreds of security and collaboration tools via APIs to provide complete visibility of the customer environment.

eSentire offers simple annual per-user, bundled pricing that allows for spikes in log data, with cost factors abstracted away but available on request. The company also offers discounts for multi-year and multi-signal deals.

Deployment is flexible according to customer circumstances and requirements for cloud-based on-premises or hybrid deployments. eSentire provides quick time to value, with the average MDR for endpoint service deployed within seven days. The solution covers all major operating systems and browsers.

eSentire MDR provides continual monitoring and analysis of all major IT environments and systems, including Edge computing environments, and provides detection and response services across all environments, including medical and industrial IoT devices, and remote workers.

The solution includes integrations with four third-party EPDR products (CrowdStrike Falcon Endpoint Protection, Microsoft Defender for Endpoint, SentinelOne Singularity Platform, and VMWare Carbon Black), two SIEM products (Microsoft Sentinel and Sumo Logic), and three behavior analytics products (Microsoft Advanced Threat Analytics, Microsoft Sentinel, and Sumo Logic), as well as eSentire’s proprietary Insider offering. There are no integrations with NDR products because eSentire MDR uses the company’s proprietary network product, which includes virtual and physical appliances, depending on a customer’s environment. eSentire’s Network offering protects on-premises, hybrid, and AWS cloud environments.

eSentire MDR provides continual monitoring and analysis of cloud applications and data stores, and detection and response services across all cloud services and applications. It can also identify data loss across cloud infrastructure and includes cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments.

The solution can detect threats across the entire IT estate, do network-based detections including full packet capture and inspection, and detect a wide range of malicious activity including ransomware and evasive malware. The solution also includes attacker behavior analytics.

On the response side, eSentire MDR can respond automatically to disrupt threats, while attack blocking capabilities include the disruption of malicious network communications and account suspensions. The solution includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced. It also supports activity recording for forensic analysis.

The solution is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, quarantining files, initiating full packet capture, carrying out sinkholing, and preventing registry changes. The solution can provide its own SOAR functionality, and it has integrations for two third-party SOAR solutions (Microsoft Sentinel and Sumo Logic). eSentire's XDR Platform's ticketing system also has an open REST API to connect to all leading SOAR and ITSM platforms.

If an automated response is not possible, eSentire's XDR platform will provide the data its SOC analyst team needs to perform a multi-signal investigation, and support manual containment actions based on predefined, approved workflows, with an MTC (mean time to contain) of 15 minutes.

eSentire's Threat Response Unit includes threat hunters on every shift, who use manual and automated threat hunting. Findings are reported regularly to customers and are used to build novel detections and complete investigative runbooks. The solution applies threat data from eSentire's threat intelligence team, customer deployments, technology partners, industry organizations, and a wide range of commercial and open-source threat intelligence feeds, including several government feeds.

The solution includes user behavior analytics, is able to capture East-West traffic for insider threat detection, and can detect and respond to insider threats, phishing attacks, and abuse of privileged access.

eSentire offers a service for assistance with initial setup and an expert team for assisting in incident analysis and remediation. Incident handling is provided as part of standard service support, but support services and documentation are available only in English. On-site support is available across North America, EMEA (Europe, Middle East, and Africa), and in Australia

Customers can use the service to outsource their SOC entirely or eSentire analysts are able to work as an extension of the internal SOC or security teams. The service includes regular risk assessment reporting and assistance in developing security and governance policies. There is also a dedicated analyst team allocated to each customer, and continual strategic and security improvement planning is included as standard.

eSentire MDR supports organizations of all sizes across most verticals, especially finance, legal, and business services. eSentire tailors its comprehensive MDR service to the needs

and capabilities of in-house SOC and security teams. eSentire plans to roll out a Cyber Resilience Score in 2023 and is enhancing its offerings for MSPs and MSSPs as part of its e3 partner ecosystem global expansion.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

eSENTIRE

Table 5: eSentire's rating

Strengths

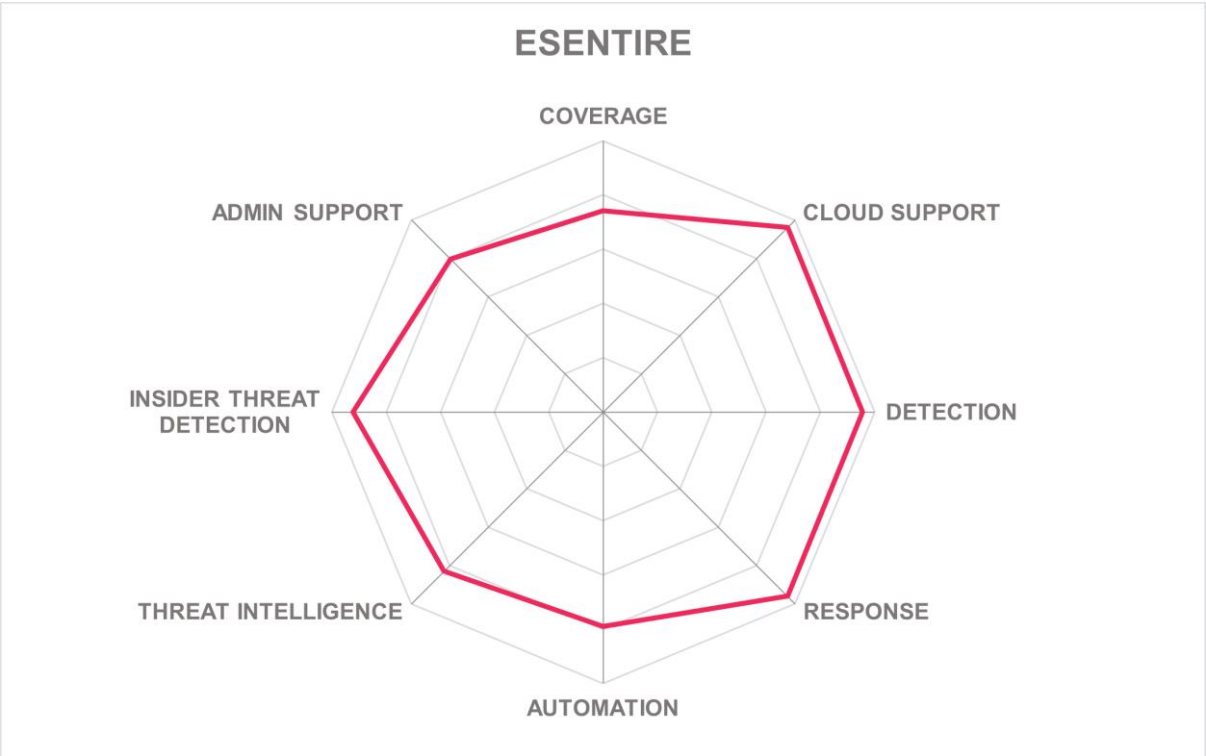
- Fast and flexible deployment.
- Coverage of all major operating systems and browsers.
- Support customers' existing technology stacks.
- Excellent support for cloud computing.
- Wide range of automated response actions supported by ML and DL.
- Strong threat hunting and threat intelligence support.
- Good detection capability for insider threats.
- Good customer support, including incident handling.

Challenges

- Providing support services and documentation in more languages could help grow existing markets and open up new ones.
- Integrating with a wider range of third-party EPDR, SIEM, and NDR products could help customers achieve better ROI.
- Reducing reliance of MDR solution on third-party products and services would improve customer confidence in ability to deploy the service.
- Increasing the diversity of cloud infrastructure used to provide services would increase customer confidence, customer choice, and flexibility in deployment.
- Currently no mobile app, but that is on the roadmap and the current web portal is mobile friendly.

Leader in





ESET – ESET PROTECT MDR

ESET is a private cybersecurity solutions company founded in 1992 and headquartered in Bratislava, Slovakia. There are SOC teams across eight SOCs in the Netherlands, France, Italy, Germany, UK, Slovakia, Japan, and the US. ESET has customers around the world, with most falling in the EMEA region and the small and medium-sized enterprise category.

ESET PROTECT MDR service is tailored to customer requirements and is delivered via the ESET PROTECT Platform based on ESET's core EDR/XDR and EPP offerings. It is therefore mainly sold as bundles made up of ESET's EPP, EDR, and other MDR related services, with pricing mostly on a per seat per year basis.

The solution covers all major operating systems and browsers, and can be deployed quickly on premises, in the cloud, or in a hybrid model, depending on customer preferences or requirements.

ESET PROTECT MDR provides continuous monitoring and analysis of all major business IT environments and systems but does not cover Edge computing environments. It also provides detection and response services across all IT and OT environments, including medical and industrial IoT devices, and remote workers.

The solution integrates with ESET's EPDR solution but does not come with any out-of-the-box integrations for any third-party EPDR, NDR, or behavior analytics products. However, ESET customers can create their own integrations using APIs. The solution does provide integrations for three SIEM solutions (IBM QRadar, ArcSight, and Splunk), and can integrate with others using SYSLOG.

ESET PROTECT MDR provides continuous monitoring and analysis of cloud applications and cloud stores, provides detection and response services across all cloud services and applications, and can identify data loss across cloud infrastructure. The solution includes cloud workload protection, but not cloud security posture management or vulnerability scanning of customer multi-cloud environments.

The solution is able to detect threats across the entire IT estate, do network-based detections that include full packet capture and inspection, and detect ransomware and evasive malware. It also includes attacker behavior analytics.

In terms of response, the solution is able to respond automatically to disrupt threats, and carry out attack blocking activities, including the disruption of malicious network communications and the suspension of accounts. The solution includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced. It also includes activity recording for forensic analysis.

ESET PROTECT MDR is able to execute predefined containment actions, including terminating processes and network sessions, isolating hosts, blocking communications by IP and port, quarantining files, sinkholing, and preventing registry changes. The solution can also provide its own SOAR capabilities and comes with out-of-the-box integrations with two third-party SOAR solutions (Microsoft Sentinel and Splunk) as well as supporting integrations with more via the ESET open API.

The solution includes the support of a dedicated threat hunting team, regular reporting on threat hunting findings, and regular and automated threat hunting activities, including retroactive threat hunting. ESET's services draw on a wide range of threat intelligence sources, including its own dedicated team of threat researchers and sensors at global customer deployments, technology partners, industry sources, and selected commercial and open-source threat intelligence sources.

ESET PROTECT MDR includes user behavior analytics, is able to capture East-West traffic for insider threat detection, and can detect insider threats, phishing attacks, and abuse of privileged access.

ESET offers a service for assistance with initial setup and an expert team for assisting in incident analysis and remediation, while incident handling is part of the standard service support. ESET offers extensive language support, with support services, management consoles, user interfaces and documentation available in up to 39 languages. ESET support is all remote with no routine provision of on-site support in any geography.

Customers can use the solution to outsource their SOC entirely or ESET SOC analysts are able to work as an extension of internal SOC or security teams. The offering includes regular risk assessment reporting, and assistance in developing security and governance policies. There is also a dedicated analyst or team allocated to each customer, and continual strategic and security improvement planning is included as standard.

ESET PROTECT MDR is suitable for organizations of all sizes, especially mid-size organizations and those organizations looking to get greater ROI from current investments, to benefit from high quality threat intelligence, and to fully outsource security operations, including threat monitoring and threat hunting, so they can focus on their core business.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Neutral
Usability	Strong Positive



Table 6: ESET's rating

Strengths

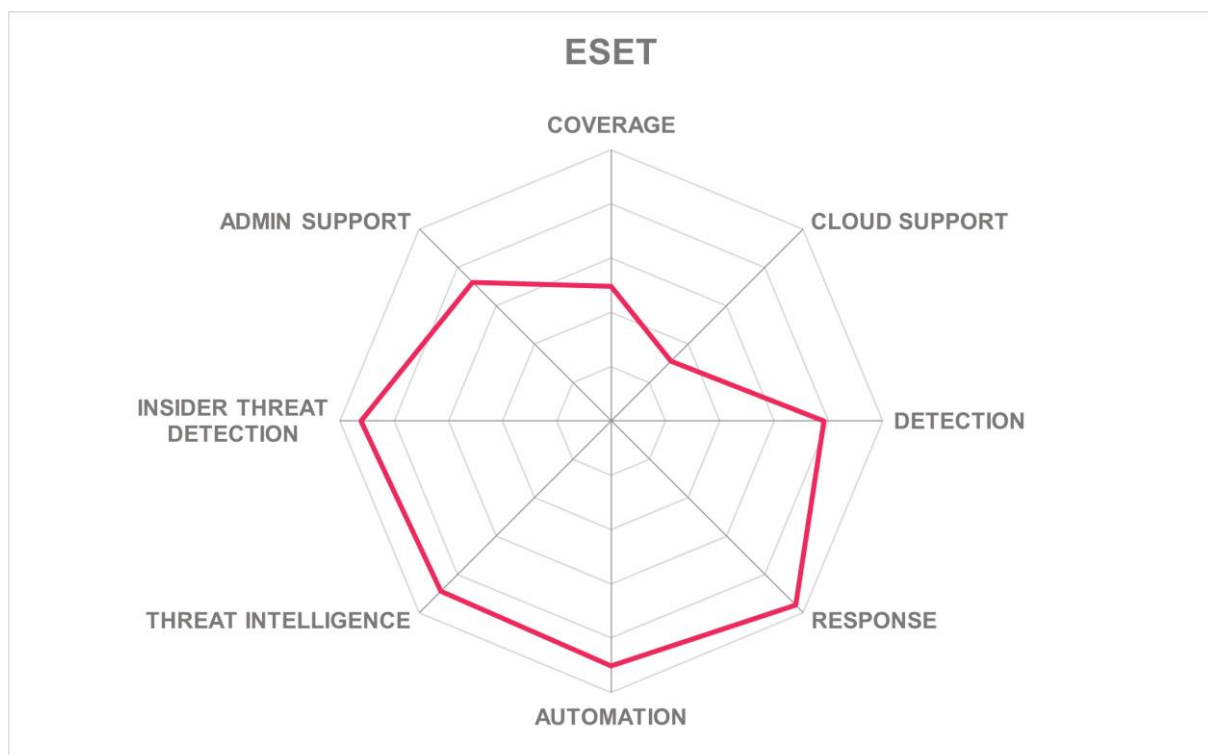
- Simple, bundled pricing model.
- Personalized, tailor made MDR service.
- Flexible deployment options.
- Wide range of automated containment actions.
- Recognized European supplier of rich threat intelligence data.
- Excellent local language support for services and documentation.
- Open API for interoperability with third-party solutions.

- Good detection capability for insider threats.

Challenges

- Expanding coverage to include Edge computing environments could drive sales among businesses that have invested in these technologies.
- Out-of-the-box integrations with EPDR, NDR, and behavior analytics products would help customers get faster value without having to create their own integrations.
- Expanding cloud support to include security posture management and multi-cloud vulnerability scanning would be attractive to customers invested in cloud computing.
- Adding a mobile app for accessing MDR information on the go would give greater flexibility and assurances to customer security teams.

Leader in



Expel – Expel Managed Detection and Response (MDR)

Expel is a private security operations provider based in the US, founded in 2016, and headquartered in Herndon, Virginia. There are three SOC teams that support a remote and distributed SOC for round-the-clock coverage for customers in major regions, except South America. Most of Expel's customers are in the US, followed by the EMEA region, and fall into the medium-sized business segment.

Expel MDR is based on its Expel Workbench, which is a tightly integrated, cloud-native, multi-tenant, transparent platform for providing monitoring and analysis of customer IT environments with the backing of Expel's team of SOC analysts. Expel Workbench is designed to support rapid, high-quality decision making, using specialist bots for triaging alerts and orchestrating response actions.

Expel's pricing model is based on a customer's attack surface, or the number of assets being protected. This is usually simplified by expressing it as a per-user cost, which is calculated based on the associated attack surface in terms of the number of SaaS accounts, desktops, laptops, servers, and cloud-based infrastructure and assets being protected.

