

# Managed Detection & Response (MDR)

Warwick Ashford

December 4, 2024



LEADERSHIP  
COMPASS  
2024

This KuppingerCole Leadership Compass provides an overview of the Managed Detection and Response (MDR) market. It examines solutions that detect, analyze, investigate, and respond to cybersecurity threats quickly and efficiently, including Security Operations Center as a Service (SOCaaS) solutions and Managed eXtended Detection and Response (MXDR) solutions. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to detect, analyze, mitigate, and respond to cybersecurity threats.

## Contents

Executive Summary .....	4
Key Findings.....	6
Market Analysis .....	7
Market Size and Segmentation.....	9
Delivery Models.....	9
Required Capabilities .....	10
Leadership .....	12
Overall Leadership .....	12
Product Leadership .....	14
Innovation Leadership .....	16
Market Leadership.....	18
Products and Vendors at a Glance.....	20
Product/Vendor evaluation.....	22
Spider graphs.....	22
Adlumin – Adlumin Managed Detection and Response .....	23
Arctic Wolf – Arctic Wolf Managed Detection and Response (MDR).....	27
Check Point – Infinity MDR.....	31
CrowdStrike – Falcon Complete Next-Gen MDR .....	35
CYREBRO – CYREBRO .....	39
eSentire – eSentire Managed Detection and Response (MDR) .....	43
ESET – ESET PROTECT MDR.....	47
Fortra – Alert Logic Managed Detection and Response.....	51
Kroll – Kroll Responder.....	55
Ontinue – ION Managed Extended Detection and Response (MXDR).....	59
Optiv – Optiv MDR.....	64
Proficio – ProSOC MDR .....	68
ReliaQuest – ReliaQuest GreyMatter .....	72

Sophos – Sophos MDR .....	76
Tata Communications – Managed Detection and Response (MDR) .....	80
ThreatLocker – Cyber Hero MDR .....	84
Uptycs – Uptycs MDR .....	88
Vendors to Watch .....	92
Barracuda Networks .....	92
Cybereason .....	92
Expel .....	92
ForeNova Technologies .....	93
Fortinet .....	93
IBM Security .....	93
Red Canary .....	93
SentinelOne .....	94
SecurityHQ .....	94
WithSecure .....	94
Xcitium .....	94

## Executive Summary

Cybercriminals and state-sponsored espionage groups are constantly targeting organizations, subjecting them to relentless cyberattacks, making it more important than ever for organizations to be able to detect and respond to cyber threats 24/7. However, a global lack of cybersecurity skills means that many organizations cannot keep pace with these threats, and their security teams are often overwhelmed by the number of security alerts being generated by a multitude of disparate security systems.

This challenge is fueling the rapid growth of a broad managed detection and response (MDR) market, which includes Security Operations Center as a Service (SOCaaS) solutions and Managed eXtended Detection and Response (MXDR) solutions. The MDR market is experiencing significant growth and becoming more relevant in the cybersecurity industry, driven by regulatory compliance, digital transformation, the shift to remote working, the lack of cybersecurity skills, and the increasing sophistication of cyber threats, including ransomware, phishing attacks, and supply chain compromises.

MDR solutions involve managing an array of cybersecurity technologies typically through an integrated platform that offers advanced detection and response capabilities with the support of an expert team of analysts. Organizations of all sizes and types are adopting these solutions to either outsource security operations or supplement in-house security teams, especially during out-of-office hours and to fill expertise gaps. MDR service providers are increasingly supporting easy collaboration with in-house security teams of larger customers with high levels of cybersecurity maturity.

MDR solutions provide comprehensive cybersecurity with 24/7 expert monitoring, threat analysis, and support, going beyond the traditional compliance focus of Managed Security Service Providers (MSSPs). Unlike MSSPs, MDR services typically incorporate advanced technology like Artificial Intelligence (AI), Machine Learning (ML), active threat hunting, incident response, and thorough threat verification. This proactive approach, combined with a broader service scope, delivers a higher level of security expertise, making MDR a more robust option for organizations seeking advanced threat detection and containment.

Organizations of all sizes face similar cyber threats and require advanced detection and response capabilities. However, smaller organizations often lack the budget or expertise, and all organizations struggle to fill critical cybersecurity roles. MDR services allow even small businesses to access a dedicated team of experts available 24/7 to detect and respond to security incidents. These services also offer guidance on security investments, strategies, and processes, all without the financial and logistical challenges of building and maintaining an in-house cybersecurity team.

When organizations lack strong in-house threat detection and response capabilities, MDR solutions provide an opportunity to outsource a significant portion of their security operations. This includes managing networks, endpoints, applications, websites, databases, and security logs. Many MDR providers also offer the option to fully outsource the Security Operations Center (SOC) for organizations unable to act on security recommendations or

handle threats autonomously. Moreover, MDR services increasingly incorporate automated response features for faster threat mitigation.

For organizations that have some security measures in place, MDR can provide supplemental support as needed. This ensures that they have all the necessary cybersecurity skills and resources to handle high-risk threats and critical incidents. This support is especially valuable for large organizations, which frequently face numerous cyberattacks and struggle with a shortage of skilled professionals. MDR helps bridge these gaps, enabling organizations to manage day-to-day threats effectively while developing long-term security strategies.

Large organizations with existing security teams often struggle to manage complex systems like Security Information and Event Management (SIEM); Network Detection and Response (NDR); Endpoint Protection Detection and Response (EPDR); Security Orchestration, Automation, and Response (SOAR); and Identity and Access Management (IAM). As a result, they are relying increasingly on MDR providers not only for assistance in managing these systems but also for quick, automated responses to common threats. The demand for MDR services is growing as cyber threats continue to rise, making it difficult for organizations to maintain an in-house SOC and consistently deliver high-quality service.

The main aims of MDR are to:

- Strengthen customers' ability to monitor, detect, and respond to security threats 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
- Provide tools and expertise to deliver or augment existing security systems such as EPDR, SOAR, SIEM, and eXtended Detection and Response (XDR)

MDR solutions typically help customer organizations to:

- Deal with high volumes of security alerts
- Reduce the time that it takes to identify and mitigate security incidents
- Apply advanced analytics to threats and user behavior
- Rationalize, update, and integrate/coordinate security tools
- Bridge skills gaps
- Improve visibility and governance of the business IT environment

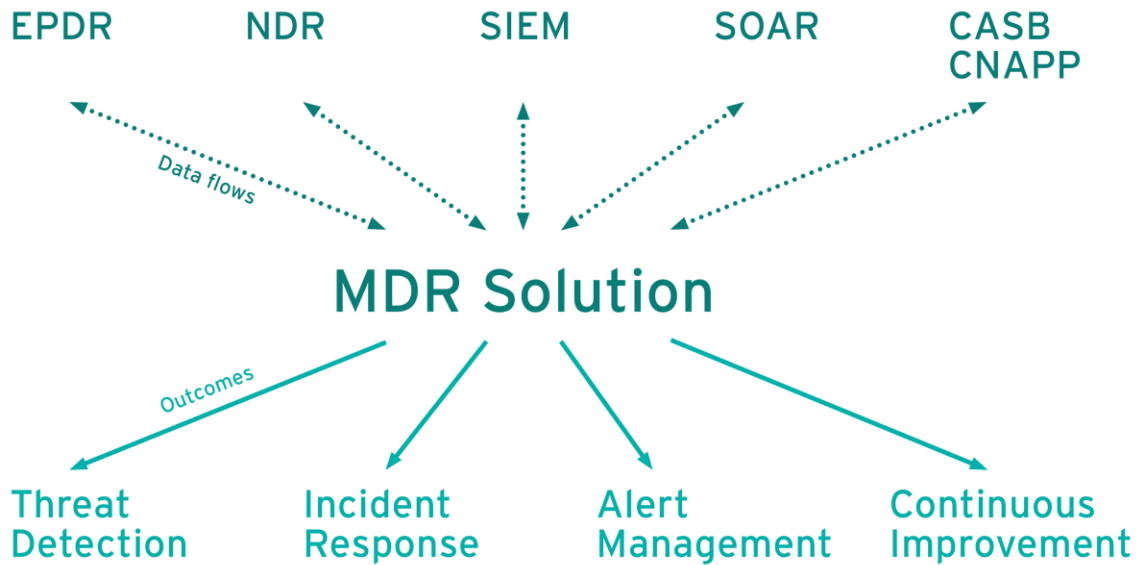


Figure 1: Cybersecurity ecosystem flowchart

This Leadership Compass is designed as a tool to help organizations to identify their requirements and map them to the capabilities offered by specific vendors, taking into consideration the size, growth, skills, and budget of the customer organization. To better understand the fundamental principles this report is based on, please refer to the [KuppingerCole Leadership Compass Methodology](#).

## Key Findings

- Increasing cyber threats, alert overload, and the worldwide shortage of cybersecurity skills are among the top drivers for the ongoing evolution and growth of MDR market.
- MDR solutions include a wide range of cybersecurity services, ranging from simple alert triage or SOCaaS to full MDR, including incident response.
- A key element of MDR is the focus on continual improvement of cybersecurity posture, going beyond traditional services from MSSPs.
- MDR solutions that cater for all sizes of organizations provide the opportunity for even small companies to get the benefit of enterprise-level SOCs.
- Most MDR solutions now meet a range of use cases from assistance of in-house SOCs and security teams to full outsourcing of security operations.
- MDR solutions typically help organizations to fill skills gaps, maintain round-the-clock monitoring of IT assets, and deal with large volumes of alerts across increasingly complex business IT environments.
- There is a concerted effort by MDR providers to focus on risk prevention and risk management.
- MDR solution adoption has increased as organizations realize technology alone cannot fully protect against cyber threats.
- KuppingerCole Analysts project the market to grow to \$7.9B by 2027.

- Security breaches, regulatory demands, mergers and acquisitions, requirements by insurers for cybersecurity coverage, and board mandates for cybersecurity reporting are the top drivers of MDR adoption.
- MDR is the only way many organizations are able to consolidate all of their security threats, tools, and systems into a single point of control.
- The Overall Leaders in MDR (in alphabetical order): Arctic Wolf, CrowdStrike, eSentire, Kroll, Proficio, ReliaQuest, and Sophos.

## Market Analysis

The adoption of MDR solutions has increased as organizations recognize that no amount of technology investment can guarantee complete protection against threats. Moreover, the growing complexity and volume of security challenges have overwhelmed many internal security teams.

The robust growth of the MDR market is being driven by several key factors:

- The increasing need to secure critical cloud data, fueled by widespread cloud adoption.
- The increase in frequency and severity of ransomware attacks.
- Growth in data protection regulations and heightened customer privacy expectations.
- The expansion of IT environments, now encompassing mobile, edge, and cloud computing.
- The shift to remote and hybrid work models post-pandemic.
- Rising threats of data breaches, particularly from state-sponsored cyberattacks.
- The escalation of cyber espionage campaigns targeting personal information, credentials, and intellectual property.
- A rapid increase in data production by organizations.
- Required by cybersecurity insurance providers as a condition for coverage.

The drivers listed above are the main reasons many organizations have already adopted MDR, and why many of those who have not yet 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, and evaluate the effectiveness of existing controls to identify where and how this can be improved.

Many modern MDR solutions focus on continuous security improvement. Increasingly, providers offer personalized concierge or white-glove services, fostering close collaboration between the vendor and customer. Some vendors are planning to introduce these high-touch services to meet growing 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, threat detection, threat triage, threat containment, and even threat recovery and remediation.

MDR solution providers are also increasingly managing complex security systems such as EPDR, NDR, SIEM, and SOAR to reduce the burden on internal security teams. There is also a concerted effort by MDR providers to focus on risk management to address board-level concerns and to move away from a “black box” approach toward greater transparency by giving customers access to the raw security data and documenting in detail all actions taken on the customers’ behalf.