Expel MDR is available mainly as a cloud-based service that can be deployed and implemented rapidly but can include on-premises elements in the form of a virtual appliance.

The solution covers Windows, Linux, and Mac OS, but not Android and iOS, and covers most of the main browsers, except Microsoft Internet Explorer.

Expel MDR provides round-the-clock monitoring and analysis of all major business IT environments and systems, including Edge computing environments, and provides detection and response services across most environments, including Kubernetes and remote workers but excluding OT environments and conventional, medical, and industrial IoT devices.

Expel MDR comes with prebuilt integrations with seven common third-party EPDR solutions, four NDR products (Check Point CloudGuard Security, Cisco Secure Network and Cloud Analytics, Darktrace, and Securonix), 16 SIEM solutions, and three behavior analytics products (Exabeam Fusion SIEM, IBM QRadar, and Securonix Next-Gen SIEM). In total, the solution has more than 100 tech integrations, with more SIEM integrations than any other vendor featured in this report.

The solution provides good support for cloud computing with round-the-clock monitoring and analysis of cloud applications and cloud data stores, and detection and response services across all cloud services and applications. It can also identify data loss across cloud infrastructure, and includes cloud security posture management and cloud workload protection, but not vulnerability scanning of customer multi-cloud environments.

Expel MDR is able to detect threats across the entire IT estate and carry out network-based detections, including full packet capture and inspection. It is able to detect a wide range of malicious activity, including ransomware and evasive malware. The solution also includes attacker behavior analytics.

Looking at response capabilities, Expel MDR is able to respond automatically to disrupt threats. Attack blocking capabilities include account suspensions and the automatic removal of malicious emails, but not the disruption of malicious network communications. The solution includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced. It also supports activity recording for forensic analysis.

Expel MDR is able to execute predefined containment actions automatically, including host isolation and quarantining files but not including terminating processes and network sessions, blocking communications by port and IP, carrying out sinkholing, or preventing registry changes. The solution can provide its own SOAR capabilities, and it comes with out-of-the-box integrations with three third-party SOAR solutions (Swimlane, Demisto, and Tines).

Looking at threat hunting, Expel MDR includes the support of a dedicated threat hunting team, regular reporting on threat hunting findings, and regular automated and manual threat hunting activities. The solution applies threat data from customer deployments, Expel's threat intelligence team, technology partners, and industry bodies. The solution also includes connectors to 13 common threat intelligence sources.

The solution is able to capture East-West traffic, which is used for insider threat detection, it can detect and respond to insider threats, phishing attacks, and abuse of privileged access, and includes user behavior analytics.

Expel offers a service for assistance with initial setup and an expert team for assisting with incident analysis and remediation. Incident handling is provided as part of standard service support. While support services and documentation are available only in English, other languages may be supported on a case-by-case basis. On-site support is available in North America and EMEA through strategic partners.

Customers can use the service to outsource their SOC entirely or Expel SOC analysts are able to work as an extension of the internal SOC or security teams. The solution includes assistance in developing security and governance policies but does not include regular risk assessment reporting. However, there is a dedicated analyst or team allocated to each customer and strategic, continual improvement planning is part of the standard solution.

Expel MDR is suitable for most companies, particularly medium-sized businesses, followed by mid-market and large enterprises, who are looking to maximize returns on existing investments and for full MDR coverage, including cloud and Kubernetes environments.

Security	Neutral
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



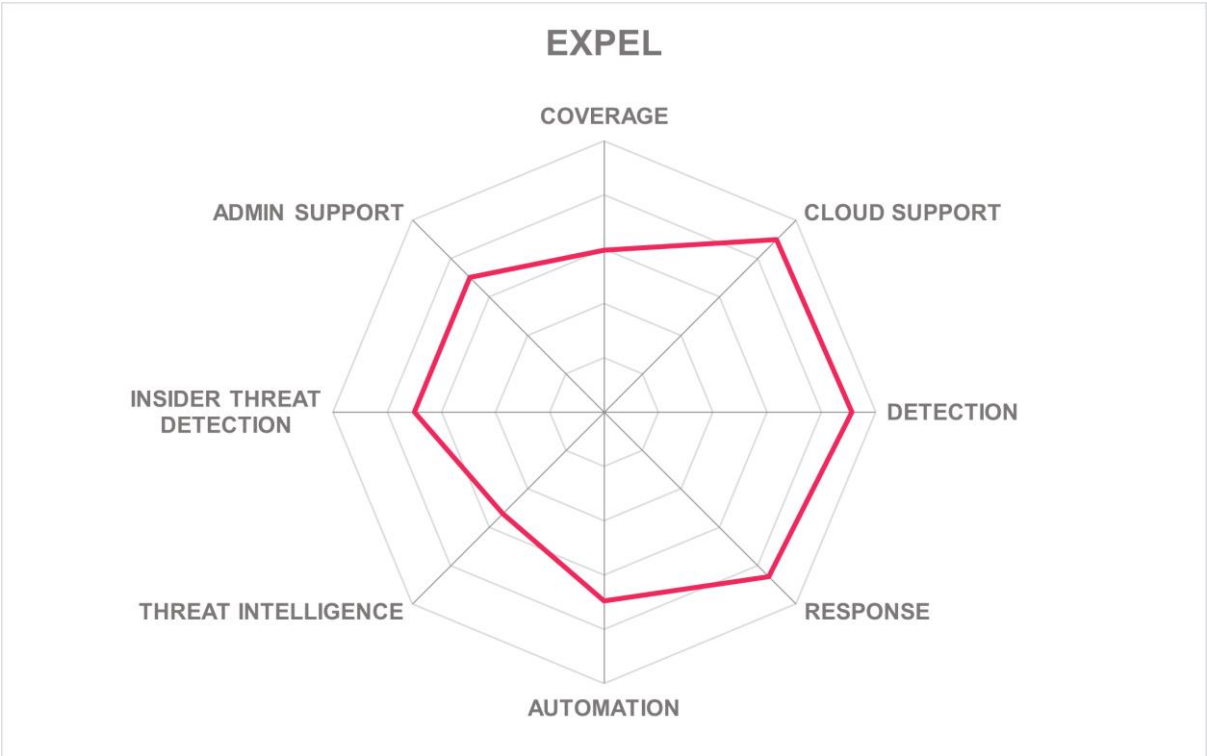
Table 7: Expel's rating

Strengths

- Rapid deployment and implementation.
- Comprehensive threat detection capabilities.
- Protection for cloud and Kubernetes environments.
- More than 100 tech integrations, including Bring Your Own Tech (BYOT).
- Highly configurable platform.
- Includes mapping to MITRE ATT&CK framework.
- Good detection capability for insider threats.

Challenges

- Extending coverage to include Android and iOS would increase appeal to customers with extensive mobile deployments.
- Expanding coverage to OT and IoT environments could grow existing markets and open up new ones, especially in manufacturing and healthcare sectors.
- Vulnerability scanning of multi-cloud environments would provide additional assurances for customers using multiple cloud service providers.
- Adding functionality to disrupt malicious network communications will improve the solution's response capabilities.
- Expanding the list of automated actions will also help to improve the solution's response capabilities.
- Risk assessment reporting would be a useful feature to add.
- No mobile app, but Expel's website is mobile ready and critical views have a mobile-optimized version.



ForeNova Technologies – NovaMDR 360°

ForeNova Technologies is a private cybersecurity company founded in 2021 and headquartered in Amsterdam, with a datacenter in Frankfurt, Germany and SOCs in Kuala Lumpur, Malaysia and Changsha, China. ForeNova is focused on small and mid-market enterprises in Europe, but it also has customers in Malaysia and Hong Kong.

NovaMDR 360° provides cloud-based management and includes the NovaCommand network sensor and the NovaGuard endpoint agent. Customers can choose to deploy collectors on premises or in the cloud.

ForeNova has a simple pricing model based on the number of “IT connected” employees being protected, which is determined during an initial scoping exercise. NovaMDR 360° is designed to make enterprise level security accessible to the mid-market.

The solution covers all main operating systems, excluding Android and iOS, and covers all main browsers. It includes round-the-clock monitoring and analysis of all major business IT environments and systems, including Edge computing environments. NovaMDR 360° provides detection and response services across most environments including medical IoT devices and remote workers, but not general and industrial IoT devices, OT environments, or mobile devices.

NovaMDR 360° includes integrations with four third-party EPDR products (Microsoft Defender for Endpoint, Sophos InterceptX Advanced with XDR, Trend Micro, and Bitdefender), but no NDR, behavior analytics, or SIEM solutions, although SIEM integrations could be supported through data sharing via SYSLOG.

The solution provides continuous monitoring and analysis of cloud applications and cloud data stores. It can identify data loss across cloud infrastructure, but it does not include cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments.

NovaMDR 360° detects threats across the entire IT estate and does network-based detections, including full packet capture and inspection. It detects a wide range of malicious activity, including ransomware and evasive malware, and includes attacker behavior analytics.

Looking at response capabilities, NovaMDR 360° can respond automatically to disrupt threats, and attack blocking capabilities include the disruption of malicious network communications but not account suspensions. The solution includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced, but it does not support activity recording for forensic analysis.

Considering automation, the solution is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, quarantining files, sinkholing, and preventing registry changes. NovaMDR 360° includes its own SOAR capabilities, with predefined and custom playbooks used to orchestrate response actions, but there are no prebuilt integrations with any third-party SOAR solutions.

NovaMDR 360° includes the support of a dedicated threat hunting team, with regular reporting on threat hunting findings. It also includes regular automated and manual threat

hunting activities. The solution applies threat intelligence data gathered from ForeNova's threat intelligence team and China-based partner, customer deployments, technology partners, industry bodies, a select number of commercial threat feeds, and a large number of open-source feeds.

The solution is able to capture East-West traffic for insider threat detection, it can detect and respond to insider threats, phishing attacks, and abuse of privileged access. It also includes user behavior analytics.

ForeNova provides a service for assistance with initial setup and an expert team for assisting in incident analysis and remediation. Incident handling is included as part of standard support. Documentation is available only in English, with German under development. Support services are mainly available in English but, where possible, they can also be provided in German, Cantonese, Mandarin, and Malaysian. On-site support is available only in Europe but may be available in other geographies via VARs if necessary.

Customers can use the service to outsource their SOC entirely or ForeNova SOC analysts are able to work as an extension of the internal SOC or security team. There is a dedicated analyst or team allocated to each customer and strategic, continual improvement planning is included as standard, but the solution does not include regular risk reporting or assistance in developing security and governance policies.

NovaMDR 360° supports organizations of all sizes but is best suited to small and mid-market enterprises, particularly in Europe, Malaysia, and Hong Kong, and those in manufacturing, healthcare, and critical infrastructure looking for a cost effective vertical specialized vendor that is responsive to customer requirements and can help maximize existing investments, including legacy systems.

Security	Neutral
Functionality	Positive
Deployment	Positive
Interoperability	Neutral
Usability	Neutral

FORENOVA 

Table 8: ForeNova's rating

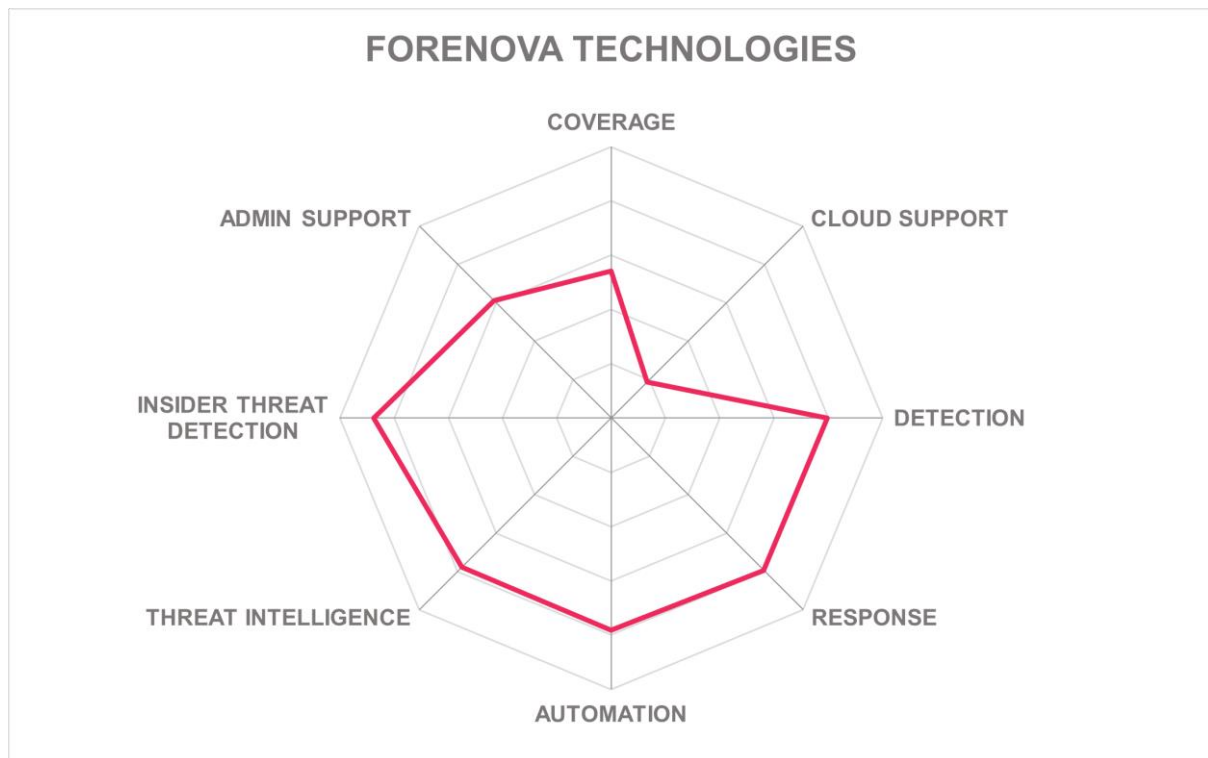
Strengths

- Strong network capabilities based on ForeNova's origins as an NDR vendor.
- Simple pricing model,
- Asia-based threat intelligence source to support APAC market.
- Fully automated alert handling supported by ML.
- Good detection capability for insider threats.
- Focus on ransomware and using honeypot techniques to lure attackers away from critical assets.
- Local language support in focus markets.
- GDPR-compliant and multi-tenant platform with fully segregated data.
- Vertical focus on critical infrastructure, manufacturing, and healthcare.

- Partnership with BSKI, the German Federal Association for the Protection of Critical Infrastructure.

Challenges

- Extending operating system support for Android and iOS would increase appeal to customers with extensive mobile deployments.
- Solution would benefit from extending coverage to all IoT and OT environments.
- Including cloud security posture management and workload protection will help assure customers that rely heavily on cloud computing services.
- Adding activity recording would help customers conduct forensic analysis of incidents.
- Providing integrations with third-party SOAR solutions would enable customers to get greater ROI out of existing SOAR investments.
- Inclusion of risk assessment reporting and help with developing security and governance policies would strengthen the offering.
- Currently limited geographical focus but planning to expand through partners.
- Adding a mobile app for accessing MDR information on the go would give greater flexibility and assurances to customer security teams.



Fortinet – Fortinet Managed Detection and Response (MDR)

Fortinet is a public, US-based cybersecurity company founded in 2000 and headquartered in Sunnyvale, California, with a single, global SOC staffed by analysts in the US, Canada, UK, Germany, India, Philippines, and Japan. Most customers are US-based, followed by EMEA, predominantly in the medium enterprise segment, followed by mid-market enterprises.

Fortinet Managed Detection and Response (MDR) leverages FortiEDR and FortiXDR technologies and is therefore sold as a bundle with an annual cost with a 100-seat minimum. Customers, including those with fewer than 100 employees, may also purchase Fortinet MDR as a managed service via MSSP partners. For customers that want to work with FortiEDR, the MDR offering is priced per node.

Fortinet MDR is a cloud-based service that includes some on-premises elements such as a virtual appliance and agents or collectors installed on endpoints. The solution covers most operating systems, excluding Android and iOS, and covers all the main browsers.

The solution provides continuous monitoring and analysis of all major business IT environments and systems, including Edge computing environments. It also provides detection and response services across all environments, including OT, remote workers, and medical and industrial IoT environments. Fortinet MDR comes with prebuilt integrations for 14 third-party behavior analytics solutions, with the option of adding others via custom python scripts using APIs, but there are no prebuilt integrations for any third-party EPDR or NDR. However, the solution supports data sharing via LEEF/CEF, making it possible to integrate with SIEM products.

Looking at support for cloud computing, Fortinet MDR provides monitoring and analysis of cloud applications and cloud data stores. It provides detection and response services across all cloud services and applications but cannot identify data loss across cloud infrastructure. It also does include cloud security posture management and cloud workload protection, but not vulnerability scanning across customer multi-cloud environments.

Considering detection capabilities, Fortinet MDR is able to detect threats across the entire IT estate, but network-based detections do not include full packet capture and inspection. However, the solution is able to detect a wide range of malicious activity, including ransomware and evasive malware, but it does not include attacker behavior analytics.

Fortinet MDR is able to respond automatically to disrupt threats, and attack blocking capabilities include the disruption of malicious network communications and account suspensions through Active Directory integration. The solution includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced, but it does not support activity recording and playback for forensic analysis.

The solution is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, quarantining files, and preventing registry changes but not carrying out sinkholing activities. The solution also provides its own SOAR functionality for basic playbook

creation and provides prebuilt integrations for 22 third-party SOAR solutions. Custom integrations are also possible.

Fortinet MDR is supported by a dedicated threat hunting and reverse engineering team which includes regular manual and automated threat hunting, as well as regular reporting on threat hunting activities. The solution applies threat data from Fortinet's threat intelligence team, more than 660,000 customer deployments, technology partners, industry organizations, and a combination of more than 200 commercial and open-source threat intelligence feeds.

The solution is able to capture East-West traffic for insider threat detection, and can detect and respond to insider threats, phishing attacks, and abuse of privileged access. However, it does not include user behavior analytics.

Fortinet offers a service for assistance with initial service setup and an expert team for assisting with incident analysis and remediation. Incident handling is provided as part of standard service support, but support services are available only in English and Spanish, while documentation is available only in English. On-site support is available at an additional fee.

Fortinet MDR is designed to support internal SOC and/or security teams in larger, more mature organizations, and cannot be used by customers to outsource their SOC function entirely. The service includes assistance in developing security and governance policies but does not include regular risk assessment reporting. Strategic continual improvement planning is not part of the standard subscription but is available for an additional fee.

Fortinet MDR supports all but the smallest of businesses and is best suited to medium and mid-market enterprises that have internal SOC and/or security teams but are looking for round-the-clock threat monitoring and analysis, alert management, automated containment actions, and support in threat response and incident remediation.

Security	Neutral
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Neutral



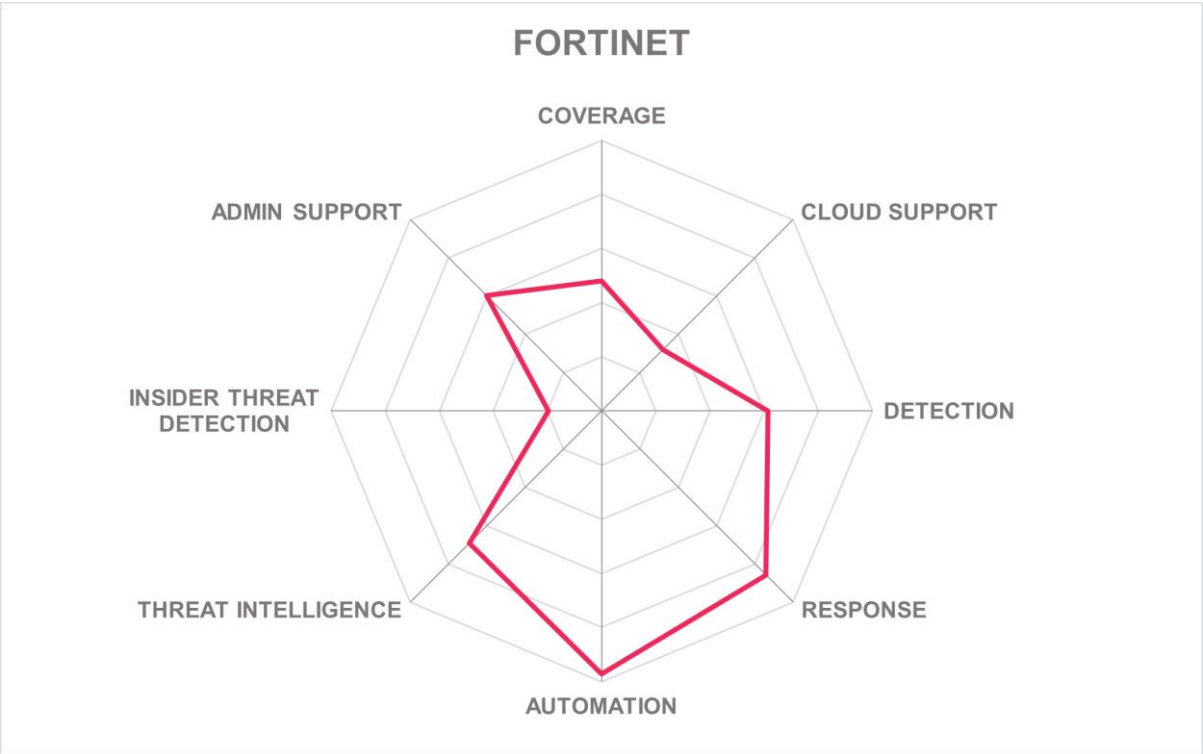
Table 9: Fortinet's rating

Strengths

- Simple pricing model based on technology bundle and optional add-ons.
- Wide range of automated containment actions available.
- Includes SOAR functionality and includes integrations with a large number of third-party SOAR solutions.
- Wide range of telemetry data from sensors in production environments and a large number of threat intelligence sources, including government feeds
- Wide range of additional security and advisory services available to MDR customers.

Challenges

- Adding integrations with third-party EPDR and NDR solutions would help customers get greater ROI from existing investments.
- Including attacker behavior analytics would help boost solution's detection capabilities.
- Adding user activity recording would help customers conduct forensic analysis of incidents.
- Including user behavior analytics would improve the solution's ability to detect insider threats.
- Expanding language support could help grow existing markets and open up new ones.
- Risk assessment reporting would be a good feature to add to enable customers to adopt a more proactive approach to security.
- Adding a mobile app for accessing MDR information on the go would give greater flexibility and assurances to customer security teams.



IBM Security – Managed Detection and Response

IBM Corporation is a multinational technology and consulting company founded in 1911 and headquartered in Armonk, New York, USA. With over 100 years of history, IBM has evolved from a computing hardware manufacturer to offer a wide range of services, including MDR. IBM has 200 SOC teams attached to 13 SOCs across the US and in Brazil, Poland, Hungary, Saudi Arabia, India, Australia, and Japan. Most customers are located in North America and EMEA, with the majority falling into the large enterprise category.

IBM Security Managed Detection and Response (MDR) is priced in various tiers based on the number of alerts with some variation depending on the number of alerts investigated and the number of incident response cases managed. Customers have the option of opting for alerting and investigation without incident management.

IBM MDR is deployed as a managed service based on the IBM MDR platform hosted in IBM facilities that can support customer technology regardless of whether it is deployed on premises, in the cloud or in a hybrid fashion.

The service covers all major operating systems and browsers, it provides round-the-clock monitoring and analysis of all major business IT environments and systems, including Edge computing environments, and provides detection and response services across all environments, including medical and industrial IoT, OT, and remote workers.

IBM MDR includes prebuilt integrations with 19 third-party EPDR products, 21 NDR products, 15 SIEM solutions, and 14 behavior analytics products.

The service provides good support for cloud computing with round-the-clock monitoring and analysis of cloud applications and cloud data stores, with detection and response services across all cloud services and applications, and the ability to detect data loss across cloud infrastructure. IBM MDR also includes cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments.

IBM MDR is able to detect threats across the entire IT estate, do network-based detections including full packet capture and inspection, as well as detect a wide range of malicious activity, including ransomware and evasive malware. The service also includes attacker behavior analytics.

In terms of response, the service is able to disrupt threats automatically, with attack blocking capabilities including the disruption of malicious network communications and account suspensions. The service includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced. It also supports activity recording for forensic analysis.

IBM MDR is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, quarantining files, carrying out sinkholing, and preventing registry changes. The service can provide its own SOAR capabilities, and also comes with prebuilt integrations for 21 third-party SOAR solutions.

The service is backed by a team of threat hunters, which is either a pooled resource or a dedicated team, depending on customer maturity level and budget. The service also includes regular manual and automated threat hunting activities as well as regular reporting on the findings. The service applies threat intelligence gathered from IBM threat intelligence team, customer deployments, technology partners, industry bodies, and a select number of commercial and open-source threat intelligence feeds. Connectors are also provided to 35 different external cyber threat intelligence sources.

IBM MDR is able to capture East-West traffic used for insider threat detection, it can detect and respond to insider threats, phishing attacks, and abuse of privileged access. It also includes a comprehensive and customizable analytics capability, including user behavior analytics.

IBM offers a service for assistance with the initial setup of the service through the company's consulting and systems integration team. It also provides the services of an expert team for assisting with incident response and remediation. Incident handling is provided as part of the standard support service. While support services are available in nine languages, documentation is available only in English, although local account managers can provide translations where necessary. On-site support is available in all major geographies.

Customers can use the service to outsource their SOC entirely or IBM SOC analysts are able to work as an extension of the internal SOC or security team. The service includes regular risk assessment reporting, and assistance in developing security and governance policies. There is also a dedicated analyst or team allocated to each customer, and continual strategic and security improvement planning is included as part of the standard subscription.

IBM Security Managed Detection and Response is best suited to large, mid-market and medium enterprises across all verticals looking for a comprehensive MDR solution with a high degree of customization and interoperability with third-party security products to maximize ROI.

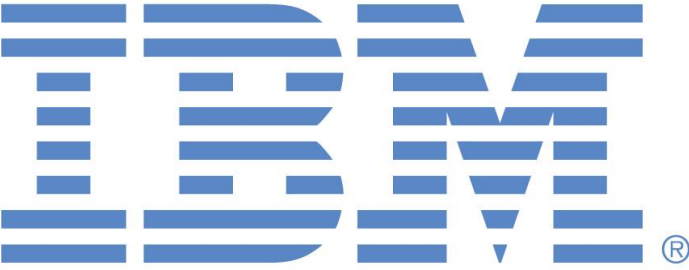
Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 10: IBM's rating

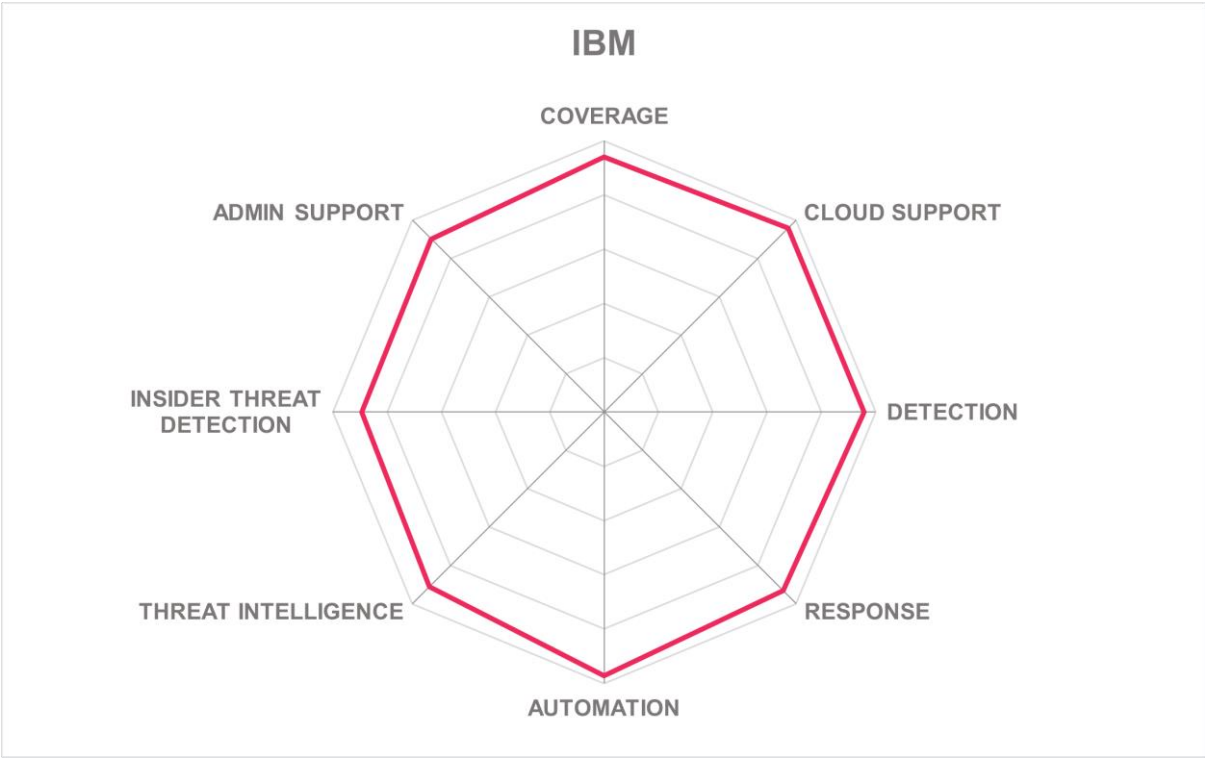
Strengths

- Flexible and fairly simple pricing model.
- Customizable IBM hosted rapid deployment model.
- Comprehensive MDR coverage of all business IT environments.
- Vendor agnostic to maximize the ROI on existing security investments.
- Prebuilt integrations with major EPDR, NDR, SIEM, and behavior analytics products.
- Strong support for cloud computing environments.
- Wide range of detection and response capabilities.
- Extensive and customizable automated response capabilities.
- Built in SOAR functionality as well as a wide range of SOAR integrations.
- Strong threat hunting and threat intelligence capability supported by ML algorithms.
- Wide range of insider threat detection capabilities.
- On-site support available around the world.
- Includes mobile app for cyber defenders wherever they may be.

Challenges

- Making non-English support services available 24/7 and documentation available in more languages could help expand existing markets and open up new ones.
- Including breach and attack simulation tools as part of the standard offering rather than as an optional extra would increase value for customers.
- Service would benefit from deeper integration with cloud-native security capabilities, but this is on the roadmap.
- Including managed WAF capability as part of the standard offering rather than an optional extra would increase value for customers.
- Service would benefit from tighter integration with attack surface management and vulnerability management, but this is on the roadmap.
- Including security awareness training support as part of the standard offering rather than an optional extra would improve security posture and increase service value.

Leader in



Kroll – Kroll Responder

Kroll is a private US-based risk and financial advisory services firm established in 1972 and headquartered in New York City. Kroll offers a range of cybersecurity services, including MDR, which is supported by a single global SOC split across four locations in the US, UK, and two in the APAC region. Most customers are in North America, followed by EMEA, and fall into the mid-market segment.

Kroll Responder is a service designed to provide MDR capabilities and offer a single pane of glass solution based on its XDR platform acquired from Redscan that uses a combination of inputs from customer SIEM, EDR, and NDR technologies. The service can be adapted to required customer outcomes and existing security technology investments.