KuppingerCole Analysts expects significant growth and evolution in the MDR market, driven by technological advancements, emerging cyber threats, and shifting business environments. Key areas of innovation are likely to include:

- Greater adoption of machine learning (ML) and artificial intelligence (AI) to improve threat detection, automate responses, and enhance the efficiency of security operations.
- Increased use of generative AI (GenAI) for threat summaries, analyst recommendations, AI assistants, natural language searches, and incident reporting.
- Heightened focus on securing cloud environments.
- Specialized support for Internet of Things (IoT) and containerized environments.
- Deeper integration with other security tools.
- Enhanced capabilities for regulatory compliance and data privacy.
- Expanded focus on ransomware detection, prevention, response, and recovery.
- Greater customization and flexibility to meet diverse organizational needs.

The MDR market has seen considerable consolidation and growth through acquisitions in recent years, as major cybersecurity firms and IT service providers aim to broaden their capabilities and increase market share. Companies like Sophos and Kroll have made significant acquisitions to enhance their MDR portfolios. This trend has led to a more mature market, offering a wider range of services to meet the demands of discerning customers looking to upgrade from their current MDR providers.

The baseline feature set for MDR is continually growing, and as a result, some established vendors may be struggling to keep pace with these rapid advancements, particularly in areas like GenAI integration and cloud-native security.

Despite the consolidation, startups are still able to enter the market by focusing on technical innovations or addressing specific use cases, with some new entrants focusing on GenAI-powered threat intelligence, specialized industry-specific or technology stack-specific MDR solutions, and advanced automation in incident response. This dynamic landscape reflects the ongoing evolution and increasing sophistication of the MDR market.

KuppingerCole Analysts expects MDR providers to offer more advanced, integrated, and user-friendly solutions to address the growing complexity of modern cybersecurity challenges.



## Market Size and Segmentation

The growing demand for MDR solutions is evidenced by the market’s projected compound annual growth rate (CAGR) of 22.5% from 2023 to 2027, with most vendors experiencing substantial sales growth following the Covid-19 Pandemic. Based on data collected for this report, KuppingerCole estimates that the MDR market will grow from \$4.19B in 2024 to \$5.15B in 2025.

### Managed Detection and Response Revenue 2023- 2027

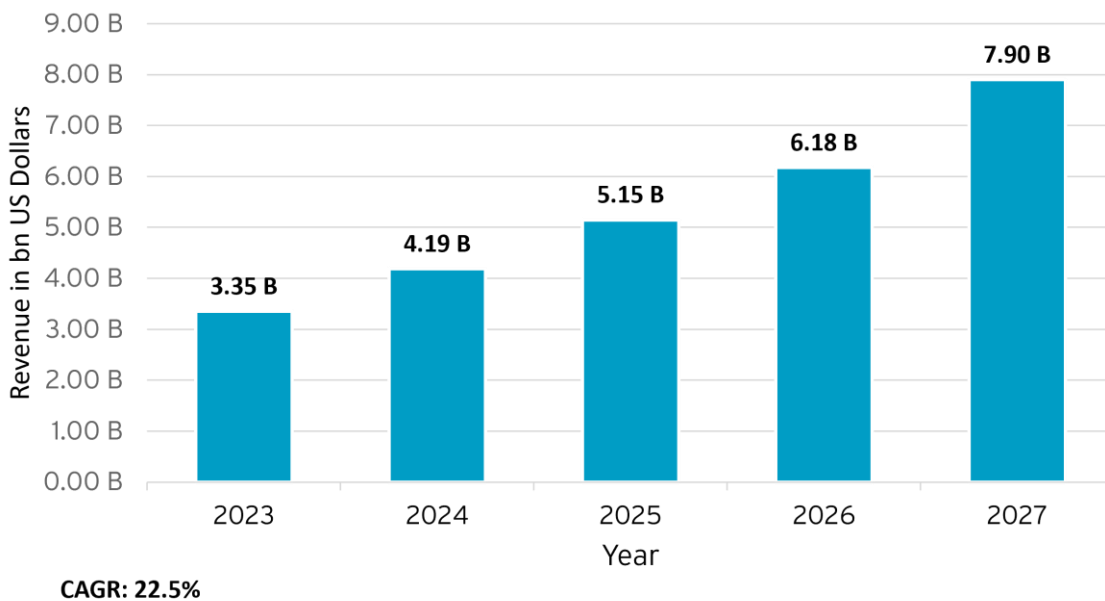


Figure 2: KuppingerCole MDR market growth projections

As shown in this report, the MDR market is made up of diverse services ranging from SOCaaS providers to full MDR services that include incident response and offer a range of optional add-on services. The market includes MDR service providers that cater to MSSPs and channel partners, that provide expertise in supporting specific security technology stacks, and that focus on supporting particular technologies like cloud and containers or market segments such as Small and Medium-sized Enterprises (SMEs). Additionally, platform-specific MDR vendors are creating purpose-built MDR services to integrate with leading XDR platform vendors, providing customers with the option to standardize and consolidate their security technology with a platform approach and then purchase an MDR service designed to operationalize their chosen platform.

## Delivery Models

The MDR market is well-established and mature, yet it continues to grow and adapt to meet rising demand, evolving business needs, increasingly complex IT environments, and ever-changing cyber-attack techniques.

Consequently, MDR solutions are increasingly transitioning away from on-premises deployments to cloud-based services, often using the Software as a Service (SaaS) model. 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 modular architectures and flexible delivery models to best meet customer requirements.

While there are some vendors in this report that are entirely cloud-based services with either lightweight agents or no agents at all, most have some degree of flexibility to cater for customers whose technology 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 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, including data centers, remote workers and contractors, cloud-based services, and IoT, Internet of Medical Things (IoMT), Industrial Internet of Things (IIoT) and Operational Technology (OT).
- Rapid detection, investigation, analysis, and mitigation/containment of cyber risks and incidents.
- Elimination of false positives and prioritization of real threats.
- Continual improvement of security posture by identifying and remediating vulnerabilities.
- Consistently high visibility of threats/incidents across all IT assets.
- Regular assessment of vulnerabilities and risks based on up-to-date threat intelligence.
- Advanced analysis of cyber threats and anomalous behavior, including attacker and behavior analytics.
- Manual and automated/proactive threat hunting.
- Collection, correlation, and analysis of all security data across the IT environment.
- Orchestration and automation of responses to threats.
- Regulatory compliance reporting.
- Mobile access to dashboards and status reports.

We expect solutions to include most of these capabilities. In addition to providing support for these features, solutions must also meet our deployment requirements and work well 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.
- Take over the operation of complex security systems such as EPDR, NDR, SIEM, SOAR, and DLP.
- 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.

# Leadership

When selecting a vendor for a product or service, the decision should not be based solely on the information provided in a KuppingerCole Leadership Compass. While the Leadership Compass offers a valuable comparison based on standardized criteria and helps identify vendors for further consideration, a thorough selection process requires a detailed analysis and a Proof of Concept (PoC), or pilot phase tailored to the specific needs of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership

## Overall Leadership

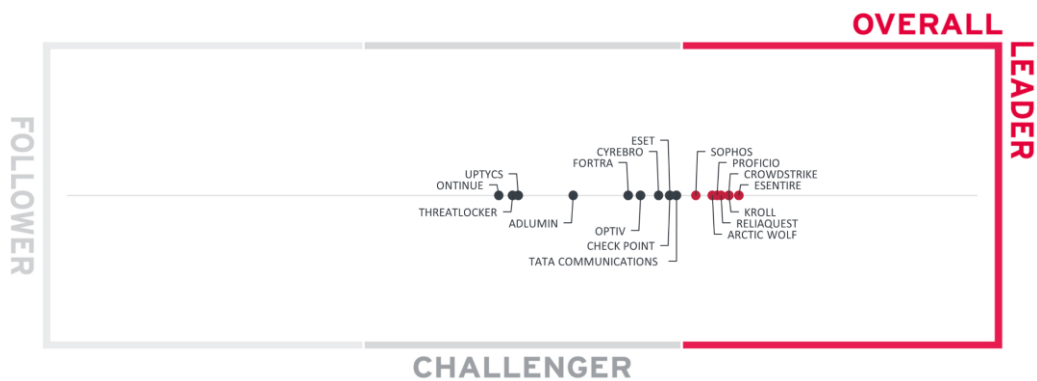


Figure 3: Overall Leadership in the MDR market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Over the past year, eSentire has focused on enhancing its AI-powered automation, adding functionality, expanding its customer base, and strengthening its network of technology, channel, and distribution partners. These efforts have significantly boosted its leadership position since the last MDR Leadership Compass, earning eSentire the highest score among the vendors in this report. However, the close grouping of top leaders highlights the highly competitive nature of the market. eSentire is closely followed by Kroll, CrowdStrike,

ReliaQuest, Proficio, Arctic Wolf, and Sophos, which all offer robust detection and response capabilities, backed by comprehensive coverage, cloud and container support, advanced threat intelligence, and good customer support.

Tata Communications is on the cusp of leadership, with ESET and Check Point close behind. Again, there is very little separating these challengers from the leaders. CYREBRO, Optiv, and Fortra are also approaching the leadership threshold. Adlumin, Uptycs, ThreatLocker, and Ontinue round out the list of overall challengers.

Overall Leaders are (in alphabetical order):

- Arctic Wolf
- CrowdStrike
- eSentire
- Kroll
- Proficio
- ReliaQuest
- Sophos

## Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

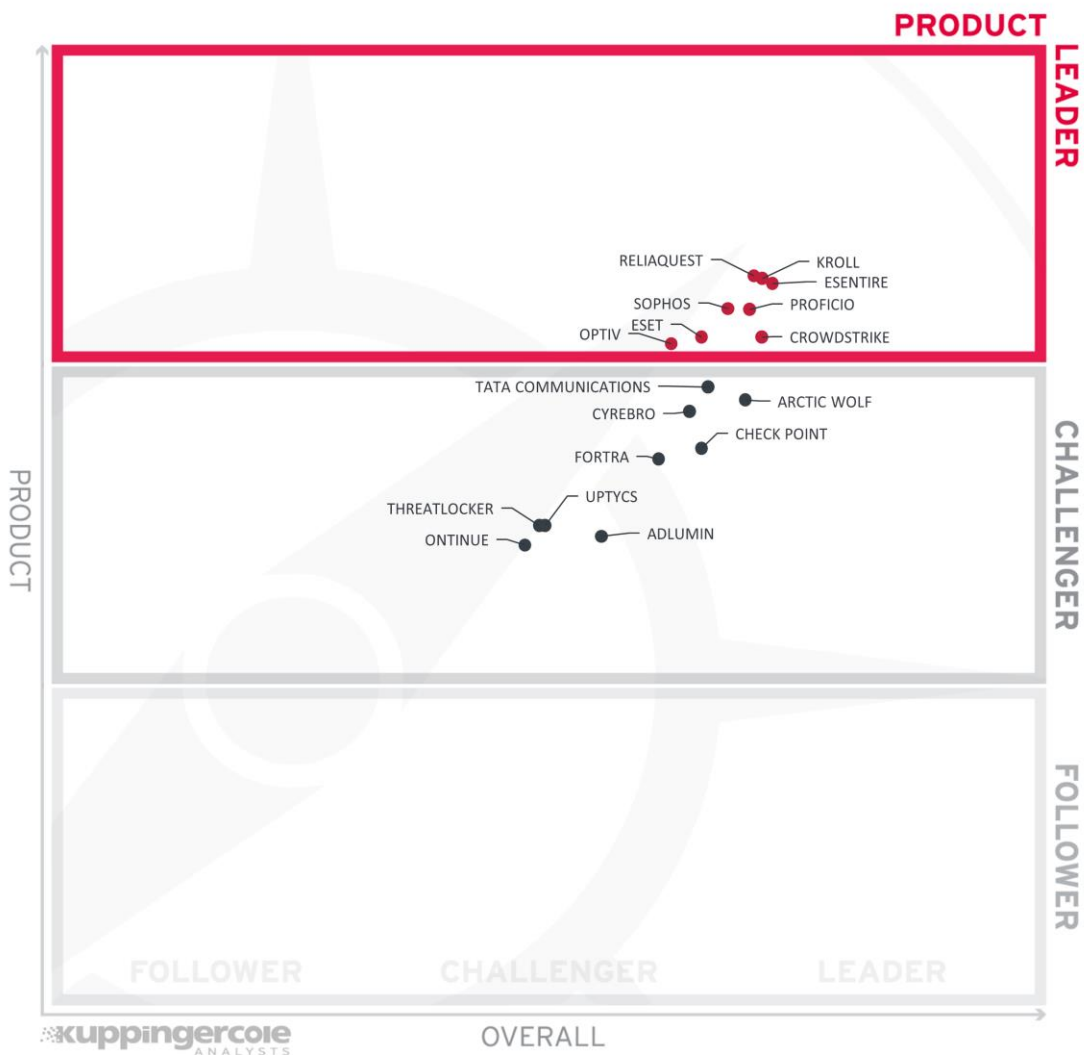


Figure 4: Product Leadership in the MDR market

In this 2024 edition of the Leadership Compass on MDR, ReliaQuest, Kroll, and eSentire top the list for Product Leadership. Sophos and Proficio are in close proximity. These MDR solutions are the most complete in terms of functionality, internal product security, deployment options, interoperability, usability, and integrations available, with ESET, CrowdStrike, and Optiv edging into the product leadership group.

Tata Communications and Arctic Wolf are at the top of the challengers for Product Leadership. CYREBRO, Check Point, and Fortra are also strong challengers. ThreatLocker, Uptycs, Adlumin, and Ontinue are in the middle of the challenger section. With the attention to the areas identified as challenges in this report, the challenger vendors have the opportunity of improving their ratings and even becoming product leaders. However, vendors that focus on supporting particular technology stacks or technology approaches are likely to remain strong niche players that meet specific customer needs.

Product Leaders (in alphabetical order):

- CrowdStrike
- eSentire
- ESET
- Kroll
- Optiv
- Proficio
- ReliaQuest
- Sophos

## Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

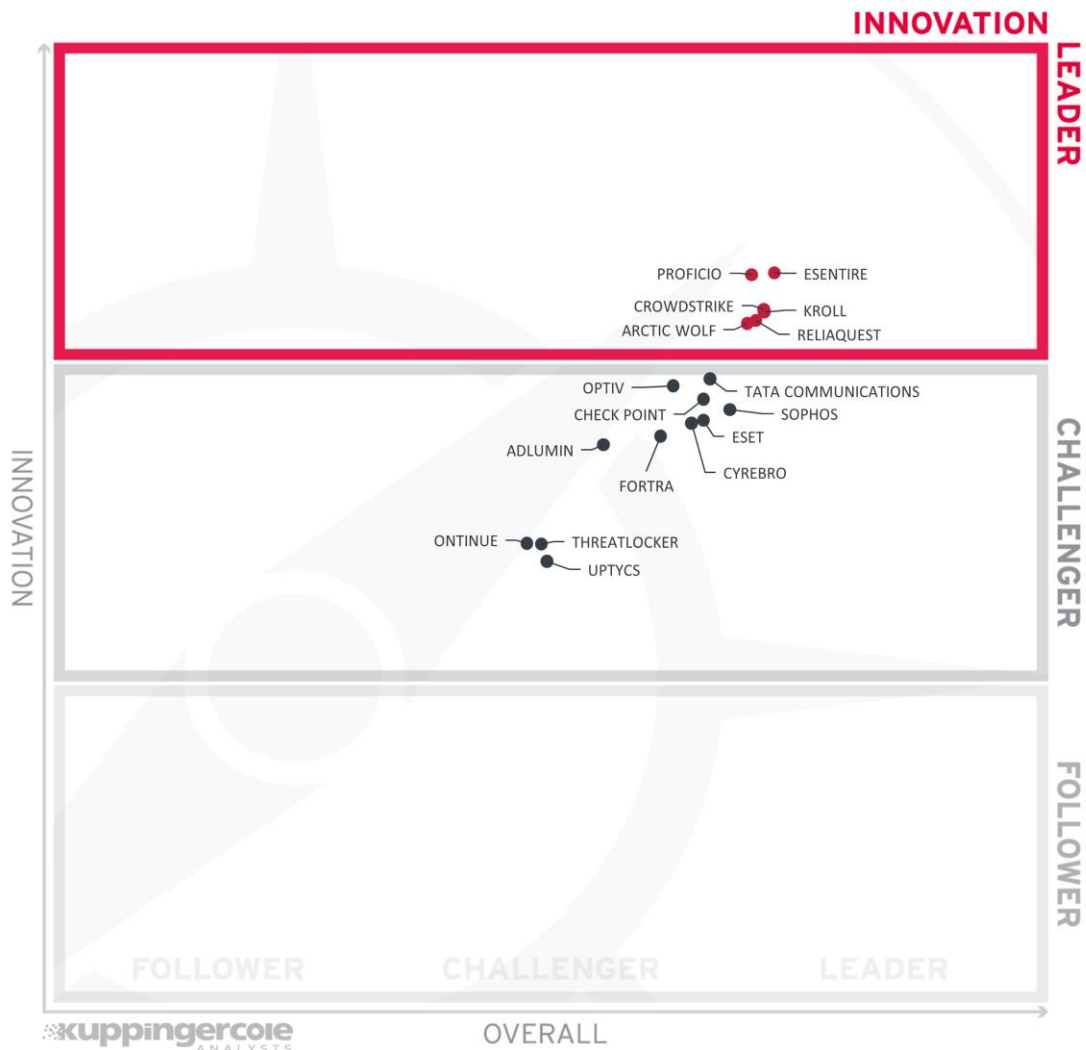


Figure 5: Innovation Leadership in the MDR market



Innovation Leaders are those vendors that deliver cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

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, detection of steganography used for malware control and/or data exfiltration, the inclusion of file integrity monitoring, validation that a threat has been neutralized, the inclusion of predictive threat hunting, support for container environments, the provision of forensic services, and the use of GenAI.

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

eSentire and Proficio are the top vendors in terms of Innovation Leaders, scoring highly in terms of behavior analytics, threat detection and validation, application of machine learning and deep learning, forensic services, and use of deception tools. CrowdStrike, Kroll, ReliaQuest, and Arctic Wolf are also in the leadership category, offering similar innovative capabilities.

Tata Communications, Optiv, Check Point, and Sophos are the top challengers in Innovation Leadership, providing strong innovative capabilities but slightly behind those in the top division. Next, we find ESET, CYREBRO, Fortra, and Adlumin, which also exhibit several areas of innovation, followed by Ontinue, ThreatLocker, and Uptycs, which all have some specific areas of innovation.

Innovation Leaders (in alphabetical order):

- Arctic Wolf
- CrowdStrike
- eSentire
- Kroll
- Proficio
- ReliaQuest

## Market Leadership

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

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

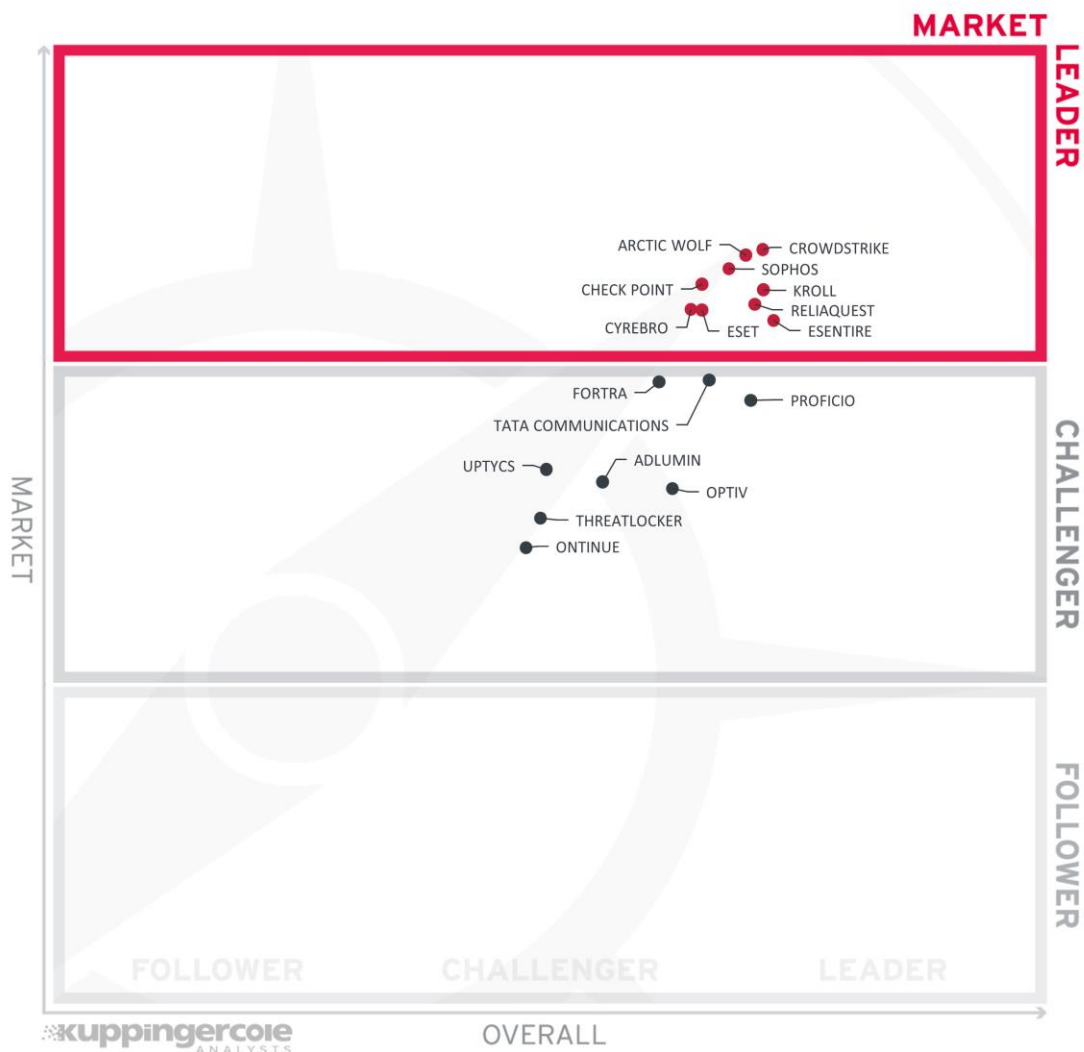


Figure 6: Market Leaders in the MDR Market

CrowdStrike, Arctic Wolf, and Sophos make up the top tier of market leaders closely followed by Check Point and Kroll. ReliaQuest, CYREBRO, ESET, and eSentire make up the remainder of market leaders. The vendors scoring the highest on the vertical axis tend to have large and diverse customer bases, global reach, scalability for large deployments, and extensive partner ecosystems, which enable them to serve more customers across a broad range of industries and geographies. Those lower down on the vertical axis tend to focus on more specialized markets, cater to fewer but more complex customers, and offer higher-touch and bespoke services.

Tata Communications, Fortra, and Proficio are strong challengers for market leadership because they also have large and diverse customer bases, large-scale deployments, global reach and wide geographic distribution, and strong partner ecosystems.