The pricing model depends on the combination of SIEM, EDR, and NDR used, taking into consideration the number of endpoints covered and the volume of SIEM data ingested by the platform.

Kroll offers flexible deployment architectures, which means the solution can be deployed as a cloud-based service only or as a cloud-based service with on-premises elements in the form of software, virtual and physical appliances, as well as agents installed on endpoints. Customers have the option of retaining all data on premises.

The MDR service covers all main operating systems, including Android and iOS, and all main browsers, including Opera and MS Internet Explorer.

The service provides round-the-clock monitoring and analysis of all major business IT environments and systems, including Edge computing environments, and provides detection and response services across all environments, including medical and industrial IoT devices and remote workers.

Kroll's MDR service includes prebuilt integrations with 11 third-party EPDR solutions, 10 NDR solutions, four SIEM solutions (Microsoft Sentinel, LogRhythm, Splunk, and AT&T Alien Vault), and four behavior analytics products (Microsoft Advanced Threat Analytics, ObserveIT, Onelidentity Safeguard, and Splunk UBA), with the option of adding further integrations via a SIEM platform.

Kroll Responder provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response services across all cloud services and applications. It is also able to identify data loss across cloud infrastructure, and includes cloud workload protection and vulnerability scanning of customer multi-cloud environments but does not include cloud security posture management.

The Kroll MDR service has the ability to detect threats across the entire IT estate, it does network-based detections including full packet capture and inspection and can detect and respond to a wide range of malicious activity, including ransomware and evasive malware. The service also includes attacker behavior analytics. All detections are intelligence led and mapped to the MITRE ATT&CK framework.

The service is able to respond automatically to disrupt threats, and attack blocking capabilities include the disruption of malicious communications and account suspensions. The service includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced. The service also includes activity recording for forensic analysis. All responses are forensics led.

Kroll Responder is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, quarantining files, carrying out sinkholing, and preventing registry changes. The service is also able to provide its own SOAR functionality and comes with integrations for three third-party SOAR solutions (Microsoft Sentinel, LogRhythm, and Swimlane).

The service does not include a dedicated threat hunting team, but this is available as an additional option. The service applies threat data gathered from Kroll's threat intelligence team, customer deployments, technology partners, industry bodies, a select number of commercial intelligence feeds and a large number of open-source feeds. It also provides connectors for seven threat intelligence sources and maintains its own database of IoCs gathered from incident response activities.

Kroll Responder is able to capture East-West traffic for insider threat detection, it can detect and respond to insider threat threats, phishing attacks, and abuse of privileged access, and includes user behavior analytics.

Kroll offers a service for assistance with initial setup and an expert team for assisting with incident analysis and remediation. Incident handling is provided as part of standard service support. Documentation is available only in English, but support services are available in English, Spanish, Portuguese, Italian, and Japanese. In addition to remote support, on-site support is available around the world.

Customers can use the service to outsource their SOC entirely or Kroll analysts are able to work as an extension of the internal SOC or security team. The offering includes regular risk assessment reporting and assistance in developing security policies but not governance policies. There is also a dedicated analyst or team allocated to each customer, and continual, strategic improvement planning is part of the standard subscription.

Kroll Responder supports organizations of all sizes, provides a \$1m Incident Protection Warranty for all customers, and is best suited to organizations focused on reducing cyber risk, requiring global support, and looking for MDR services based on insights from incident response engagements around the world.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 11: Kroll's rating

Strengths

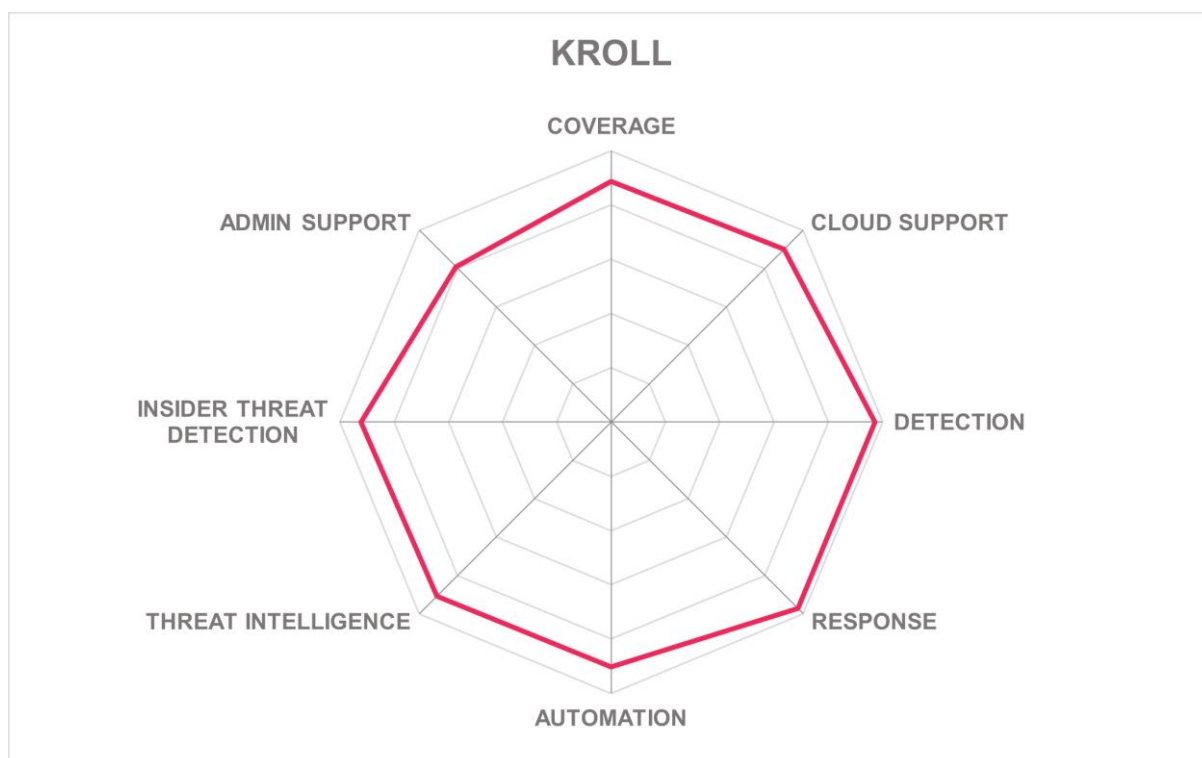
- Cloud-first approach with rapid deployment.
- Flexible deployment options.
- Good MDR coverage of cloud computing environments.
- Wide range of detection coverage and capabilities.
- Good response capabilities, including post-remediation and forensic support.

- Provides Kroll incident responders for major incidents to restore business operations.
- Wide range of automatic containment actions.
- A large number of threat intelligence sources.
- Supports detection and response to insider threats.
- Mobile app to support cyber defenders wherever they are.

Challenges

- Adding cloud security posture management would improve cloud security support.
- Increasing language support for documentation and support services could help grow existing markets and open up new ones.
- Adding assistance in developing governance policies would complement the support for security policy development and risk assessments.
- Including security awareness training as part of the standard subscription would increase value to customers looking for continual security improvement.
- Increasing the number of prebuilt integrations with third-party SOAR solutions would enable customers to get better ROI from exiting SOAR investments.

Leader in



Proficio – ProSOC MDR

Proficio is a private, American managed security services provider (MSSP) founded in 2010 and headquartered in Carlsbad, California, with SOCs in Carlsbad (US), Singapore, and Barcelona (Spain). Proficio has customers around the world, with the majority based in the US, followed by APAC. They cater to all sizes of organization with most customers in the mid-market segment.

Proficio's MDR service is built around its cloud-based ProSOC MDR Platform, which includes SIEM (Splunk), SOAR, XDR, and ITSM (ServiceNow) functionality.

Proficio's charging can be per user, per node or based on volume of log ingestion depending on the combination of services provided with MDR. Proficio's Active Defense XDR automated response, vulnerability management, and managed services for third-party SIEM, SOAR, and EDR are all optional extras to the standard MDR offering.

If logs can be collected by API, Proficio's ProSOC MDR may be entirely cloud based, but if logs require local collection and parsing, Proficio uses a software virtual image as a log collector on premises. Proficio also offers a delivery model where the customer owns the SIEM/SOAR that may be either cloud based or on premises. Proficio offers specialist support for Splunk and Microsoft Sentinel.

ProSOC MDR covers Windows, Linux, and Mac OS but not Android and iOS, and covers all the main browsers.

The solution provides round-the-clock monitoring and analysis of all major business IT environments and systems, including Edge computing environments, and provides detection and response services across all environments, including medical and industrial IoT devices, and remote workers.

ProSOC MDR includes integrations with 14 common third-party EPDR products, four SIEM products (Micro Focus ArcSight, Microsoft Sentinel, Splunk, and ElasticSearch), six SOAR solutions, 11 NDR products, and four behavior analytics products (HPE Security ArcSight, Microsoft Advanced Analytics, ObserveIT, and Splunk UBA), with custom integrations available for a fee.

There is good support for cloud computing with monitoring and analysis of cloud applications and cloud data stores, with detection and response services across all cloud services and applications, and the ability to identify data loss across cloud infrastructure. ProSOC MDR also includes cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments.

ProSOC MDR is able to detect threats across the entire IT estate, do network-based detections including full packet capture and inspection, and detect a wide range of malicious activity, including ransomware and evasive malware. The solution also includes attacker behavior analytics.

In terms of response, the solution is able to automatically disrupt threats. Attack blocking capabilities include the disruption of malicious network communications, account suspensions, and endpoint quarantining. The solution includes post-remediation support to

validate that a threat has been neutralized and verify that it has not resurfaced. It also supports activity recording for forensic analysis.

ProSOC MDR is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, and blocking communications by port and IP but not quarantining files, carrying out sinkholing, or preventing registry changes. The solution can provide its own SOAR capabilities and has integrations for six common third-party SOAR solutions, with custom integrations available for a fee.

Looking at threat hunting and threat intelligence capabilities, ProSOC MDR includes the support of a dedicated threat hunting team, regular reporting on threat hunting findings, and regular automated threat hunting activities supported by machine learning capabilities. The solution applies threat data from customer deployments, Proficio's threat intelligence team, and commercial and open-source external threat intelligence sources. It includes connectors to 15 common threat intelligence sources, with custom connections available for a fee.

The solution is able to capture East-West traffic for insider threat detection, it can detect and respond to insider threat threats, phishing attacks, and abuse of privileged access and includes user behavior analytics.

Proficio offers a service for assistance for initial service setup and an expert team for assisting in incident analysis and remediation. Incident handling is provided as part of standard service support, but support services and documentation are available only in English and Spanish. On-site support is available in all major geographies, except South America.

Customers can use the service to outsource their SOC entirely or Proficio SOC analysts are able to work as an extension of the internal SOC or security teams. The solution includes regular risk assessment reporting, and assistance in developing security and governance policies. There is also a dedicated analyst team allocated to each customer and continual strategic and security improvement planning is included as part of the standard subscription.

Proficio's MDR service supports organizations of all sizes with flexible delivery models for full SOC outsourcing or co-management of customer-owned SIEM/SOAR systems, with a focus on detecting and blocking authenticated but unauthorized access, and triggering response actions through integration with standard security devices and controls.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 12: Proficio's rating

Strengths

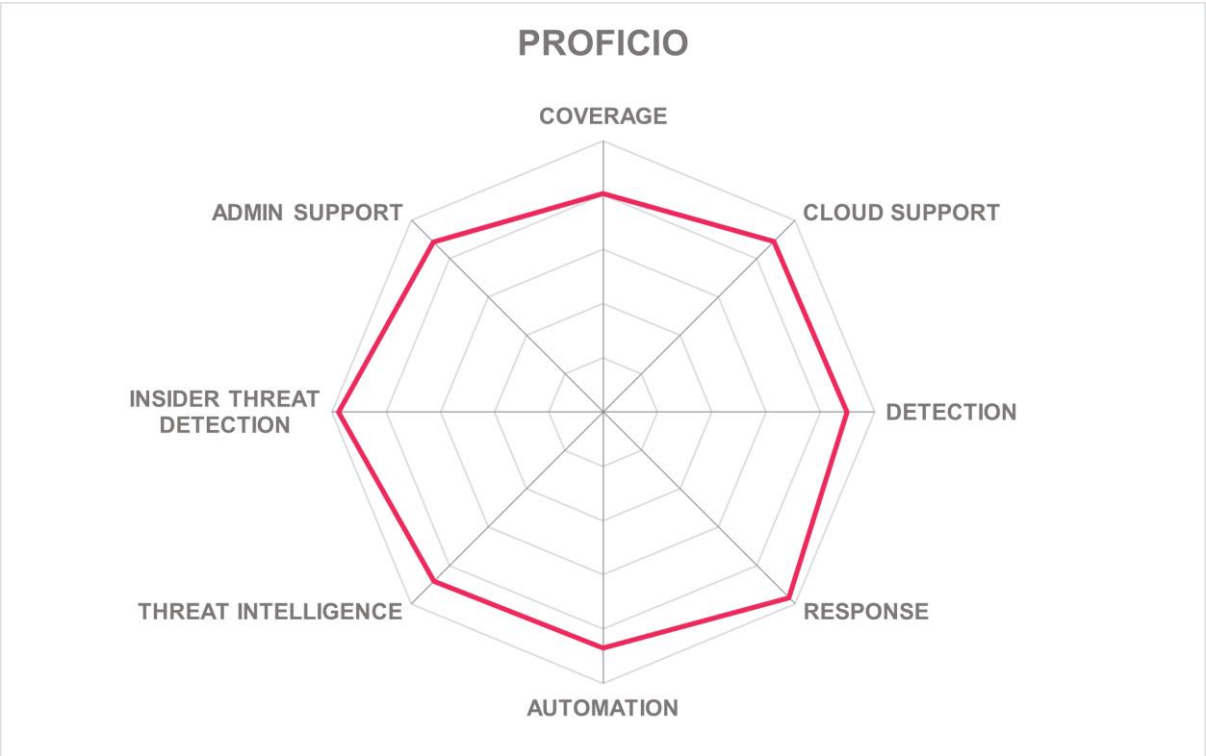
- Flexible deployment and delivery.
- Covers all main business IT environments.
- Specialist support for Splunk and Microsoft Sentinel.
- Coverage of Windows, Linux, and Mac OS.
- Strong support for cloud computing environments.
- Can execute predefined containment actions automatically.
- Strong threat hunting and threat intelligence capabilities.
- Good customer support, including incident response and on-site support.
- Mobile app to support cyber defenders wherever they are.

Challenges

- Extending coverage to Android and iOS mobile operating systems would provide support to customers with large mobile deployments.
- Expanding language support beyond English and Spanish could grow existing markets and open up new ones.
- Extending on-site support to South America could open up new markets.
- Increasing the communication channels with in-house security teams such as SMS and Slack would improve support through greater flexibility and faster interactions.

Leader in





Red Canary – Red Canary MDR

Red Canary is a private, American managed detection and response company founded in 2014 and based in Denver, Colorado. It has a global virtual SOC staffed by more than 30 analysts located in North America. Most customer organizations are medium enterprises, with most located in North America.

Red Canary MDR is deployed exclusively as a cloud-based service allowing for rapid deployment, and has a simple pricing model for three different types of coverage. For endpoint and network coverage, pricing is on a per endpoint basis. Cloud coverage (AWS, GCP, Azure) is charged according to the cloud resources protected. Pricing for user protection is based on the number of accounts monitored.

The solution covers all operating major systems, excluding Android, and all major browsers, except MS Internet Explorer and Opera. Round-the-clock monitoring and analysis is provided for most elements of IT, including Edge computing environments. Detection and response is provided for most environments, including OT, IoT, and IIoT but excluding medical IoT, and mobile devices.