Uptycs, Adlumin, and Optiv make up the middle tier of challengers, followed by ThreatLocker and Ontinue. 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
- Check Point
- CrowdStrike
- CYREBRO
- eSentire
- ESET
- Kroll
- ReliaQuest
- Sophos

## Products and Vendors at a Glance

This section offers an overview of the products analyzed in this Leadership Compass. In addition to the rating overview, we provide comparisons that highlight the relationship between Product Leadership, Innovation Leadership, and Market Leadership. These comparisons help identify vendors that are highly innovative yet specialized, as well as local players with strong product features but without a global presence or large customer base.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name

Vendor	Security	Functionality	Deployment	Interoperability	Usability
Adlumin	Positive	Positive	Neutral	Neutral	Neutral
Arctic Wolf	Strong Positive	Strong Positive	Strong Positive	Positive	Positive
Check Point	Strong Positive	Strong Positive	Positive	Neutral	Positive
CrowdStrike	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
CYREBRO	Positive	Strong Positive	Strong Positive	Positive	Positive
eSentire	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
ESET	Strong Positive	Positive	Strong Positive	Neutral	Strong Positive
Fortra	Positive	Positive	Strong Positive	Neutral	Positive
Kroll	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Ontinue	Positive	Positive	Positive	Neutral	Neutral
Optiv	Strong Positive	Positive	Positive	Strong Positive	Positive
Proficio	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
ReliaQuest	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
Sophos	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Tata Communications	Strong Positive	Strong Positive	Positive	Strong Positive	Positive
ThreatLocker	Neutral	Neutral	Neutral	Positive	Positive
Uptycs	Positive	Neutral	Positive	Neutral	Positive

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

In addition, we provide in Table 2 an overview which also contains four additional ratings for the 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
Adlumin	Positive	Neutral	Positive	Neutral
Arctic Wolf	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Check Point	Strong Positive	Strong Positive	Strong Positive	Strong Positive
CrowdStrike	Strong Positive	Strong Positive	Strong Positive	Strong Positive
CYREBRO	Positive	Strong Positive	Positive	Strong Positive
eSentire	Strong Positive	Strong Positive	Strong Positive	Positive
ESET	Positive	Strong Positive	Strong Positive	Strong Positive
Fortra	Positive	Positive	Strong Positive	Positive
Kroll	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Ontinue	Neutral	Neutral	Neutral	Neutral
Optiv	Strong Positive	Positive	Positive	Neutral
Proficio	Strong Positive	Strong Positive	Positive	Positive
ReliaQuest	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Sophos	Positive	Strong Positive	Strong Positive	Strong Positive
Tata Communications	Positive	Strong Positive	Strong Positive	Positive
ThreatLocker	Neutral	Neutral	Positive	Neutral
Uptycs	Neutral	Positive	Positive	Positive

Table 2: Comparative overview of the ratings for vendors

## Product/Vendor evaluation

This section contains a quick rating for every product/service included in this KuppingerCole Leadership Compass report. 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 standard ratings for categories like Product Leadership and Innovation Leadership, we include a spider chart for each vendor that highlights specific capabilities relevant to the market segment being evaluated in the respective Leadership Compass. For this market segment, we assess the following categories:

**Coverage** – 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 evaluates integrations with other security technologies.

**Cloud/container support** – A measurement of the degree to which solutions provide monitoring and analysis of cloud, multi-cloud, and container environments, including service providers, applications, infrastructures, and data stores. It also looks at cloud security posture management, cloud workload protection, and vulnerability scanning.

**Detection** - An evaluation of threat detection coverage and capabilities across modern business IT environments. It includes behavior and attacker 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 automated response actions, software patching capabilities, ransomware blocking, SOAR capabilities 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, reporting on emerging threats, real-time threat intelligence integration, and threat intelligence research.

**Customer/admin support** - An evaluation of the support provided by the solution to customers in terms of things like 24/7 services, dashboards, collaboration, reporting, continuous improvement, risk management, languages, and regulatory compliance.

## Adlumin – Adlumin Managed Detection and Response

Adlumin is a private cybersecurity company founded in 2016 and headquartered in Washington, DC in the US with offices in more than 20 countries around the world. Adlumin has a global SOC team, with analysts located across the US and a single physical location in Manila, Philippines. Most customers are in North America, followed by EMEA, and fall into the medium market segment.

Adlumin's MDR service is based on its multi-tenanted and technology agnostic eXtended Detection and Response (XDR) Platform that is automatically bundled into the MDR service, which is focused on threat prevention as much as detection and response. The XDR Platform is designed to work with whatever customers have in their technology stack, it is able to gather data from all relevant security data sources using Application Programming Interfaces (APIs) in combination with endpoint agents, is accessible by customers for complete transparency, and applies a consistent methodology to every incident. Adlumin's XDR Platform also provides patented AI-supported User and Entity Behavior Analytics (UEBA), threat intelligence, and automated response capabilities. The MDR service includes round-the-clock monitoring, incident detection, disruption and containment, threat hunting, and incident reporting. A range of optional integrated add-on modules are also available, including vulnerability scanning and patching, security awareness training, automated penetration testing, log management, ransomware defense, and incident response. This helps consolidate licensing and improve performance of the MDR service due to the high level of integration. As an incentive to make use of two or more of these add-ons, Adlumin offers a \$500,000 warranty in partnership with a third-party insurance company.

Adlumin offers a simple tiered pricing model based on the number of devices covered, with an optional Incident Response (IR) retainer, which can be converted to other services if not consumed.

Adlumin MDR is deployed as a cloud service using endpoint agents which facilitates rapid deployment, with most deployments completed within 90 minutes. The service is available exclusively through channel partners, including Value-Added Resellers (VARs), Managed Service Providers (MSPs), and MSSPs.

The service covers all main operating systems, including environments using Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), but excluding Android and iOS. Similarly, it covers all main browsers, including Opera and MS Edge, but excluding Safari.

The service provides 24/7 monitoring and analysis of all major business IT environments and systems, excluding Edge computing environments. It provides detection and response services across all environments, including IIoT, IoMT, OT, and remote workers, but not mobile devices.

Adlumin MDR includes pre-built integrations with five EPDR solutions (CrowdStrike Falcon Endpoint Protection, Microsoft Defender for Endpoint, SentinelOne Singularity Platform, Sophos InterceptX Advanced with XDR, and VMware Carbon Black) and two NDR solutions

(Cisco Secure Network and Cloud Analytics and Darktrace). There are no integrations with third-party SIEM solutions because all SIEM functionality is included in the Adlumin XDR Platform, enabling it to pull information from across customer IT environments.

The service provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. However, it does not include Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), and vulnerability scanning of customer multi-cloud environments. Adlumin MDR can detect a wide range of threats to Kubernetes environments and can handle logging and monitoring across multiple Kubernetes clusters. It can monitor several cloud services out-of-the-box (OOTB), but there is room for improvement.

Adlumin MDR can detect and respond to a wide range of malicious activities, including Remote Desktop Protocol (RDP) exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time and includes network intrusion detection capabilities, but not attacker behavior analytics. It provides OOTB integrations with third-party Intrusion Detection Systems (IDS) and can detect and report privilege escalation.

The service can take response actions regardless of what security technology customers already have, it features a single platform that can respond automatically to disrupt threats, and it includes a wide range of automated response actions, but does not offer software patching functionality. It can block ransomware attacks before any data is encrypted due to strong ransomware detection capabilities supported by Adlumin's UEBA technology in its XDR Platform that identify ransomware-related activities across the whole IT environment. The service includes automated proactive threat hunting, provides playbooks for incident response, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting. Adlumin XDR Platform includes its own SOAR functionality eliminating the need for a third-party SOAR and potential vendor lock-in. Consequently, the service does not include integrations into third-party SOAR solutions.

Adlumin MDR includes threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a dedicated threat hunting team, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The service does not offer real-time threat intelligence integration and provides connectors for only a select set of threat intelligence sources, including but not confined to Shodan, CISA KEV, Malpedia, and Dark Web monitoring. All support services are remote, the service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The service does not include functionality to generate reports that map detected threats to MITRE ATT&CK® tactics and techniques, but it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, but it does not include an ROI calculator or the services of a dedicated risk advisor. Tools for Attack Surface Management (ASM) are available as part of the standard subscription. There is no mobile app to provide access to dashboards and status reports, but there is a



dedicated customer success manager for all customers. Customers have access to the same data, tools, and reporting as Adlumin, and the company does provide potential customers with a pre-sales trial period to allow them to assess if Adlumin MDR is a good fit. Adlumin’s rapid deployment capability means that it can run live demonstrations and customers are able to see the system running in their environment and measure the benefits before making a purchase. The service is audited for SSAE SOC 2 Type 2, it is certified for UK Cyber Essentials and Cybersecurity Maturity Model Certification (CMMC), and offers guaranteed data residency in the US and the EU.

Adlumin MDR is best suited to small to medium-sized businesses with up to 5,000 employees that have limited security resources and internal expertise, and operate in highly regulated sectors such as financial services, government, healthcare, travel and hospitality, education, and manufacturing.

<b>Security</b>	Positive
<b>Functionality</b>	Positive
<b>Deployment</b>	Neutral
<b>Interoperability</b>	Neutral
<b>Usability</b>	Neutral



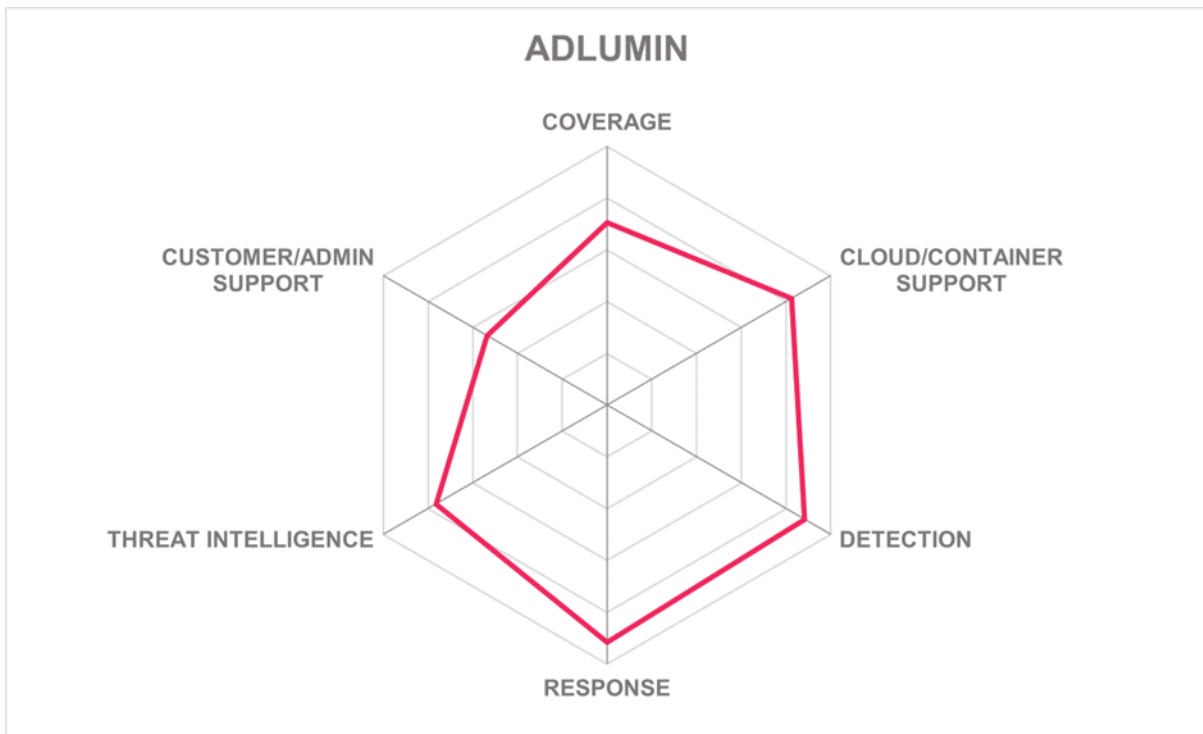
Table 3: Adlumin’s rating

### Strengths

- Designed to work with all technology stacks
- Cloud based, allowing for rapid deployment
- Simple pricing model based on number of devices covered
- Multi-tenanted, providing full visibility for partners and customers
- Patented UEBA technology for additional anomaly detection
- Provides coverage of Kubernetes environments
- Experience in supporting financial services institutions and other highly regulated verticals
- Strong ransomware detection capabilities

### Challenges

- No coverage of mobile devices or mobile operating systems
- Does not cover Edge computing environments
- Does not include CSPM
- Can monitor only a limited number of cloud services
- Does not include attacker behavior analytics
- Documentation and support services available only in English
- Does not provide the services of a dedicated risk advisor



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

Arctic Wolf is a private US cybersecurity company, founded in 2012 and specializing in security operations, including MDR and SOCaaS. Arctic Wolf is headquartered in Eden Prairie, Minnesota, with SOC's in Eden Prairie, San Antonio, and Pleasant Grove in the US, Waterloo in Canada, Frankfurt in Germany, and Sydney in Australia. Arctic Wolf caters to all sizes of organization and has customers around the world with the majority in North America, followed by Europe, Middle East, and Africa (EMEA).

Arctic Wolf MDR is a vendor-neutral concierge-style service based on the Arctic Wolf Platform built on open XDR architecture. The service is available in three outcomes-based and risk-focused packages: Security Operation Core, Plus, and Total. All three packages include MDR, support for continual security improvement, access to a concierge security team, data search, and log retention. Core comes with a warranty of up to \$100,000 based on a three-year contract. Plus offers a greater level of risk mitigation/transfer by adding Arctic Wolf's managed risk service, with a warranty of up to \$1M based on a three-year contract. Total offers the greatest level of risk mitigation/transfer by adding Arctic Wolf's managed security awareness service and an IR retainer, with a warranty of up to \$1.5M based on a three-year contract. Customers can also choose between three levels of concierge engagement: Silver, Gold, and Platinum. All three levels include a dedicated security team, 24/7 SOC support, escalation follow up, security posture reviews, and scheduled proactive engagements increasing from four (Silver) to 12 (Gold) to 18 (Platinum). Pricing of the packages and concierge tiers 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.

Arctic Wolf offers rapid deployment times and flexible on-premises, cloud, and hybrid deployment models, depending on customers' requirements. The solution is available directly to end user organizations, but mainly through channel partners, MSPs, and MSSPs.

Arctic Wolf MDR covers all major operating systems, including collecting telemetry for Android and iOS, and all main browsers. The service provides 24/7 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 remote workers, but not OT and medical and industrial IoT devices.

Arctic Wolf MDR includes prebuilt integrations with 14 common third-party EPDR products and 20 NDR products, but none for any third-party SIEM solutions. However, 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 continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also includes CSPM, CWP, and vulnerability scanning of customer multi-cloud environments. Arctic Wolf MDR can detect a wide range of threats to Kubernetes environments, and can handle logging and

monitoring across multiple Kubernetes clusters. It can also monitor a selection of cloud services for MDR purposes, including Azure AD, MD Office 365, MS Defender for Cloud Apps, Google Workspace, Salesforce.com, and Box.

Arctic Wolf MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, and includes network intrusion detection capabilities. The service also includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to detect and report privilege escalation.

Arctic Wolf MDR is designed to integrate with existing technology stacks and can take response actions regardless of what customers already have, it features a single platform that can respond automatically to disrupt threats and includes a limited number of automatic response actions, such as terminating network sessions, isolating hosts or endpoints, and blocking communications by port and IP. There is a focus on BEC to ensure affected users can be isolated in the event of a compromise. The solution does not include software patching functionality, but can block ransomware attacks before any data is encrypted. If ransomware does execute, Arctic Wolf can isolate any affected endpoints. If a customer has Arctic Wolf's sensors deployed through an internal Test Access Point (TAP) configuration, the sensors can be used to isolate parts of the compromised network. The solution includes automated proactive threat hunting, provides more than 50 playbooks for incident response, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting.

The solution has its own SOAR capabilities based largely on technology integrated into the Arctic Wolf Platform after the company's 2023 acquisition of Revelstoke, a SOAR platform built on a unified data layer (UDL). Consequently, there are no OOTB integrations with any third-party SOAR solutions, but integration with customer-owned SOAR platforms is possible through integrations with the likes of ServiceNow.

Arctic Wolf MDR includes strong threat intelligence capabilities for advanced threat detection and risk mitigation, uses ML-supported threat detection models, includes the support of a dedicated threat hunting team and a global team of threat intelligence researchers, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The solution offers real-time threat intelligence integration and provides connectors only to a select set of proprietary and third-party threat intelligence sources. It also includes Dark Web monitoring for threat intelligence and extracts threat intelligence from Arctic Wolf's thousands of MDR and IR customers.

Arctic Wolf MDR can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The solution includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, an ROI calculator, the services of a dedicated risk advisor and customer success manager, and tools for ASM. There is no mobile app that provides access to dashboards and status reports. Customers have access to the same data and reporting as Arctic Wolf, and there is

provision of a pre-sales trial for potential customers to see if the solution is a good fit for their organization. The solution complies with the standards and principles of ISO 27001 and SSAE SOC 2 Type 2. Although not HITRUST certified, the solution shows alignment to HITRUST controls, and offers data residency for the EU and the US.

Arctic Wolf MDR is suitable for all sizes of business in all verticals, particularly medium and mid-market enterprises in the finance, manufacturing, and healthcare sectors looking for a comprehensive, flexible, and personalized concierge-style MDR service with a focus on continual security improvement, risk reduction, ransomware, and BEC.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Deployment</b>	Strong Positive	
<b>Interoperability</b>	Positive	
<b>Usability</b>	Positive	

Table 4: Arctic Wolf's rating

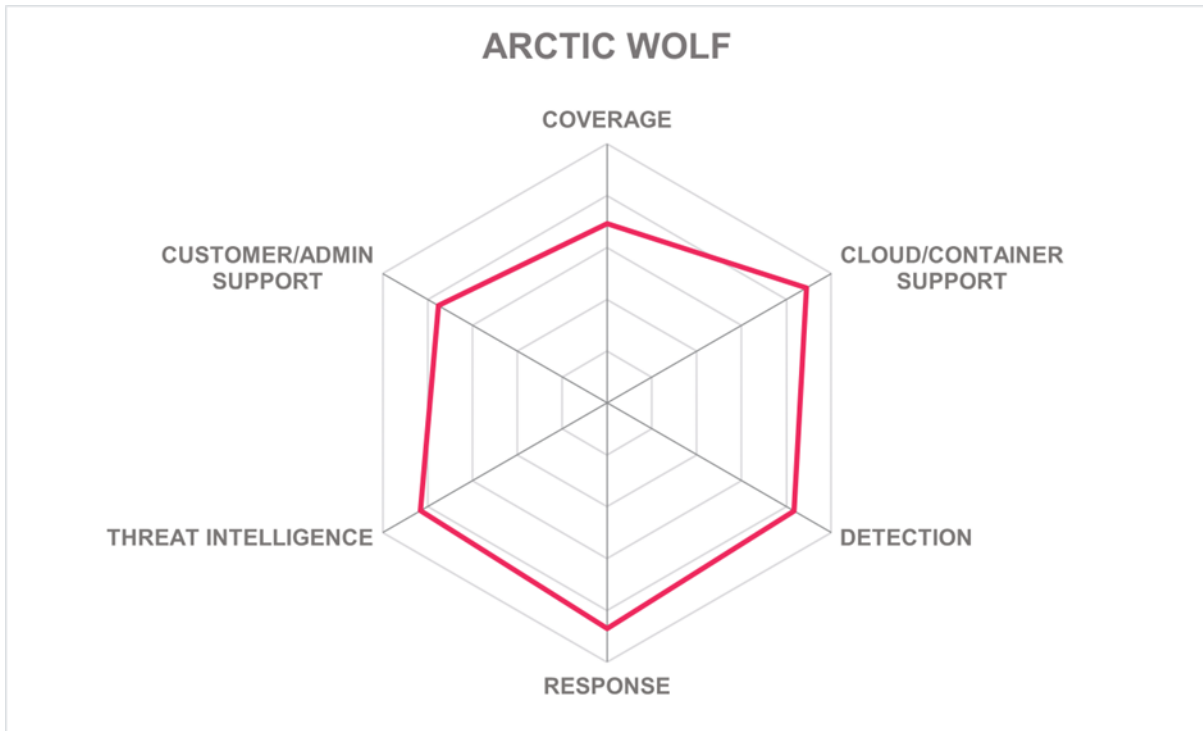
### Strengths

- Rapid and flexible deployment
- Choice of outcome and risk-based packages
- Choice of concierge engagement level
- Fixed, predictable contract pricing
- Warranty program aimed at incentivizing risk management
- Good MDR coverage of cloud and container environments
- Includes user and attacker behavior analytics
- Good ransomware protection capabilities
- Strong SOAR capabilities based on Revelstoke acquisition
- Strong threat intelligence capabilities with cross-industry visibility

### Challenges

- No OOTB integrations for third-party SIEM solutions
- Not able to detect container vulnerabilities in Kubernetes environments
- Limited set of automatic response actions
- Does not include software patching functionality
- Support services and local documentation available only in English and German
- No Mobile app to access dashboards and status reports

Leader in



## Check Point – Infinity MDR

Founded in 1993 and headquartered in Tel Aviv, Israel, Check Point is a public multinational cybersecurity company that provides software and hardware products for network security, endpoint security, cloud security, and threat intelligence, including MDR. Check Point has a single global SOC with operates on a follow-the-sun model with SOC analysts in three virtual teams located in Australia, Spain and UK, and the US. Most customers are small to medium-sized businesses located in EMEA, followed by North America.

Check Point's MDR service is an integral part of the Check Point Infinity architecture, leveraging the Infinity SOC platform to provide 24/7 proactive threat prevention as well as detection and response. The service is technology agnostic and combines advanced AI-driven threat intelligence with human oversight to provide comprehensive security coverage across networks, cloud environments, and endpoints.

Check Point has a simple per-user, per-year pricing model, which includes 100 hours of incident response. The MDR service is cloud-based and does not use sensors or agents, enabling rapid deployment times of between one and seven days. The solution is available through MSSPs and channel partners, enabling global coverage.

The MDR service covers all major operating systems, including Android and iOS, and all main browsers.

Infinity MDR provides 24/7 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, OT, and remote workers.

The service is designed to enable API-based integrations with as many third-party products as possible. However, it has no prebuilt integrations for third-party NDR solutions, only five with third-party EPDR solutions (CrowdStrike Falcon Endpoint Protection, MS Defender for Endpoint, SentinelOne Singularity Platform, Sophos InterceptX Advanced with XDR, and TrendMicro), and only two with third-party SIEM solutions (MS Sentinel and Trend Vision One).

Infinity MDR provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also includes CSPM, CWP, and vulnerability scanning of customer multi-cloud environments. The service can detect a wide range of threats to Kubernetes environments, and can handle logging and monitoring across multiple Kubernetes clusters. It can monitor seven cloud services (Azure AD, MS Office 365, MS Defender for Cloud Apps, Google Workspace, Google Drive, ServiceNow, and Slack).

Infinity MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, it can detect malicious executables before they run,

and includes network intrusion detection capabilities. The service also includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to detect and report privilege escalation.

The service offers a response SLA of 30 minutes for critical incidents, although detection and containment is typically achieved well within that time. It can take response actions regardless of what security technology customers already have, it features a single platform that can respond automatically to disrupt threats, it includes a wide range of automated response actions, and it includes functionality for software patching. It also blocks ransomware attacks before any data is encrypted, includes automated proactive threat hunting, provides playbooks for incident response, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting. The service includes its own SOAR platform that uses Check Point Playblocks pre-defined, automated response workflows, and comes with a prebuilt integration for Microsoft Sentinel.