Red Canary MDR includes integrations with six common third-party EPDR products, three NDR products (Darktrace, ExtraHop Reveal X, and Cisco Umbrella), two SIEM products (Microsoft Sentinel and Splunk). There are no out-of-the-box integrations with any third-party behavior analytics solutions. Red Canary has thousands of proprietary behavior-based analytics and detectors running across the environments of all its customers.

The solution provides monitoring and analysis of cloud applications and cloud data stores and can identify data loss across cloud infrastructure. It provides detection and response capabilities across all cloud services and applications with which it integrates. The solution includes cloud security posture management and cloud workload protection but not vulnerability scanning of customer multi-cloud environments.

Red Canary MDR is able to detect threats across the entire IT estate, but network detections do not include full packet capture and inspection. The solution is able to detect and respond to a wide range of malicious activity, including ransomware and evasive malware, and includes attacker behavior analytics.

On the response side, the solution is able to automatically disrupt threats. Attack blocking capabilities include the disruption of malicious network communications and account suspensions. The solution also provides post-remediation support to validate that a threat has been neutralized and to verify that it has not resurfaced. It also supports activity recording for forensic analysis.

Red Canary MDR is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, suspending users and forcing reauthentication, and quarantining files, but it cannot carry out sinkholing activities or preventing registry changes. The solution can provide its own SOAR functionality and has prebuilt integrations with three common third-party

SOAR solutions (Microsoft Sentinel, ServiceNow, and Splunk), with other SOAR integrations possible using webhooks or APIs.

The solution includes the support of a dedicated threat hunting team and regular automated threat hunting and provides regular reporting on threat hunting findings. Red Canary MDR includes the application of threat data from customer deployments, incident response engagements, technology partners, Red Canary's threat intelligence team, and commercial and open-source threat intelligence feeds. Machine learning models are trained on more than 365 petabytes of data ingested from customers per year.

Red Canary MDR is able to capture East-West traffic for insider threat detection, it can detect and respond to phishing attacks, abuse of privileged access, and insider threats, and includes behavior analytics.

Red Canary offers a service for assistance with initial setup and an expert team for assisting in incident analyst and remediation. Incident handling is part of the standard service support, although support and documentation are available only in English. There is no direct on-site support in any region due to the SaaS delivery model, but it can be provided by IR consulting partners if necessary.

The service can be used to outsource customers' SOC's entirely or Red Canary analysts are able to work as an extension of the internal SOC or security teams. The solution includes regular risk assessment reporting, and assistance in developing security and governance policies. Red Canary does not allocate a dedicated analyst team to each customer, but continual strategic and security improvement planning is included as part of the standard subscription, and there is 24x7 support by the threat hunting team.

Red Canary MDR caters for all sizes of organization as well as MSPs and MSSPs but is best suited to mid-market and enterprise level companies, especially organizations with Linux based production systems and those looking for an MDR partner to enable them to focus more on their core business.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive



Table 13: Red Canary's rating

Strengths

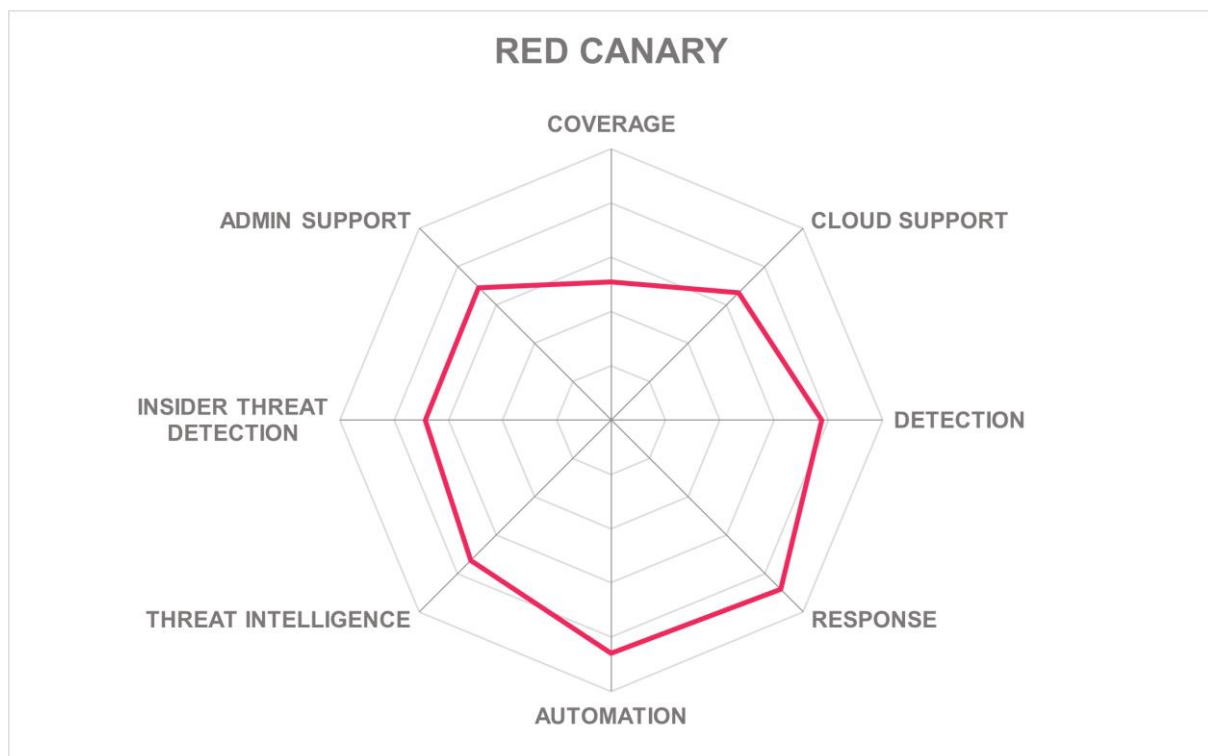
- SaaS model with deployment within seven days.
- Simple pricing model.

- Covers all major operating systems.
- Strong threat intelligence capability.
- ML models supported by rich threat data from customer sites.
- Accurate threat detection capability supported by analytics and telemetry.
- Good response capabilities.
- Provide Linux EDR protection for production systems.

Challenges

- Extending coverage to medical IoT and mobile devices may open up new markets.
- Extending detection and response to all cloud services and applications will provide greater assurances to customers heavily invested in cloud.
- Expanding support languages beyond English may open up new markets.
- Adding a mobile app for accessing MDR information on the go would give greater flexibility and assurances to customer security teams.

Leader in



ReliaQuest – ReliaQuest GreyMatter

ReliaQuest is private, US-based, cybersecurity technology company founded in 2007 and headquartered in Tampa, Florida, with eight security teams across five technical operations centers located in Ireland, India, and three cities in the US. ReliaQuest's customers come from companies of all sizes with the majority from large and mid-size segments. Most customers are mainly located in the US, followed by EMEA.

ReliaQuest's MDR services are wrapped around its GreyMatter cloud-based, AI-supported security operations platform built on an open XDR architecture, and come in three packages: Managed, Extended, and Automated. The packages are designed to meet different use cases depending on the level of co-management required by a customer.

Within the three packages, the price of services is made up of a base cost for the GreyMatter platform, depending on the size of the organization and the amount of data coming into the customer SIEM and EDR solutions, and a range of other factors such as the number of users and the number of technology integrations required.

Deployment is either entirely cloud based, or cloud based with some on-premises elements, such as software installed on enterprise hardware and virtual appliances.

The solution covers all major operating systems and browsers, and provides continuous monitoring and analysis of all major business IT environments and systems, including Edge computing environments. It provides detection and response services across all environments, including medical and industrial IoT, OT, and remote workers.

The ReliaQuest MDR service provides integrations with a wide range of third-party EPDR and NDR products. It also comes with integrations for eight common SIEM solutions and four behavior analytics products (Exabeam Fusion SIEM, IBM QRadar UBA, Microsoft Advanced Threat Analytics, and Splunk UBA).

The solution provides continuous monitoring and analysis of cloud applications and cloud data stores, with detection and response services across all cloud services and applications, and the ability to identify data loss across cloud infrastructure. ReliaQuest's MDR service also includes cloud security posture management and cloud workload protection, but not vulnerability scanning of customer multi-cloud environments.

Looking at detection, the service detects threats across the entire IT estate, with network-based detections that include full packet capture and inspection. It can detect a wide range of malicious activity, including ransomware and evasive malware. The service also includes attacker behavior analytics.

On the response side, the solution responds automatically to disrupt threats, while attack blocking capabilities include the disruption of malicious communications and account suspensions. The solution includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced. It also supports activity recording for forensic analysis.

The ReliaQuest MDR service is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts,

blocking communications by port and IP, quarantining files, carrying out sinkholing activities, and preventing registry changes. The service also includes its own SOAR functionality and comes with integrations for eight third-party SOAR solutions.

The service includes the support of a dedicated threat hunting team, regular automated and manual proactive and retroactive threat hunting activities, and regular reporting on the findings. ReliaQuest applies threat intelligence from its own threat intelligence team, customer deployments, technology partners, industry bodies, and a select number of commercial and open-source intelligence feeds, supplemented by ReliaQuest's analysis of deep and dark web data. It includes connectors to five common threat intelligence sources.

Looking at insider threats, the service is able to capture East-West traffic for detecting insider threats, it can detect and respond to insider threats, phishing attacks, and abuse of privileged access, and includes user behavior analytics.

ReliaQuest offers a service for assistance with initial service setup and an expert team for assisting with incident analysis and remediation. Incident handling is provided as part of standard service support, but support services are available only in English and Spanish, while documentation is available only in English. On-site support is available in all major geographies.

Customers can use the service to outsource their SOC entirely or ReliaQuest SOC analysts are able to work as an extension of the internal SOC or security teams. The service includes regular risk assessment reporting, and assistance in developing security and governance policies. There is also a dedicated analyst or team allocated to each customer and continual strategic and security improvement planning is included as standard.

The ReliaQuest MDR service supports organizations of all sizes, including small businesses, especially those needing to integrate with legacy security tools or looking to get greater ROI from security technology investments.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive



Table 14: ReliaQuest's rating

Strengths

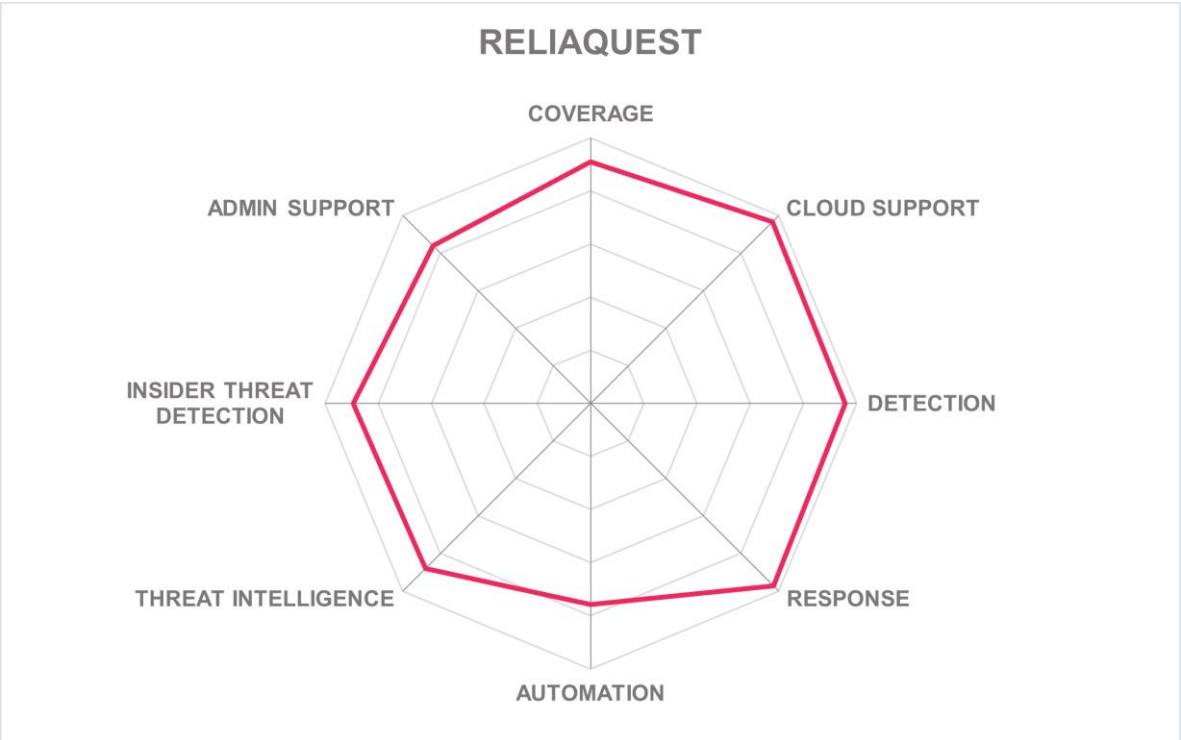
- Comprehensive MDR coverage of business IT environments.
- Wide range of integrations with third-party EPDR and NDR products.
- Supports bi-directional integrations to maximize ROI from security tools.
- Good MDR coverage of cloud computing environments.
- Wide range of automated containment actions.
- Includes SOAR functionality and comes with SOAR integrations.
- Strong threat hunting capability that is proactive and retroactive.
- Detection capabilities for insider threats.
- On-site support available around the world.
- Mobile app to support cyber defenders wherever they are.

Challenges

- Building integrations with more SIEM and behavior analytics products will help customers increase their ROI on existing investments. This is on ReliaQuest's roadmap.
- Adding vulnerability scanning of multi-cloud environments would add support to customers using multiple cloud providers. This is planned for 2023.
- Expanding language options for documentation and support services could help grow existing markets and open up new ones.
- Including security awareness training as part of the standard subscription would increase value to customers looking for continual security improvement.
- Adding capabilities to analyze OT and IoT protocols would improve offering. This is on the roadmap and currently under development.

Leader in





SecurityHQ – Managed Detection and Response (MDR)

SecurityHQ is a privately held global Managed Security Services Provider (MSSP), founded in 2003 with headquarters in London. The company has six SOC's located in the US, the UK, the UAE, South Africa, India, and Australia. Most customers are located in the EMEA region, followed by APAC, with most falling in the mid-market and medium enterprise segments.

SecurityHQ's Managed Detection and Response (MDR) service was established in 2008, and is underpinned by the company's Response Platform, which includes all necessary functionality and does not require any additional software purchases. The MDR service sits alongside the company's CISO-as-a-Service offering and other managed security services, including gap analysis, threat intelligence, and vulnerability management.

The solution is deployed as a cloud-based service using a SaaS model, but a hybrid deployment with some on-premises elements is available, including on-premises software installation, virtual appliances, and agents on endpoints. Pricing is based on a combination of the number of users and events per second (log volume), with additional costs on a per appliance basis for things like their firewall services.

SecurityHQ MDR provides coverage of all major operating systems and browsers, and round-the-clock monitoring and analysis of all major business IT environments and systems, including Edge computing environments. It also provides detection and response services across all environments, including medical and industrial IoT, OT, and remote workers.

The solution includes integrations with 13 third-party EPDR products, 10 NDR products, seven SIEM solutions, and five behavior analytics products.

SecurityHQ provides round-the-clock monitoring and analysis of cloud applications and cloud data stores. It provides detection and response services across all cloud services and applications, and includes the ability to identify data loss across cloud infrastructure. The service also includes cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments.

Looking at detection, the solution is able to detect threats across the entire IT estate, do network-based detections including full packet capture and inspection, and detect a wide range of malicious activity, including ransomware and evasive malware. The service also includes attacker behavior analytics.

On the response side, the solution is able to disrupt threats automatically, while attack blocking capabilities include the disruption of malicious network communications and account suspensions. Post-remediation support includes validation that a threat has been neutralized and verification that it has not resurfaced. The service also supports activity recording for forensic analysis.

SecurityHQ MDR is able to execute predefined containment actions, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, and quarantining files. The solution cannot carry out sinkholing activities or prevent registry changes. It can however provide SOAR functionality through the inclusion of IBM's Resilient SOAR Platform but does not come with integrations for any other third-party SOAR solutions.

The solution includes the support of a dedicated threat hunting team, regular automated and manual threat hunting activities, and regular reporting on threat hunting findings. It applies threat data gathered from its own threat intelligence team, customer deployments, technology partners, industry bodies, and a select number of commercial and open-source intelligence feeds. It also provides connectors to eight cyber threat intelligence sources and shares threat intelligence across customers from different regions and sectors.

SecurityHQ MDR is able to capture East-West traffic for insider threat detection and can detect and respond to insider threats, phishing attacks, and abuse of privileged access. It includes ML-supported user behavior analytics for insider threat detection.

SecurityHQ offers a service for assisting with initial setup and the services of an expert team for assisting with incident analysis and remediation. Incident handling is part of the standard service support, but support services and documentation are available only in English. On-site support is available in North America, EMEA, and APAC but not Latin America.

Customers can use the service to outsource their SOC entirely or SecurityHQ SOC analysts are able to work as an extension of the internal SOC or security team. The offering includes regular risk assessment reporting but not assistance in developing security and governance policies. There is a dedicated analyst or team allocated to each customer and strategic continual improvement planning is included as standard.

SecurityHQ MDR supports organizations of all sizes but is best suited to medium and mid-market enterprises looking for a customizable and scalable MDR service that includes continual security recommendations from a vendor with a global presence.

Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

SecurityHQ

Table 15: SecurityHQ's rating

Strengths

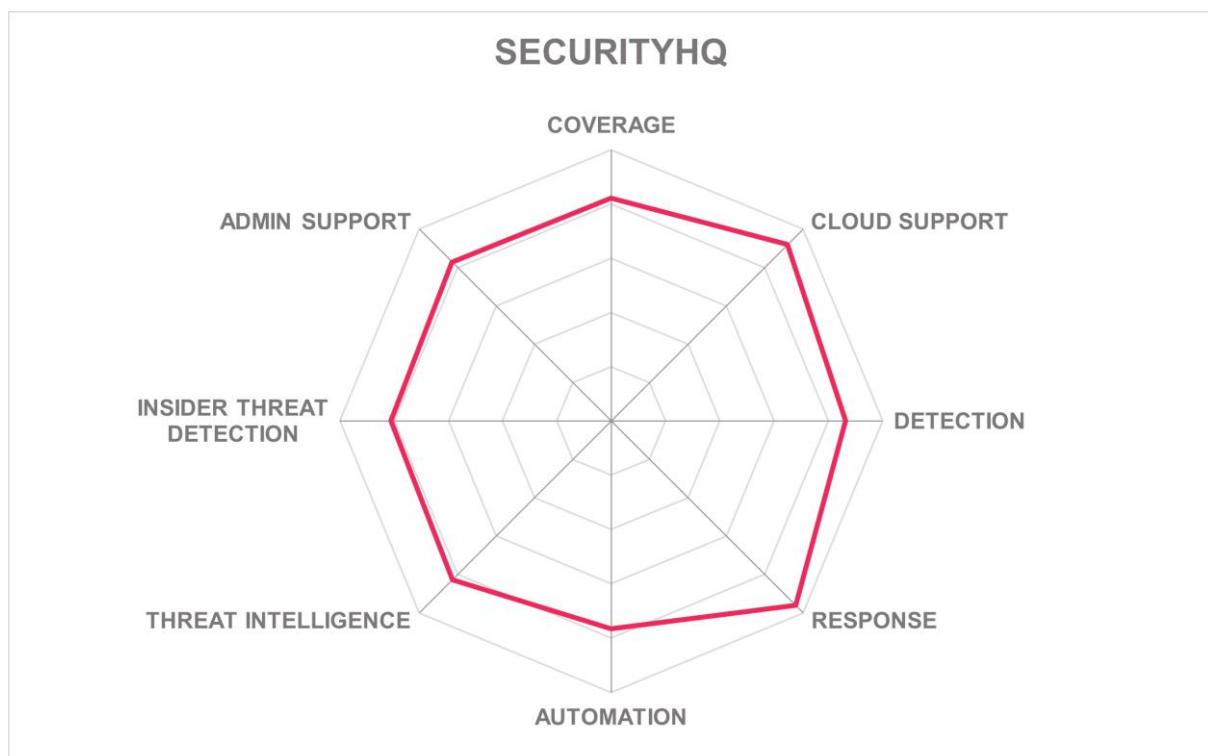
- Flexible, cloud-based deployment model.
- Fixed base price based on end users and log volumes with no hidden costs.
- Provision of a range of integrations with EPDR, NDR, and SIEM products.
- Comprehensive MDR coverage of cloud computing environments.
- Good detection and response capabilities across the entire IT estate.
- Strong automated response capabilities and post-remediation support.
- Modern user interface.
- SecurityHQ Response app to support cyber defenders wherever they are.
- Big data analytics to identify risk and enhance security posture.
- Service includes regular SecOps workshops.

- Good forensics support.
- Platform includes Asset Management which monitors if devices are reporting.
- Mobile app to support cyber defenders wherever they are.

Challenges

- Providing integrations with a wider range of third-party SOAR solutions would help customers get greater ROI from existing investments.
- Expanding the number of languages available for support services and documentation would help grow existing markets and potentially open up new ones.
- Adding assistance with developing security and governance policies would help customers requiring this kind of assistance.

Leader in



Sophos – Sophos MDR

Sophos is a private global cybersecurity company that was founded in 1985 and headquartered in Abingdon in the UK, with SOC analysts and Ops supporting teams centralized in hubs in the UK, US (Hawaii, Utah, and Indiana), India, and Australia. Most customers are based in North America, followed by EMEA, with the majority falling into the small and medium enterprise market segments.

Sophos provides MDR services in three packages: Sophos Threat Advisor, Sophos MDR, and Sophos MDR Complete, which includes full incident response services and a \$1M breach protection warranty. Licensing is on a per user, per year basis, taking into consideration the total number of users and servers (physical and virtual) in an organization. Deployment is mainly as a cloud-based service, with MDR services provided on top of the core Sophos SaaS platform. However, the XDR component is deployed as an agent on endpoints and services, and customers adding additional integrations to ingest non-Sophos security telemetry across endpoint, email, identity, network, public cloud, and firewall may require a virtual machine and virtual NDR appliance on-site to collect logs and capture packet data.

The solution covers most major operating systems, except Android, and all the main web browsers. It also provides round-the-clock monitoring and analysis of all major business IT systems and environments, including Edge computing environments as well as detection and response services across most environments, including industrial and medical IoT, and remote workers but excluding OT environments and mobile devices.

Sophos MDR comes with prebuilt integrations with 18 third-party EPDR products, only two NDR products (Darktrace and Sophos) with Vectra integration in development, no behavior analytics solutions, and only one third-party SIEM product (Microsoft Sentinel), although custom integrations for SIEM products are available using the Sophos open API.

The solution provides round-the-clock monitoring and analysis of cloud applications and cloud data stores, detection and response services across all cloud services and applications, and can identify data loss across cloud infrastructure. Sophos MDR also includes cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments.

The solution can detect threats across the entire IT estate, it can perform network-based detections including full packet capture and inspection, and detect a wide range of malicious activity, including ransomware and evasive malware. The solution also includes attacker behavior analytics.

In terms of response, Sophos MDR can respond automatically to disrupt threats, attack blocking capabilities include the disruption of malicious network communications and the suspension of accounts. The solution also includes post-remediation support to validate that a threat has been neutralized and verify that it has not resurfaced but does not support activity recording for forensic analysis.

The solution is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, quarantining files, and preventing registry changes but not carrying out sinkholing actions. The solution also provides its own SOAR functionality and comes with prebuilt integrations for only one SOAR solution (Sophos Factory). A global threat hunting

team supports the solution, which includes regular automated and manual threat hunting as well as regular reporting on the findings. There is also a dedicated team of threat experts in Germany to address unique local security needs. The solution does not include the application of data from many external threat intelligence sources, instead drawing on threat intelligence mainly gathered from the Sophos threat intelligence team, customer deployments, technology partners, and industry bodies. The solution uses only a single commercial threat intelligence feed, and no open-source feeds. There are also no connectors for third-party threat intelligence sources, but the Sophos open API can be used to enrich telemetry in the platform with data from AbuseIPDB.

Looking at insider threat detection, the solution is able to capture East-West traffic for those purposes. In addition to insider threats, it can detect and respond to phishing attacks and any abuse of privileged access, and includes user behavior analytics.

Sophos offers a service for assisting with initial setup and the services of an expert team for assisting in incident analysis and remediation. Basic incident handling is included in standard service support, but full incident response is available only in the MDR Complete service. All support services are remote with no on-site services.

Support services are available in 11 languages, including Chinese, Japanese, Brazilian Portuguese, Czech and Korean, while documentation is available in nine languages, excluding Russian, Arabic, Czech, and Polish.

Customers can use the service to outsource their SOC entirely or Sophos SOC analysts are able to work as an extension of the internal SOC or security team. The service includes regular risk assessment reporting and assistance in developing security policies but not in developing governance policies. There is a dedicated analyst team allocated to each customer, but the service does not include strategic, continual improvement planning.

Sophos MDR supports organizations of all sizes in all verticals looking for a flexible and comprehensive MDR service that can be tailored to specific requirements, includes its own SOAR and NDR capabilities, and is designed to work with all existing security tools to ingest telemetry and carry out response actions.

Security	Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

SOPHOS

Table 16: Sophos's rating

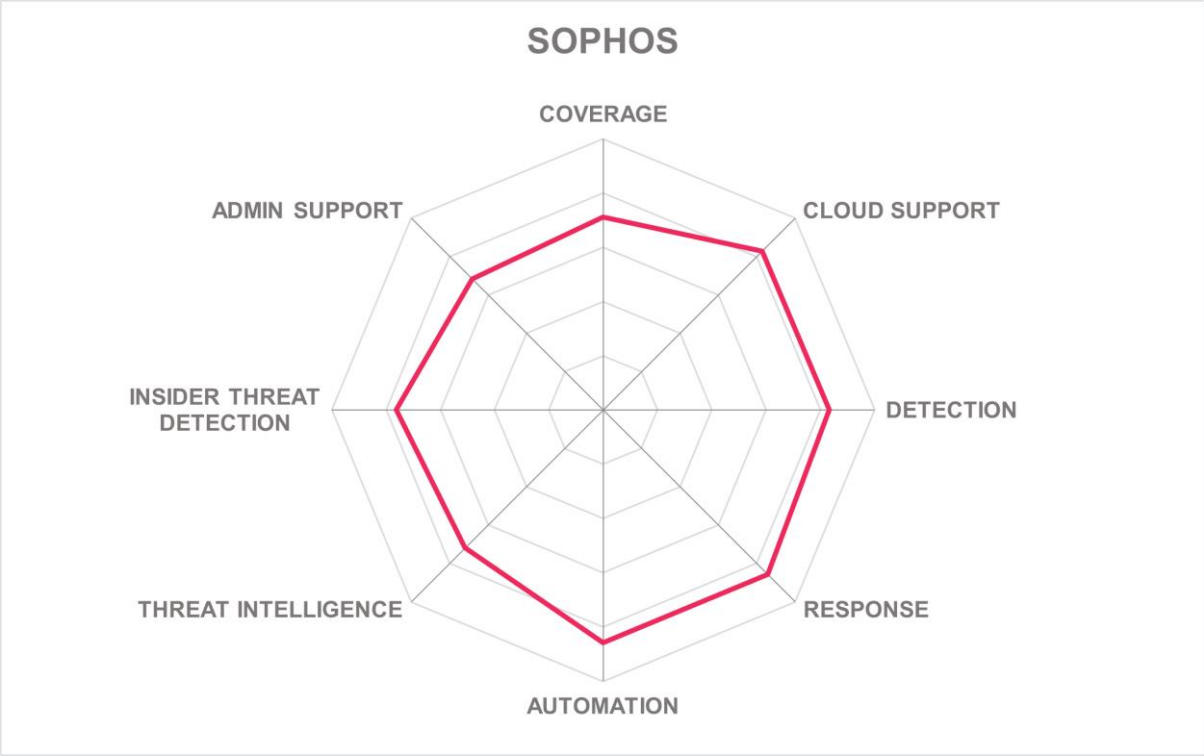
Strengths

- Simple licensing model based on number of users and servers.
- Flexible and fast cloud-based deployment.
- Wide, but not exhaustive MDR coverage of business IT environments.
- Good support for integrations with third-party EPDR products.
- Comprehensive MDR coverage of cloud computing environments.
- Strong threat detection capabilities.
- Modern user interface.
- Wide range of automated response and containment capabilities.
- Good threat hunting capabilities and support.
- Excellent language support for support services and documentation.
- Automated telemetry data ingestion, filtering, parsing, normalization, and correlation.

Challenges

- Extending MDR coverage to include OT, Android, and mobile devices would round out the offering to provide fully comprehensive coverage.
- Adding prebuilt integrations for third-party behavior analytics and more NDR and SIEM products would enable faster and wider ROI for customers on investments.
- Adding activity recording would strengthen the offering for customers looking for a strong forensic capability.
- Extending SOAR integrations would help customers get better ROI.
- A greater number of threat intelligence sources could boost customer confidence.
- Adding assistance in developing governance policies would complement the support for security policy development and risk assessments.
- Adding strategic, continual improvement planning would round out the service.
- Adding a mobile app for accessing MDR information on the go would give greater flexibility and assurances to customer security teams.

Leader in



Tata Communications – Managed Detection and Response

Tata Communications is a global public communication and digital services company providing a range of communication services, network services, cloud services, and cybersecurity services, including MDR. It was founded in 2002 and is headquartered in Mumbai, India, with SOCs in India (Pune and Chennai) and Dubai, plus 11 dedicated SOCs on customer premises. Most customers are in the APAC region, followed by EMEA, with the majority falling into the large enterprise market segment.

Tata Communications MDR is part of the company's threat management portfolio and combines several security platforms (SIEM, native SOAR, EDR, NDR, and UEBA). The service can be deployed as cloud only, on premises only, or in a hybrid model, in which case, on-premises elements include a virtual appliance and agents installed on the network for NDR and endpoints for EDR. There is a simple licensing model based on events per second (EPS), which can include EPS metrics derived from the number of log sources feeding into the service.

The service covers Windows and Linux but not Mac OS, Android, or iOS, while coverage includes all major browsers, except Safari. The service provides continuous monitoring and analysis of all major business IT environments and systems, including Edge computing environments, and provides detection and response services across several environments, including remote workers but not all on-premises applications, and excluding medical and industrial IoT, OT environments, and mobile devices.

Tata Communications MDR includes prebuilt integrations with four third-party EPDR products (CrowdStrike Falcon Endpoint Protection, Microsoft Defender for Endpoint, SentinelOne Singularity Platform, and TrendMicro), 22 NDR products, seven SIEM solutions, and 15 behavior analytics products, but custom integrations can be built for other third-party products if the necessary APIs are available.

There is good support for cloud computing, with the service providing continuous monitoring and analysis of cloud applications and cloud data stores, with detection and response capabilities across all cloud services and applications, and the ability to identify data loss across cloud infrastructure. Tata Communications MDR also includes cloud security posture management, cloud workload protection, and vulnerability scanning of customer multi-cloud environments.

Tata Communications MDR is able to detect threats across the entire customer IT estate, do network-based detections including full packet capture and inspection, and detect a wide range of malicious activity, including ransomware attacks but not evasive malware. The service includes attacker behavior analytics.

The service is able to disrupt threats automatically, while attack blocking capabilities include the disruption of malicious network communications and account suspensions. However, the service does not include post-remediation support to validate that a threat has been neutralized or verify that it has not resurfaced, nor does it support activity monitoring for forensic analysis.