Infinity MDR includes threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a dedicated threat hunting team backed by 200 security researchers around the world, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. While the service offers real-time threat intelligence integration and uses Check Point Threat Cloud that incorporates hundreds of commercial and open-source threat intelligence sources, it does not provide customers with any connectors to third-party threat intelligence sources. The service includes Dark Web monitoring for threat intelligence.

The MDR service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience and a dedicated customer success manager. However, the service does not include the services of a dedicated risk advisor, an ROI calculator, or ASM tools, but these are available as an optional extra. There is no mobile app that provides access to dashboards and status reports. Customers have access to the same data, tools, and reporting as Check Point, and potential customers can take advantage of a 30-day POC. Check Point encourages POCs to ensure that Infinity is a good fit and to learn what customers are looking for. The service provides reporting for compliance teams and complies with standards and principles of ISO 27001 and SOC 2 Type 2. It also offers guaranteed data residency for the EU, US, and UAE.

Check Point Infinity MDR supports organizations of all sizes and verticals, particularly the public sector, defense, critical infrastructure, manufacturing, and chemical/pharmaceutical, and will appeal to organizations looking for rapid prevention, detection, and full incident response services in a single solution that is easy and quick to deploy.



<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Neutral
<b>Usability</b>	Positive



Table 5: Check Point's rating

**Strengths**

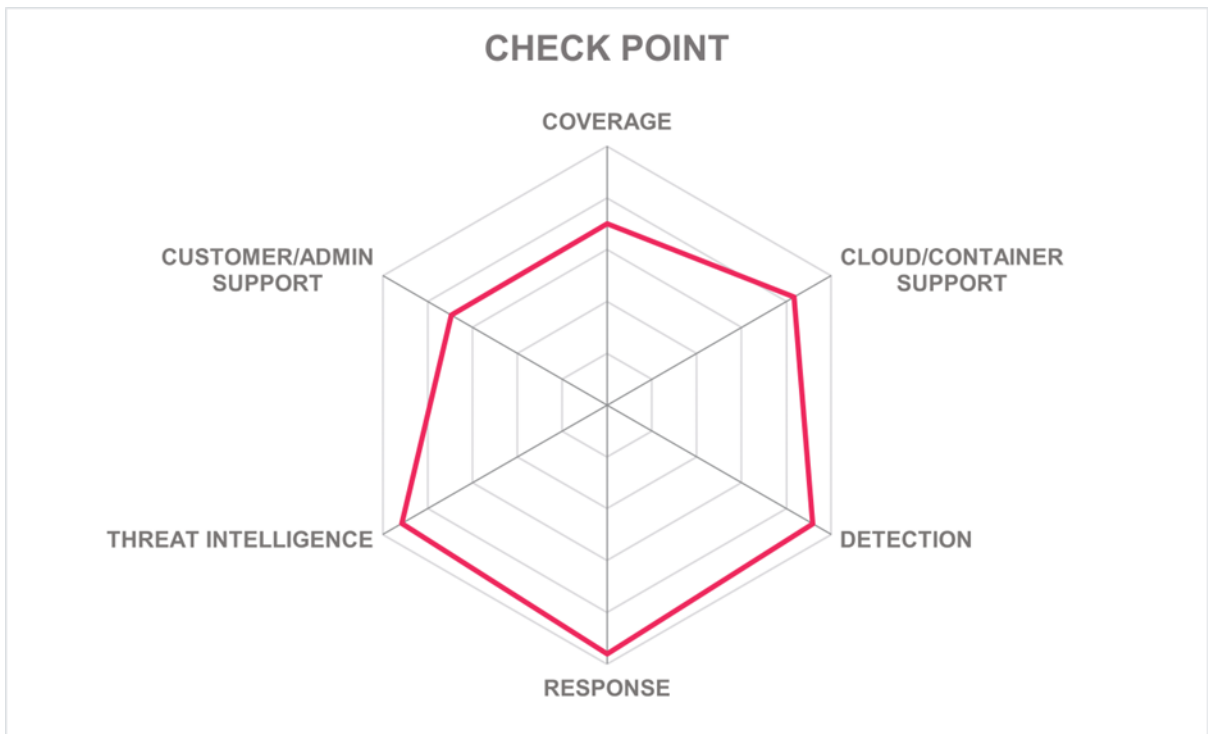
- Technology agnostic
- Simple, predictable pricing model that includes IR
- No limit to the number of log sources or integrations
- Cloud-based service without sensors or agents
- Rapid deployment
- Good coverage of cloud and container environments
- Wide range of automated response actions
- 30-minute SLA for critical incidents
- Strong threat intelligence capabilities
- Guaranteed data residency for the EU, US, and UAE
- Emphasis on threat prevention and continuous improvement

**Challenges**

- Limited number of prebuilt integrations with third-party SIEM solutions, but more on the roadmap
- Limited number of prebuilt integrations with third-party NDR and EPDR solutions
- No mobile app for access to dashboards or status reports

Leader in





## CrowdStrike – Falcon Complete Next-Gen MDR

CrowdStrike was founded in 2011 and is headquartered in Sunnyvale, California. CrowdStrike's MDR Service, Falcon Complete Next-Gen MDR, has SOC locations in the US, UK, Australia, New Zealand, and Japan.

CrowdStrike has customers in all market segments, particularly medium-sized businesses, and has customers around the world, mainly in North America followed by EMEA and APAC.

Falcon Complete Next-Gen MDR provides 24/7 monitoring, threat hunting from the Falcon Adversary OverWatch team, and remediation services, combining the capabilities of the broader AI and cloud-native CrowdStrike Falcon Platform with a team of security experts who provide continuous monitoring, threat hunting, and incident response. CrowdStrike launched its MDR service in 2018, and has continued to expand capabilities beyond endpoint protection to deliver comprehensive AI-supported detection protection and response capabilities across endpoints, identities, cloud workloads, and critical third-party data without requiring the customer to manage these operations themselves.

Offered as a cloud-native SaaS solution with an annual subscription, the service is based on the size of the customer environment and licensed by the number of endpoints protected. The service features rapid deployment, a single lightweight-agent architecture, dynamic scaling, and continual updates. For customers looking for managed protection beyond the endpoint, Identity Protection (licensed by the number of identities), Falcon Cloud Security, and Falcon Next-Gen SIEM (licensed by ingest) are available as add-ons.

For customers looking for more flexible procurement options, Falcon Complete Next-Gen MDR is also available through CrowdStrike Falcon Flex. This offers a pre-negotiated commitment that can be used to expand access to additional CrowdStrike offerings, including newly released modules and services.

The core service is available directly to end user organizations, with MSPs, MSSPs, and channel partners providing additional managed security services (customizations), and strategy and consulting services through the Falcon Complete for Service Providers program.

Falcon Complete Next-Gen MDR provides round-the-clock monitoring, threat detection and response services across all major business IT environments and systems, including Edge computing environments, medical and industrial IoT devices, OT, and remote workers. The service leverages Falcon Next-Gen SIEM and purpose-built integrations from Falcon Next-Gen SIEM ISV partners to enable the ingestion of third-party data and response across security domains such as firewalls, email security, SSE, and NDR.

The service provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It can detect and respond to threats to multi-cloud environments, and it can monitor most cloud services. It also includes CWP and can detect a wide range of threats to Kubernetes environments using AI/ML, indicators of attack (IOA) and custom hash blocking. It can also handle logging and monitoring across multiple Kubernetes clusters.

Falcon Complete Next-Gen MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, it can detect malicious executables before they run, and includes network intrusion capabilities. The service also includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to detect and report privilege escalation. CrowdStrike has an independently verified Mean Time to Detection (MTTD) of four minutes and claims an MTTR of 43 minutes.

The Falcon Complete team can take actions to respond to threats, including removing malicious files, isolating hosts, enforcing MFA and password reset, and containing command and control (C2) traffic. However, it does not include functionality for software patching. The service provides playbooks for incident response, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting. The service also provides its own SOAR functionality.

Falcon Complete Next-Gen MDR leverages native threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a dedicated threat hunting team backed by a global team of researchers, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models.

The service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, an ROI calculator, the services of a security advisor, and several dashboards to help customers get instant visibility into their managed environment, including key metrics like median time to triage and time to resolve. There is no mobile app to provide access to dashboards and status reports but customers can access the Falcon UI as a single place to view information around security investigations and communications. The service provides a security advisor, and customers have access to the same data, tools, and reports as CrowdStrike.

CrowdStrike has obtained an [impressive list of certifications](#), complying with the standards and principles of ISO 27001, SSAE SOC 2 Type 2, PCI-DSS, CSA Star Level 1 and 2, US FedRAMP, HIPAA/HITRUST, NIST 800-53, NIST 800-171, UK Cyber Essentials, GDPR, UK G-Cloud, TISAX, and APEC. The service offers guaranteed data residence for the EU and the US.

Falcon Complete Next-Gen MDR can cater to a wide range of organizations, particularly those with higher cybersecurity demands or those undergoing transformation in their security operations. Any organization looking for a flexible, scalable, and rapidly deployable MDR service should have CrowdStrike Falcon Complete Next-Gen MDR near the top of their list for RFPs.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive



Table 6: CrowdStrike's rating

**Strengths**

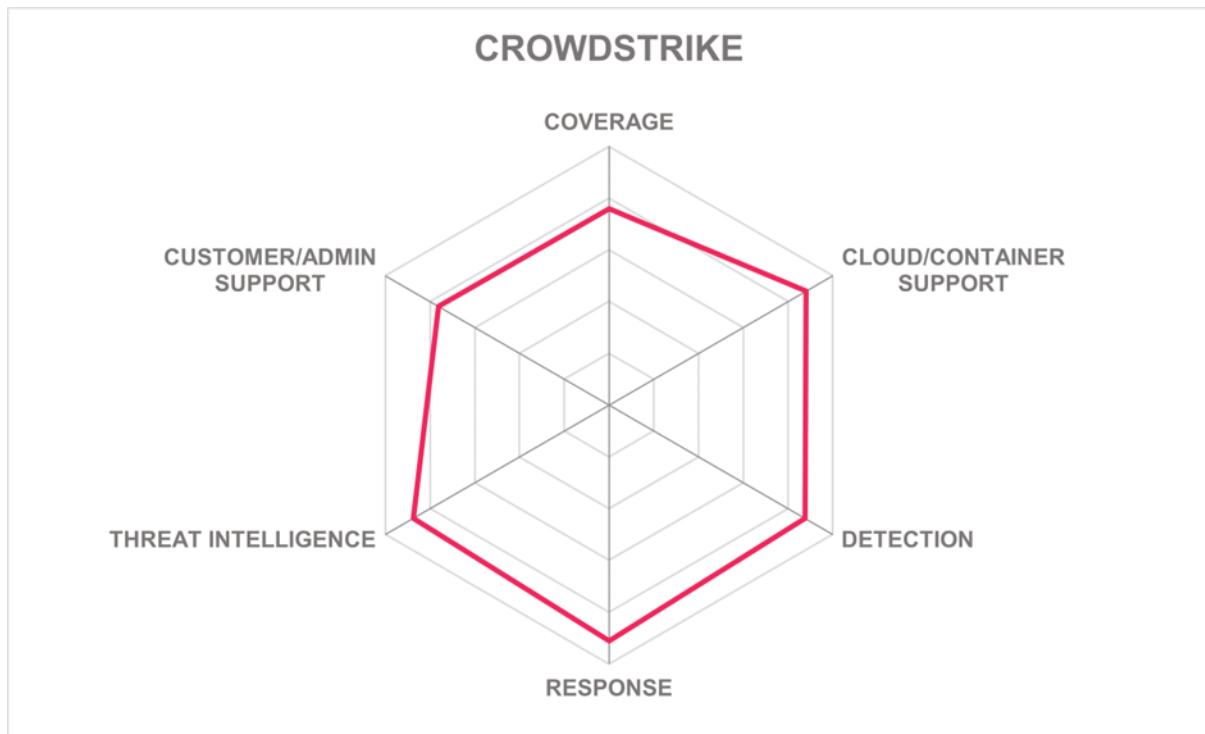
- Deployed as a cloud-native SaaS solution
- Rapid deployment with dynamic scaling
- A single lightweight-agent architecture
- Service built on the AI-native CrowdStrike Falcon platform
- Good coverage of business IT environments, including OT and IoT
- Wide range of automated response capabilities
- Strong support for cloud and container environments
- Rapid detection with verified MTTD of four minutes
- Good response time with an MTTR of 43 minutes
- Strong support for compliance
- Support and documentation available in a wide range of languages

**Challenges**

- Does not include functionality for software patching
- No mobile app for access to dashboards and status reports

Leader in





## CYREBRO – CYREBRO

CYREBRO (formerly Cyberhat) is a private cybersecurity company founded in 2013 and based in Tel Aviv, Israel with a second office in New York, US. There is a single global SOC in Tel Aviv. Most customers are in EMEA, closely followed by North America, and fall into the mid-market segment.