Tata Communications MDR is able to execute predefined containment actions automatically, including terminating processes and network sessions, isolating hosts, blocking communications by port and IP, and quarantining files but not carrying out sinkholing actions or preventing registry changes. The service includes its own SOAR functionality with multiple playbooks to improve MTTR and has integrations for 21 third-party SOAR solutions, with custom integrations available.

The service includes the support of a dedicated threat hunting team, regular automated and manual threat hunting including retrospective threat hunting and regular reporting on the findings. The service applies threat intelligence from the company's threat intelligence team, NetFlow Data, customer deployments, honeypot environments, technology parties, industry bodies, two commercial threat intelligence feeds, and a large number of open-source intelligence feeds. Additionally, Tata Communications generates threat intelligence from the internet traffic visibility it has as a Tier one ISP as well as from deep and dark web monitoring. The service also includes connectors to five cyber threat intelligence sources.

The service is able to capture East-West traffic for insider threat detection, it can detect and respond to insider threats, phishing attacks, and abuse of privileged access. It also includes user behavior analytics.

Tata Communications offers a service for assistance with initial setup of the service and the services of an expert team for assisting with incident analysis and remediation. Incident handling is provided as part of standard service support, but support services and documentation is available only in English. On-site support is available only in the APAC region.

Customers can use the service to outsource their SOC entirely or SOC analysts from Tata Communications can work as an extension of the internal SOC or security team. The service includes regular risk assessment reporting but does not include assistance in developing security and governance policies. There is a dedicated analyst or team allocated to each customer, and continual strategic and security improvement planning is included as part of the standard subscription.

The Tata Communications MDR service is suitable for organizations of all sizes, particularly those with specific regulatory compliance requirements such as those in financial services, healthcare, and auto manufacturing, who are looking for a wide ranging MDR capability that is easy to use, has a high degree of interoperability for ROI purposes, has a good range of insider threat detection, and has strong support for cloud computing.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

TATA COMMUNICATIONS

Table 17: Tata's rating

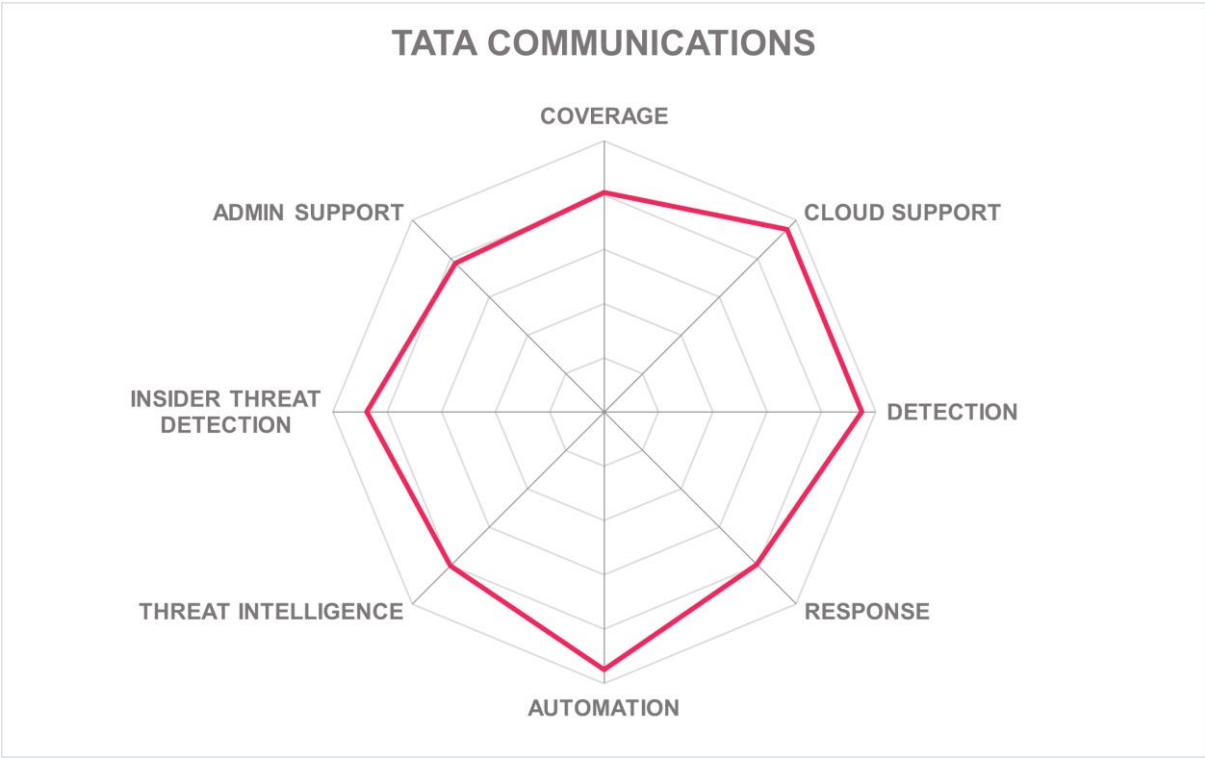
Strengths

- Simple licensing model.
- Onboarding within 15 days.
- Flexible deployment options available to suit customer requirements.
- Interoperable with a wide range of third-party security products.
- Strong MDR coverage of cloud computing environments.
- Good range of detection and response capabilities.
- Maps threats to MITRE ATT&CK framework.
- Wide range of automated response capabilities.
- Built in SOAR functionality as well as a wide range of SOAR integrations.
- Strong threat intelligence, data analytics, and threat hunting capability.
- Wide range of insider threat detection capabilities.
- A good range of support for customer admins.

Challenges

- Greater flexibility in deployment options could grow existing markets and open up new ones.
- Expanding coverage to a wider range of operating systems would support a greater number of potential customers.
- Expanding MDR coverage to include all on-premises applications, IoT, OT, and mobile devices would strengthen the offering.
- Adding post-remediation support to validate a threat has been neutralized and verifying that it has not resurfaced would strengthen the offering.
- Adding activity recording would help customers conduct forensic analysis of incidents.
- Providing support services and documentation in more languages could help grow existing markets and open up new ones.
- Adding assistance in developing security and governance policies would complement the risk assessment reporting and increase the value of the service to customers.
- No mobile app available yet, but this is on the roadmap.

Leader in



Xcitium – Xcitium Managed (MDR) - Xcitium Complete (XDR)

Xcitium is a privately held, US-based provider of cybersecurity solutions based on technologies under development since 2018, originally by Comodo Security Solutions, which rebranded in 2022. Xcitium is headquartered in Bloomfield, New York and has a global virtual SOC with team members located in the US, India, and Pakistan. Most of Xcitium's customers are located in North America, followed by EMEA, with the majority falling into the medium enterprise market segment.

Xcitium services are sold internationally through direct sales, value added distributors (VADs), technology solutions brokers (TSBs), and MSPs/MSSPs, and licensing is on a per endpoint, per year basis. Xcitium offers four service packages: Advanced, Guided, Managed, and Complete. Advanced is focused on endpoint protection, detection, and response. Guided is an MDR "light" service, which provides high-fidelity alerting. Managed is a full 24x7x365 MDR service, including no-cost incident response. Complete is MDR plus XDR based on Xcitium's network/cloud sensor technology.

Xcitium's MDR services are deployed as cloud services but with endpoint agents on premises. There is also a network sensor (on-premises or cloud-based) for customers subscribing to Xcitium Complete, which includes XDR. This is capable of network anomaly collection as well as third-party party log collection.

Xcitium MDR covers all operating systems and browsers, and provides continuous monitoring and analysis of all major IT environments and systems, including Edge computing environments. It also provides detection and response services across most environments, including mobile devices and remote workers, but excluding proprietary medical and industrial IoT, and OT environments.

The service does not include prebuilt integrations with any third-party EPDR, NDR, SIEM, or behavior analytics products, but most of these technologies are built in.

The service includes continual monitoring and analysis of cloud applications and cloud data stores, provides detection and response services across all cloud services and applications, and can detect data loss across cloud infrastructure. However, it does not include cloud security posture management, cloud workload protection, or vulnerability scanning of customer multi-cloud environments.

Xcitium MDR is able to detect threats across the entire IT estate, do network-based detections including full packet capture and inspection and detect a wide range of malicious activity, including ransomware and evasive malware. The service also includes attacker behavior analytics and Xcitium's patented ZeroDwell Containment technology which isolates unknown files and suspicious code while allowing it to execute in a virtualized environment to identify if they are malicious and prevent any impact to the production environment of the endpoint.

The service is able to respond automatically to disrupt threats, while attack blocking capabilities include the disruption of malicious network communications and account suspension. The service includes post-remediation support to validate that a threat has been

neutralized and verify that it has not resurfaced, but it does not support activity recording for forensic analysis. However, Xcitium's MDR service has the ability to collect endpoint telemetry continuously as well as collect forensic artifacts to conduct investigations using advanced digital forensic techniques and timeline analysis.

Xcitium MDR is able to execute predefined containment actions automatically, including terminating processes and network connections, isolating hosts, blocking communications by port and IP, quarantining files, and preventing registry changes but does not include sinkholing. The solution does not come with any prebuilt integrations with third-party SOAR solutions.

The service includes the support of a dedicated threat hunting team, includes regular automated and manual threat hunting activities as well as regular reporting on threat hunting findings. The service applies threat data from external sources, including Xcitium's threat intelligence team, customer deployments, technology partners, industry bodies, and a large number of open-source threat intelligence feeds but no commercial feeds. Connectors are provided only for Xcitium Verdict Cloud but no third-party intelligence sources.

Xcitium MDR is able to capture East-West traffic for insider threat detection, and can detect and respond to insider threats, phishing attacks, and abuse of privileged access. However, it does not include user behavior analytics.

Xcitium offers a service for initial setup via its Professional Services division and the services of an expert team for assisting with incident analysts and remediation via its Managed XDR service offering. Incident response is provided as part of standard service support, but remote support services are available only in English, Chinese, and Russian, while documentation is available only in English. However, the user interface is supported in 17 languages. On-site support is not available in any region.

Customers can use the service to outsource their SOC entirely or Xcitium SOC analysts are able to work as an extension of the internal SOC or security team. The service includes regular risk assessment reporting, and assistance in developing security and governance policies. There is also a dedicated analyst team allocated to each customer and strategic, continual improvement planning is included in the standard subscription.

Xcitium is suitable for companies of all sizes looking for a wide range of flexible and comprehensive MDR services to suit their particular support requirements.

Security	Neutral
Functionality	Positive
Deployment	Strong Positive
Interoperability	Weak
Usability	Positive



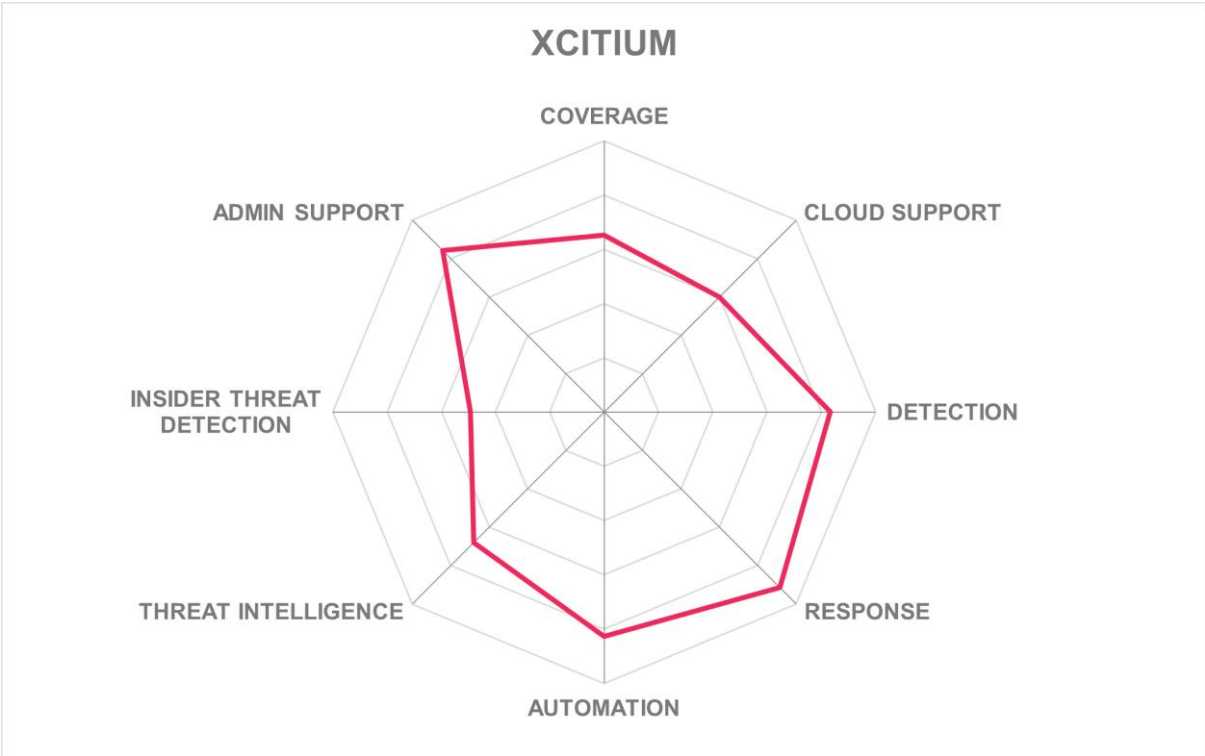
Table 18: Xcitium's rating

Strengths

- Good basic coverage of cloud computing environments.
- Wide range of threat detection and response capabilities.
- A good range of automated response and containment capabilities.
- A large number of open-source threat intelligence sources.
- Zero Dwell Containment technology for determining if unknown files are malware.
- Includes unlimited incident response.
- Xcitium Verdict Cloud for recording all unknown files found to be malicious.
- Strong threat hunting capability.
- Malware mapping to MITRE ATT&CK framework.
- Heat map of all EDR rules that have been triggered across IT estate.
- Wide range of language support for the user interface.
- Strong support for customer admin, SOC, and security teams.
- Licenses include patch management and vulnerability management at no extra cost.

Challenges

- Expanding coverage to OT and IoT environments could grow existing markets and open up new ones, especially in manufacturing and healthcare sectors.
- Including prebuilt integrations with third-party EPDR, NDR, SIEM, SOAR, and behavior analytics products would enable greater ROI for customers on investments.
- Including cloud security posture management, workload protection, and multi-cloud scanning will help assure customers that rely heavily on cloud computing services.
- Adding activity recording would help customers conduct forensic analysis of incidents.
- Making support services and documentation available in more languages would help to grow existing markets and open up new ones.
- Adding a mobile app for accessing MDR information on the go would give greater flexibility and assurances to customer security teams.



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors may not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment, or maybe a fast-growing startup that may be a strong competitor in the future. Other companies listed here are considered MDR vendors but did not participate in this report.

Accenture – A multinational professional services firm that provides consulting, technology, and outsourcing services to businesses and organizations around the world. The company was founded in 1989, is listed on the New York Stock Exchange, and is headquartered in Dublin, Ireland, with offices and operations in more than 50 countries.

Why worth watching: Accenture has a Managed Extended Detection and Response capability that covers the detection, response to, and remediation of both IT and OT threats, supported by an AI-supported, cloud-based, global platform and dedicated expert cybersecurity teams.

Alert Logic – Founded in 2002 and headquartered in Houston, Texas, Alert Logic provides cloud-native MDR solutions. Alert Logic was acquired by Fortra (formerly HelpSystems) in April 2022 as part of a strategic shift toward providing global customers with a single source of cyber defense solutions.

Why worth watching: Alert Logic has team members and channel partners worldwide, is now part of Fortra, and Alert Logic MDR provides comprehensive 24x7 attack surface coverage across public cloud, SaaS, on-premises, and hybrid environments with embedded SOAR and automated response capabilities, globally distributed SOCs, personalized support, and a 15-minute SLA.

Atos – A French multinational IT services and consulting company founded in 1997 and headquartered in Bezons, France. Atos provides a range of managed security services, including MDR, SOC, and CERT Services.

Why worth watching: Atos MDR provides threat intelligence, threat hunting, 24x7 security monitoring, incident analysis, and incident response. Atos MDR is supported by edge computing; advanced security analytics on endpoints, user behavior, applications, and the network; 16 SOCs and more than 6,000 security analysts worldwide; and ML and other AI technologies to investigate, automatically contain threats, and orchestrate the response.

Binary Defense – An American managed security solution provider (MSSP) founded in 2014 and headquartered in Stow, Ohio, offering a range of services, including SOC-as-a-Service (SOCaaS) and Managed Detection and Response (MDR).

Why worth watching: Binary Defense SOCaaS combines best of breed security with a security team that works as an extension of customer teams to shield the business from cyber-attacks 24x7, with personalized service and customized escalation procedures. Binary Defense MDR uses a human driven, technology-assisted approach to fill security gaps, proactively identify threats, investigate alerts, and recommend remediation steps.

Bitdefender – A cybersecurity solutions company founded in 2001 in Romania, with Romanian headquarters in Bucharest and US headquarters in Santa Clara, California. Bitdefender also has offices in Canada, UK, France, Germany, Spain, Denmark, Italy, Sweden, Netherlands, UAE, and Australia.

Why worth watching: Bitdefender is continually innovating with 440 patents for core technologies. Bitdefender's Managed Detection and Response service provides customers

with 24x7 access to cybersecurity experts and is backed by Bitdefender's GravityZone and eXtended Detection & Response technologies, threat hunting teams, threat intelligence analytics, automated response capabilities, and a SOC with security analysts from global intelligence agencies. The service includes brand and IP protection. Bitdefender also offers a specialized MDR service for MSPs.

BlackBerry – A Canadian multinational company founded in 1984 and headquartered in Waterloo, Ontario, which initially focused on pagers and smartphones but now specializes in enterprise software and services, including security.

Why worth watching: BlackBerry has a long history of providing security mobile devices and continues to innovate to help organizations improve security. BlackBerry CylanceGUARD is a 24x7 Managed Extended Detection and Response service that integrates with other BlackBerry security products, provides 24x7 monitoring and automated response, correlates telemetry across devices, provides actionable intelligence and multi-regional compliance support, and is backed by an AI-enhanced analytics platform and an expert analyst team.

BT Global Services – A division of the publicly listed multinational telecommunications holding company BT (formerly British Telecom) established as a private company in 1984 and headquartered in London. BT Global Services provides security, cloud, and networking services to corporate and government customers around the world.

Why worth watching: BT Global Services was formed in 2002 and is a leading global provider of managed security services, including Extended Detection and Response (XDR) designed to provide optimized threat detection and response through deeper, richer telemetry of critical business applications across cloud, end user, and OT environments. BT Global Managed XDR solution follows a co-managed approach to strengthen existing defenses, particularly Microsoft security controls. It is supported by global experience, best of breed technology, ML-supported threat detection, and 24x7 monitoring by security experts.

VMware Carbon Black – An American cybersecurity company headquartered in Waltham, Massachusetts, founded in 2002, and acquired by VMWare in 2019.

Why worth watching: VMware Carbon Black Managed Detection and Response provides critical insight into attacks using ML to prioritize alerts and uncover new threats. The service is supported by a team of security experts that monitors threats 24x7 in the VMWare Carbon Black Cloud and provides rapid response, threat containment, actionable alerts, and remediation recommendations. Service also includes reports on threats, security trends, activity summaries, and strategic priorities as well as security policy recommendations.

Check Point – Founded in 1993 and headquartered in Tel Aviv, Israel, Check Point is a multinational cybersecurity company that provides software and hardware products for network security, endpoint security, cloud security, and threat intelligence, including MDR through Horizon MDR/MPR.

Why worth watching: Horizon MDR/MPR is designed to take MDR to the next level by focusing on prevention as well as detection. The service is supported by AI technologies, Check Point research, and the Check Point ThreatCloud real-time threat intelligence. The service is designed to provide continual updates, automated prevention actions, optimal configurations, recommendations, and best practices to improve defenses. The service provides 24x7 monitoring of all IT infrastructure and is designed to proactively prevent, monitor, detect, investigate, hunt, respond to, and remediate cyber-attacks.

Cisco – A US-based multinational technology company founded in 1984 and headquartered in San Jose, California, that designs, develops, and sells networking hardware, telecommunications equipment, and other high technology services and products. Cisco's MDR offering is called Cisco SecureX Managed Detection and Response (MDR).

Why worth watching: Cisco SecureX is a cloud-native, security platform that is integrated with other Cisco security solutions and third-party security tools to provide comprehensive

security capabilities using automation, customizable playbooks, and advanced technologies such as ML and behavioral analytics to detect and respond to threats in real time.

Claranet - A private European network, hosting, and managed services company founded in 1996 and headquartered in London UK, with 24 offices across Europe, US, and Brazil.

Claranet offers Managed Detection and Response as part of its Managed Security Services.

Why worth watching: Strong EU presence and designed to combine the knowledge of a multidisciplinary and dedicated global Security Operations Center (SOC), best-in-class threat intelligence, AI-led analysis, proactive threat hunting, and Security Information and Event Monitoring (SIEM) capabilities to provide round-the-clock threat analysis and continual security optimization across on-premises and cloud IT environments.

Clone Systems - A privately owned global managed security service provider (MSSP) founded in 1998 and headquartered in Philadelphia with additional offices in Greece. They offer a range of customizable services including SOCaaS, MDR, and XDR.

Why worth watching: Clone Systems SOCaaS offering monitors security threats across on-premises and cloud environments, including SaaS applications and endpoints, to detect emerging and evolving threats with continually updated threat intelligence. It also provides automated response and remediation. The MDR offering provides 24x7 proactive security monitoring for detection of, response to, and recovery from cyber-attacks supported by consolidated security visibility across on-premises and cloud IT environments, and compromise and behavior analytics.

ConnectWise – An American software and services company founded in 1982 and headquartered in Tampa, Florida that focuses on providing solutions for managed service providers, IT solution providers, and value-added resellers to make enterprise level security consumable for SMBs.

Why worth watching: ConnectWise is focused on partnership, innovation, and software security, and solutions are backed by its Asio unified platform, which is designed to deliver scalability, intelligent automation, and value-added reporting and insights using open APIs. ConnectWise MDR includes next-generation endpoint security, AI-powered monitoring, automated remediation, SOC services for 24x7 monitoring and response, and best-in-class EDR solutions.

Critical Start – Critical Start is a private US cybersecurity company founded in 2012 and based in Plano, Texas with offices in 16 other US cities. Critical Start provides a range of cybersecurity solutions and services, including MDR services and Cyber Incident Response Team (CIRT) services.

Why worth watching: Critical Start claims an immediate reduction of 90% in false positives, MDR services are tailored to meet individual needs and are supported by Critical Start's Zero-Trust Analytics Platform and 1Trusted Behavior Registry, a customer success manager, and a 24x7 US-based SOC that provides real-time monitoring, rapid investigation and response, and continual threat hunting. Critical Start also offers a mobile app that enables customers to triage and respond to incidents on the go.

CrowdStrike – A public American cybersecurity company founded in 2011 and headquartered in Sunnyvale, California, with offices in Europe, Asia, and Australia.

CrowdStrike's MDR offering is called Falcon Complete.

Why worth watching: Falcon Complete, based on the cloud-native Falcon Platform, combines ML and other AI technologies with 24x7 monitoring, behavioral analysis, global threat intelligence and support from CrowdStrike's security analysts threat hunters. It can analyze millions of endpoint events in real time to identify threats very quickly and respond automatically. Falcon Complete also provides configuration management based on best practices, covers all major cloud service providers, and provides coverage for container environments.

CyberArm – A cybersecurity services company founded in 2016 and headquartered in Beirut, Lebanon, focusing on the Middle East and North Africa, with additional offices in Portugal and Saudi Arabia. CyberArm provides a range of complementary security services, including Managed Security.

Why worth watching: CyberArm follows a client-centric, partnership approach, with services and solution recommendations based on objective metrics to achieve affordable and tailored cybersecurity for any size of organization. CyberArm's SOC 2 Type 2 Managed Security service is supported by leading SOC technology and is designed to protect critical assets, monitor for intrusions, and respond to incidents 24x7.

CyberMaxx – A global IT software solutions and services provider founded in 2002 and is headquartered in Nashville, Tennessee. CyberMaxx offers a wide range of cybersecurity services, including MDR.

Why worth watching: CyberMaxx MDR services provide a turnkey, tailor-made, "white glove" solution for quick implementation of a round-the-clock security operations center (SOC). Maxx MDR combines the company's security information and event management (SIEM), network intrusion and detection, and endpoint detection and response (EDR) capabilities to give customers the ability to detect, analyze, investigate, and actively respond to threats. The solution is available in managed and co-managed deployment models, and includes a proprietary cloud-native analytics platform for better integration with SaaS and IaaS.

Cyrebro – An Israeli cybersecurity firm (formerly known as Cyberhat) founded in 2013 and based in Tel Aviv with offices in New York City in the US and Toronto in Canada, a second R&D center in Ukraine, and a new site in Costa Rica. The company offers a technology agnostic SOC platform called Cyrebro to maximize the benefits of existing security tools.

Why worth watching: The AI-supported Cyrebro platform, launched in 2020, is designed to provide enterprise level real-time detection, risk analysis, and remediation of security threats. The Cyrebro platform is the basis for a complete SOC solution that includes proactive detection through threat intelligence and threat hunting, MDR with forensic investigation and incident response capabilities, and support for security operations with strategic monitoring and SIEM optimization.

inSOC – A dedicated SOCaaS provider founded in 2019 and headquartered in Los Angeles, California with another office in Edinburgh, UK. inSOC services are available only through channel partners and cybersecurity consulting partners.

Why worth watching: inSOC's One Stop SOC offers to MSPs and MSSPs SOC services backed by an enterprise level, multi-tenant, AI-driven breach detection platform that is powered by the Starlight security analytics from Stellar Cyber and vulnerability scanning from Rapid7. One Stop SOC follows a policy and security framework-based approach and is available in three service levels to cater for all sizes of business, including SMBs looking for enterprise grade security.

Open Systems - Founded in 1990 and headquartered in Zurich, Switzerland, Open Systems has with two business units: Ontinue, the MDR division and Open Systems, the SASE division.

Why worth watching: Ontinue ION is a risk-based Managed Extended Detection & Response (MXDR) service that provides round-the-clock SecOps to accelerate organizations' response to incidents and continually reduce risk. Ontinue ION is based on a cloud-delivered SecOps platform, is supported by AI driven automation, and is specifically designed to use organizations' existing Microsoft security and collaboration stack, including MS Sentinel, the MS Defender Suite, and MS Teams. Ontinue also offers add-op services for Managed Vulnerability Mitigation and IoT Security.

Rapid7- A public global cybersecurity solutions provider founded in 2000 and based in Boston, Massachusetts, with offices across the US and in Canada and Australia supporting customers in 144 countries.

Why worth watching: Rapid7 Managed Threat Complete provides MDR that combines XDR technology, internal and external threat intelligence, forensics tools, and threat hunting, featuring a dedicated security advisor and unlimited data collection, vulnerability management, and digital forensics and incident response (DFIR).

Secureworks - A US cybersecurity company founded in 1999 and based in Atlanta, Georgia, with SOC's in the US, UK, and Japan. Secureworks meets market demand for SOCaaS functionality via its Managed Detection and Response (MDR) offering, which combines SaaS XDR with threat hunting and incident response.

Why worth watching: Secureworks has a strong threat intelligence unit that uses insights from more than 1,500 incident response engagements annually.

SilverSky – A mature Managed Detection and Response (MDR) company founded in 1997 and headquartered in Raleigh, North Carolina, with SOC's in Raleigh, Belfast in Northern Ireland, and Manila in the Philippines.

Why worth watching: SilverSky's three SOC's support companies of all sizes and security maturity in North America, South America, Europe, and the Asia Pacific region. A range of services are based on SilverSky's cloud-native, multi-tenant MDR platform, which is supported by military grade behavioral tracking and machine learning in combination with human analysis and support. SilverSky's MDR offering is designed to provide complete visibility into the endpoint security environment with full context and real-time forensics, plus 24x7 SOC support, automated threat containment. SilverSky offers a range of other integrated security services, including Managed SIEM, Extended Detection and Response, and Security Consulting Services.

Trend Micro – A multinational cybersecurity company that was founded in 1988 and headquartered in Tokyo, Japan. Trend Micro is a leading provider of cybersecurity solutions, serving a wide range of industries and organizations worldwide. Trend Micro's MDR solution is called Managed XDR.

Why worth watching: Trend Micro's Managed XDR offers 24/7 analysis and monitoring. Email, endpoint, server, cloud, workload, and network sources are correlated for stronger detection and greater insight into targeted attack source and spread. Detection, investigation, and threat hunting are optimized by security analytics and enriched by Trend Micro's threat research.

Trustwave - A global cybersecurity and managed security services company that is an independent subsidiary of multinational telecommunications company Singtel Optus group. Trustwave was founded in 1995, is headquartered in Chicago, Illinois in the US, and provides a range of cybersecurity services, including MDR.

Why worth watching: Trustwave MDR combines security engineers, incident response teams, Trustwave threat intelligence, and its XDR platform Trustwave Fusion, which improves visibility by collecting telemetry from customers' existing security tools and infrastructure, thereby maximizing the return on investment. Trustwave MDR specializes in connecting hybrid multi-cloud operations and is supported by a cyber success team.

Verizon Business – A division of Verizon Communications founded in 2000, Verizon Business was formed in 2006, is headquartered in Basking Ridge, New Jersey, and provides enterprise-level solutions to businesses of all sizes, including managed security, networking, communication solutions, and professional and consulting services.

Why worth watching: Managed Detection and Response from Verizon Business is a security service that combines advanced technologies and human expertise to identify and respond

to security incidents quickly. It is supported by a vast global repository of threat intelligence and dedicated threat hunters.

WithSecure – Formerly F-Secure Business founded in 1988, WithSecure is headquartered in Helsinki, Finland, and is one of the first companies formed specifically to help customers prevent malware. WithSecure’s MDR service is called Countercept Managed Detection and Response.

Why worth watching: Backed by a proprietary Endpoint Detection and Response agent, log collectors, and a dedicated Detection and Response Team, Countercept 24x7 MDR is designed to remediate incidents before they impact the business and act as an extension of the internal team, sharing proactive threat hunting expertise and helping internal teams to learn and grow to improve security. Europe-only Countercept MDR option available.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn’t provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e., a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logical and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly, and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength is an important factor for customers when making decisions, even though KuppingerCole doesn't consider size to be a value by itself. In general, publicly available financial information is an important factor in customer decision-making processes. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are:

Strong positive	Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.
Positive	Strong support for a feature area or strong position of the company but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network but a rather small number of partners.
Neutral	Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.
Weak	Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.
Critical	Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is to provide a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in the chapter on Vendors to Watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

[Leadership Compass: Endpoint Protection, Detection & Response](#)

[Leadership Compass: Network Detection & Response \(NDR\)](#)

[Market Compass: Security Operations Center as a Service \(SOCaaS\)](#)

[Market Compass: Cybersecurity for Industrial Control Systems](#)

[Buyer's Compass: Security Operations Center as a Service \(SOCaaS\)](#)

[Leadership Brief: Do I Need Endpoint Detection & Response \(EDR\)?](#)

[Leadership Brief: The Differences Between Endpoint Protection \(EPP\) and Endpoint Detection & Response \(EDR\)](#)

Copyright

©2023 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.