CYREBRO's MDR services are based on the cloud-native CYREBRO platform, which was launched in 2020 and is designed to provide state-level detection, analysis, and investigation of security threats to micro, small, and medium-sized businesses as well as large enterprises. The platform, which was relaunched in 2024 after being rearchitected in partnership with Google Cloud to provide robust and scalable multi-tenancy, combines Security Data Lake with SIEM and SOAR-like capabilities, SOC, ticketing, and Digital Forensics and Incident Response (DFIR). EDR is optional. The platform features automated and AI-based log ingestion with multi-language support. Log data is automatically parsed and normalized into a unified schema based on the Open Cybersecurity Schema Framework (OCSF).

CYREBRO MDR is a cloud-based service and therefore can be deployed quickly, its pricing model is based on the number of endpoints, resources, and network devices. The service is available through MSSPs, MSPs, and other channel partners. It is also available directly to customer organizations that have the necessary in-house skills to configure the platform and implement recommendations based on investigations by analysts.

The service covers all operating systems, including Android and iOS, and all browsers. It provides detection and response services across most environments, including industrial IoT devices, OT, and remote workers, but not medical IoT devices and mobile devices. The service includes prebuilt integrations with most third-party EPDR solutions and a dozen NDR solutions, but none with third-party SIEM solutions.

CYREBRO provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threat to multi-cloud environments. It also includes CWP, but not CSPM or vulnerability scanning of customer multi-cloud environments. CYREBRO is able to detect some threats specific to Kubernetes environments, and can handle logging and monitoring across multiple Kubernetes clusters. It can also monitor most cloud services for MDR purposes.

CYREBRO can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, and evasive malware, but not insider threats. It can detect and respond to phishing attacks in real time, and it can detect malicious executables before they run. The platform includes a detection engine that combines rule-based detection with AI anomaly detection, and is applied continuously from data ingestion to reduce the number of alerts by around 90%, according to the company. CYREBRO includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to detect and report privilege escalation.

The platform can take response actions regardless of what security technology customers already have, it can respond to disrupt threats automatically, and it includes a wide range of automated response actions, but does not include software patching functionality. It can block ransomware attacks before any data is encrypted, includes automated proactive threat hunting, provides playbooks for incident analysis, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting. The service includes the support of four tiers of analysts and a strong DFIR team with a track record in military, government, finance, and gaming sectors. The platform provides its own SOAR functionality that can be tailored to customers' specific automation needs, and comes with integrations for eight third-party SOAR solutions (IBM Resilience, Manage Engine, MS Sentinel, Palo Alto XSOAR, ServiceNow, Siemplify, Splunk, and Swimlane).

CYREBRO includes strong threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a dedicated threat hunting team backed by a global team of researchers, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The platform offers real-time threat intelligence integration and provides connectors for a dozen commercial threat intelligence sources. The platform includes Dark Web monitoring for threat intelligence.

CYREBRO provides on-site support through channel partners. The service can be used to outsource the SOC function with the support of MSP or MSSP, and the platform enables collaboration with and support for customer SOC teams at large, mature organizations. The platform includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and includes customizable reporting for business executives, but not for technical teams and compliance teams. The service includes recommendations on improving cyber resilience and tools for ASM, but it does not include a dedicated risk advisor as part of the standard subscription. This is available for an additional fee. However, it does include a dedicated customer success manager as part of the standard subscription. The service does not include an ROI calculator or a mobile app for accessing dashboards and status reports. Customers have access to the same data, tools, and reporting as CYREBRO. Potential customers can take advantage of a pre-sales trial period to assess if CYREBRO is a good fit in the form of a limited proof of concept (POC). The service complies with the standards and principles of ISO 27001, PCI-DSS, and SSAE SOC 2 TYPE 2, and offers guaranteed data residency for the EU and the US.

CYREBRO caters to organizations of all sizes and verticals, particularly small and medium businesses through MSSPs and MSPs, who benefit from a multi-tenant solution, and organizations looking for fast onboarding, transparency, access to raw data, precision detections, and maximum benefit from existing security technology investments.



<b>Security</b>	Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Positive



Table 7: CYREBRO's rating

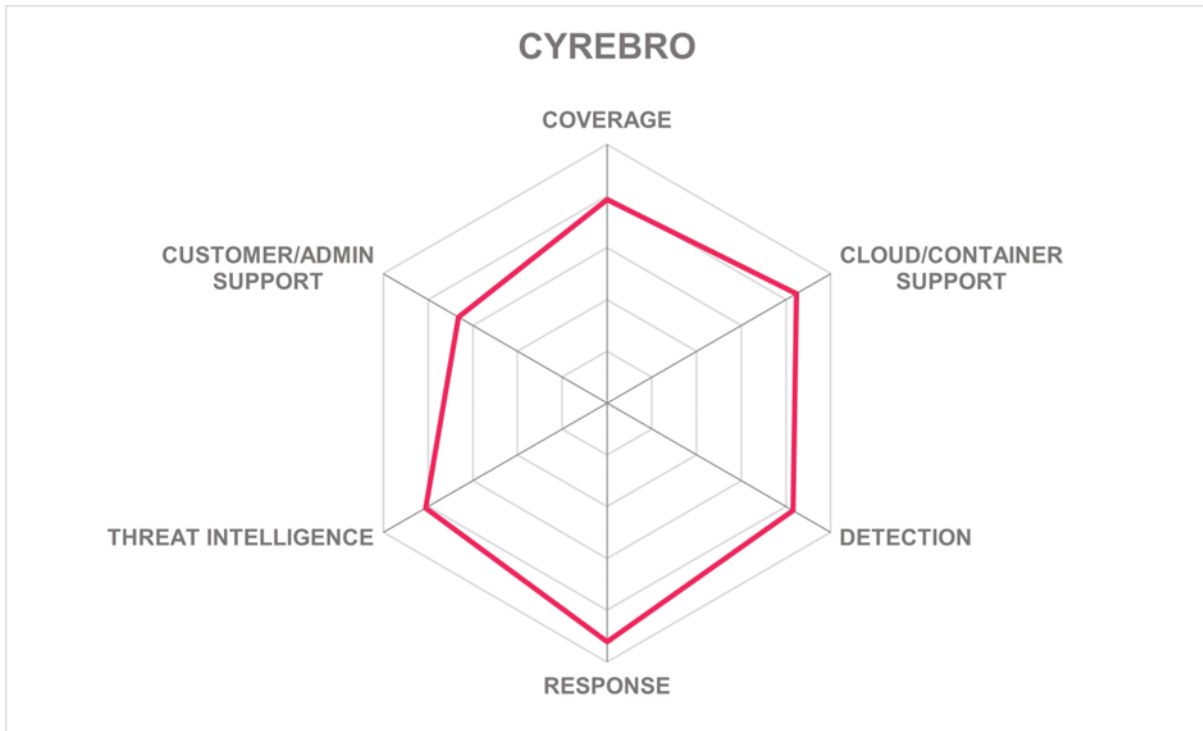
### Strengths

- State-level threat detection, analysis, and investigation capabilities
- Simple pricing model
- Rapid deployment and highly scalable
- Technology agnostic
- Automated and AI-based log ingestion with multi-language support
- Data parsed and normalized into a unified schema based on OCSF
- Rule-based detection engine combined with AI anomaly detection
- Coverage of all major operating systems and browsers
- Includes a wide range of automated response actions
- Features own AI-native Security Data Lake build in collaboration with Google Cloud
- Includes own customizable SOAR functionality
- Local language support through channel partners
- Strong channel and technology partners, including Google Cloud

### Challenges

- Does not provide coverage of medical IoT and mobile devices
- No natural language search but on the roadmap
- No prebuilt integrations with third-party SIEM solutions
- Does not include CSPM or vulnerability scanning of multi-cloud environments.
- Limited support for Kubernetes environments
- Does not detect insider threats
- Documentation available only in English and Spanish
- No mobile app for accessing dashboards or status reports
- Lacks no-code automation workflow capabilities but this on the roadmap

Leader in



## eSentire – eSentire Managed Detection and Response (MDR)

eSentire is a private global MDR company founded in Canada in 2001, with its headquarters and a SOC in Waterloo, Ontario, and an additional SOC in Cork, Ireland. The company operates in 80 countries around the world with most customers in North America, followed by EMEA, and serves organizations of all sizes, with most falling into the medium and mid-market enterprise segments.

Launched in 2008, eSentire MDR combines its proprietary, open cloud-native Atlas XDR Platform, multi-signal threat intelligence, and teams of round-the-clock SOC analysts and threat hunters. The Atlas Platform ingests network, cloud, log, endpoint, and identity threat signals, and correlates Indicators of Compromise (IoCs) to detect and respond to threats automatically. The platform “learns” from positive SOC investigations, adding more than 200 IoCs to its global block list every day to improve 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 MDR includes 24/7 SOCaaS protection across three pricing bundles: Essentials for SMEs, Advanced for the mid-market, and Complete for large mature organizations. All pricing bundles are based on the number of endpoints, which allows for occasional spikes in log data without extra cost. 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. The network sensor can be virtual or physical. eSentire’s endpoint agent is deployed as software and is designed to facilitate easy technology migration, prevention, detection, response, and notification. eSentire provides quick time to value, with deployments and initial operation within a day and the average MDR for endpoint service deployed within seven days, and log tuning completed within 21 days.

The solution is available directly to end user organizations, via MSSPs, and via channel partners. eSentire works with Technology Service Brokers (TSBs) to service the small to mid-market in North America and globally with value added resellers (VARs) and with technology partners to service the mid-market and enterprise segments.

eSentire MDR covers all major operating systems, including Android and iOS, and main browsers.

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 all environments, including medical and industrial IoT devices, OT, and remote workers.

eSentire MDR offers OOTB integrations with only four EPDR solutions: CrowdStrike Falcon Endpoint Protection, Microsoft Defender for Endpoint, SentinelOne Singularity Platform, and VMware Carbon Black. However, eSentire also provides its own proprietary EDR offering, the eSentire Atlas Agent, which includes a deep learning-based malware detection capability

in partnership with Deep Instinct. The eSentire Atlas Agent can also be deployed alongside other EDR solutions to provide multi-layered defense by supporting things like EDR bypass detection, additional threat hunting, and forensic analysis and response. In addition to eSentire's proprietary network product, eSentire MDR offers OOTB integrations with most third-party NDR solutions, but only three SIEM solutions: Microsoft Sentinel, SumoLogic, and Splunk. In addition to these bi-directional response integrations, eSentire also integrates with more than 300 technologies through API and logging support for complete coverage of customer technology stacks.

eSentire MDR provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services. It can identify data loss across cloud infrastructure, detect and respond to threats to multi-cloud environments, and monitor most cloud services OOTB. It also includes CSPM, CWP, and vulnerability scanning of customer multi-cloud environments. eSentire MDR can detect a wide range of threats to Kubernetes environments, and can handle logging and monitoring across multiple Kubernetes clusters.

eSentire MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, it can detect malicious executables before they run, and includes network intrusion detection capabilities. The solution includes both user and attacker behavior analytics as well as integrations with third-party IDS, and the ability to detect and report privilege escalation. eSentire claims a Mean Time to Contain (MTTC) of 15 minutes.

The solution can take response actions regardless of what security technology customers already have, it features a single platform that can respond automatically to disrupt threats, and includes a wide range of automated response actions. However, it does not include software patching functionality. It can block ransomware attacks before any data is encrypted, includes automated proactive threat hunting, provides playbooks for incident response, and applies AI/ML for detecting anomalous behavior and identifying threats, but not for predictive threat hunting. While the solution provides its own SOAR functionality, it can integrate with all major SOAR platforms through APIs.

eSentire MDR includes strong threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a dedicated threat hunting team, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The solution offers real-time threat intelligence integration and provides connectors for a select number of commercial threat intelligence sources. eSentire also uses an undisclosed number of open-source intelligence sources as well as Canadian, US, and UK government feeds in addition to curating its own threat intelligence, including through Dark Web monitoring. The in-house threat intelligence capability is backed by a global team of researchers. eSentire claims that of the threat intelligence they operationalize, 35% is ahead of the commercial feeds, 12% is never seen in commercial feeds, and that their intelligence has a 99% positive hit rate.

On-site support is available in North America, EMEA, and APAC. eSentire MDR can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The solution includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, an ROI calculator, and the services of a dedicated risk advisor as part of a higher-level subscription or as an optional extra. Tools for ASM are available as part of the standard subscription. There is no mobile app, but the eSentire MDR portal has been optimized for mobile access. A dedicated customer success manager is available as part of the standard subscription. Customers have access to the same data, tools, and reporting as eSentire. An innovation worth mentioning here is the ability for customers to use natural language queries to search their own security data. The company will also support pre-sales proof of concept (POC) implementations. eSentire MDR complies with the principles and standards of ISO 15408, ISO 27001, PCI-DSS, SSAE SOC 2 TYPE 2, HIPAA/HITRUST, UK Cyber Essentials, GDPR, NIST, SIG Lite, and AITEC. The solution offers guaranteed data residency for the US, EU, and UAE.

eSentire MDR supports organizations of all sizes across 30 verticals seeking to improve their cyber resilience, especially finance, legal, critical infrastructure, healthcare, business services, and manufacturing. eSentire tailors its comprehensive MDR service to the needs and capabilities of in-house SOC and security teams. It boasts a strong AI-supported automated response capability and a rapid response time, with full cyber resilience score services to be available by the end of 2024.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Deployment</b>	Strong Positive	
<b>Interoperability</b>	Strong Positive	
<b>Usability</b>	Strong Positive	

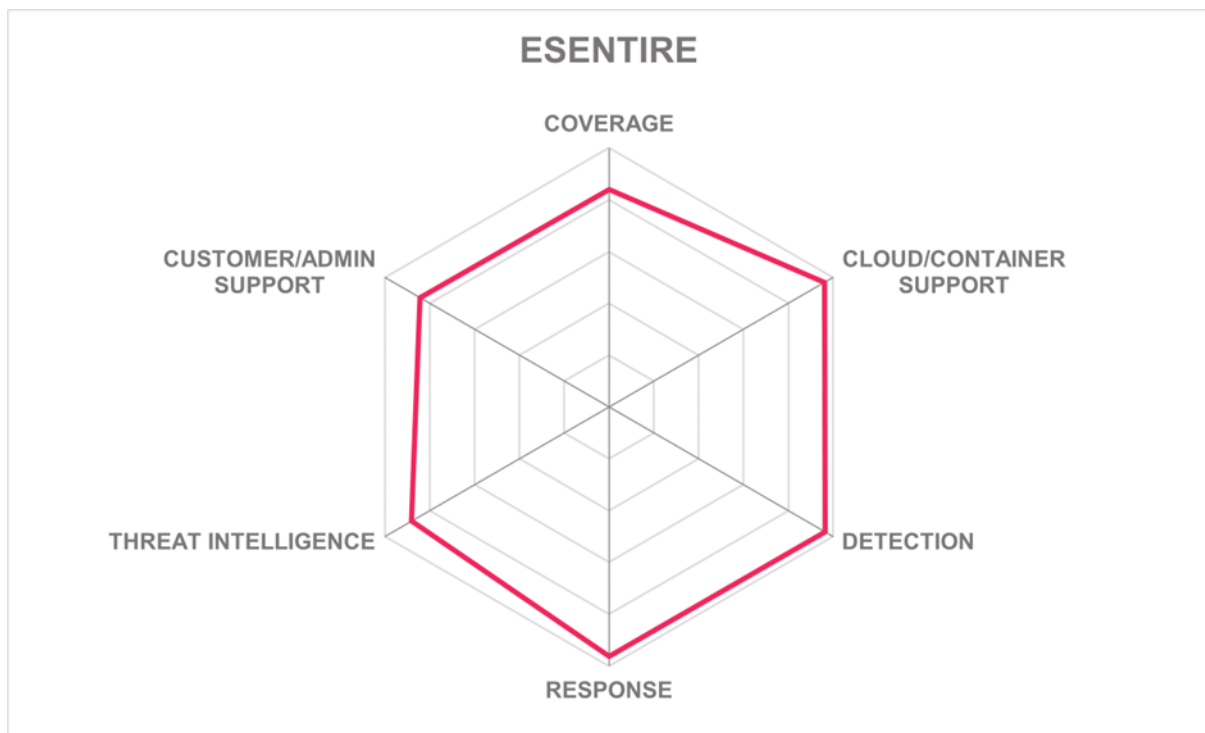
Table 8: eSentire's rating

**Strengths**

- Fast and flexible deployment
- Simple endpoint-based pricing model
- Strong channel ecosystem
- Comprehensive coverage of business IT environments
- Very strong threat intelligence capability
- Rapid response with a MTTC of 15 minutes

### Challenges

- Offers OOTB integrations with relatively few third-party EPDR and SIEM solutions
- Does not monitor all cloud services OOTB
- Does not include software patching functionality



## ESET – ESET PROTECT MDR

ESET is a private global cybersecurity solutions company founded in 1992 and headquartered in Bratislava, Slovakia, with offices in the US, Argentina, Brazil, Mexico, Canada, Mexico, the Czech Republic, Poland, UK, Germany, Italy, Romania, Singapore, Australia, Japan. There are 12 SOC teams across 10 SOCs in the US, UK, Netherlands, France, Spain, Italy, Germany, Slovakia, Japan, and Argentina. ESET has customers around the world, with most in the EMEA region and falling into the small and medium-sized enterprise category.

The 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 using AI, SIEM, and SOAR in combination with SOC supervision. ESET PROTECT MDR is available in two service tiers: ESET MDR (Standard) and ESET Detection & Response Ultimate.

The recently introduced ESET MDR (Standard) tier is tailored for small and medium businesses that need 24/7 monitoring and the ability to stop threats as soon as they are detected. It includes a dashboard showing all SOC activity and time to resolution of incidents, total number of incidents, and number of incidents with low, medium, and high severity. ESET Detection & Response Ultimate is for medium to large enterprises that want greater involvement in investigations, more control over response actions, and regular meetings to discuss security findings. Both tiers include 24/7 threat monitoring, threat hunting, triage, response, threat intelligence, behavior analytics, and customized reporting. ESET Detection & Response Ultimate adds deployment, configuration, and tuning services, historical and customized threat hunting, Digital Forensic Incident Response Assistance, a dedicated response lead, and additional support and context for MDR alerts, including an AI advisor to answer questions using natural language processing (NLP).

There is a simple per-seat, per-year pricing model, starting at the minimum of 25 seats for the ESET MDR (Standard) tier. SME customers can purchase seats in blocks up to 999. However, MSPs can sell any number of licenses for ESET MDR (Standard). ESET Detection & Response Ultimate is recommended for organizations with 1,000 seats or more.

The solution can be deployed quickly on premises, in the cloud (public and private), or in a hybrid model, depending on customer preferences or requirements. The solution is available directly to end user organizations, but also via MSSPs and channel partners.

The solution covers all main operating systems, including Android and iOS, and all main browsers.

ESET PROTECT MDR provides round-the-clock monitoring and analysis of all major business IT environments, but not including Edge computing environments, and provides detection and response services across all environments, including medical and industrial IoT devices, OT, and remote workers.

The solution does not include pre-built integrations for any third-party EPDR and NDR systems. There are pre-built integrations with three SIEM solutions (Microsoft Sentinel,

Elastic Security, and Splunk) but customers can create their own integrations via ESET PROTECT's open API or using syslog.

The solution provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It cannot identify data loss across cloud infrastructure, but it can detect and respond to threats to multi-cloud environments. It does not include CSPM, CWP, and vulnerability scanning of customer multi-cloud environments. ESET PROTECT MDR is able to scan containers during the building and deployment phases, using ESET Server Security for Linux.

ESET PROTECT MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, it can detect malicious executables before they run, and includes network intrusion detection capabilities. The solution also includes user and attacker behavior analytics, and can detect and report privilege escalation, but does not offer OOTB integrations with third-party IDS. ESET claims a Mean Time to Respond (MTTR) of 20 minutes.

The solution can take response actions regardless of the security technology customers already have in place. It features a single platform that can automatically respond to disrupt threats and includes a wide range of automated response actions. Additionally, it offers functionality for software patching. It blocks ransomware attacks before any data is encrypted or stolen for extortion, includes automated proactive threat hunting, provides more than 1,000 External Intelligence (EI) rules for incident response, and applies AI/ML for detecting anomalous behavior and identifying threats, but not for predictive threat hunting. ESET's Automatic Incident Creator uses AI and automation to correlate metadata and create incidents, while ESET's Automated Remediation for Detections uses predefined and regularly updated rules to mark common benign detections as "remediated". The solution provides its own SOAR functionality and comes with pre-built integrations for two third-party SOAR solutions (Microsoft Sentinel and Splunk).

The solution is supported by strong threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a dedicated threat hunting team that is backed by a global team of threat intelligence researchers, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The solution offers real-time threat intelligence integration.

ESET can provide on-site support in exceptional circumstances. The MDR solution can be used to outsource the SOC function entirely, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The solution includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and includes customizable reporting for business executives, technical teams, and compliance teams. It includes recommendations on improving cyber resilience and the services of a dedicated risk advisor and customer success manager, but does not include an ROI calculator. Tools for ASM are not available and customers do not have access to the same data as ESET. Potential customers can take advantage of a pre-sales trial period to see if the solution is a good fit. ESET MDR complies with the standards and principles of ISO



15408, ISO 27001, ISO 9001, PCI-DSS, HIPAA/HITRUST, LINCE, NIST Cybersecurity Framework, NORAM Cybersecurity Insurance, Cybersecurity Essentials, and ECSO Cybersecurity Made in Europe.

ESET PROTECT MDR supports organizations of all sizes (with tailored support for SMEs) and most verticals (including education, finance, insurance manufacturing, healthcare and government), especially organizations looking for fast response, strong threat intelligence, good compliance support, strong local language support, and comprehensive ransomware protection.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Positive	
<b>Deployment</b>	Strong Positive	
<b>Interoperability</b>	Neutral	
<b>Usability</b>	Strong Positive	

Table 9: ESET's rating

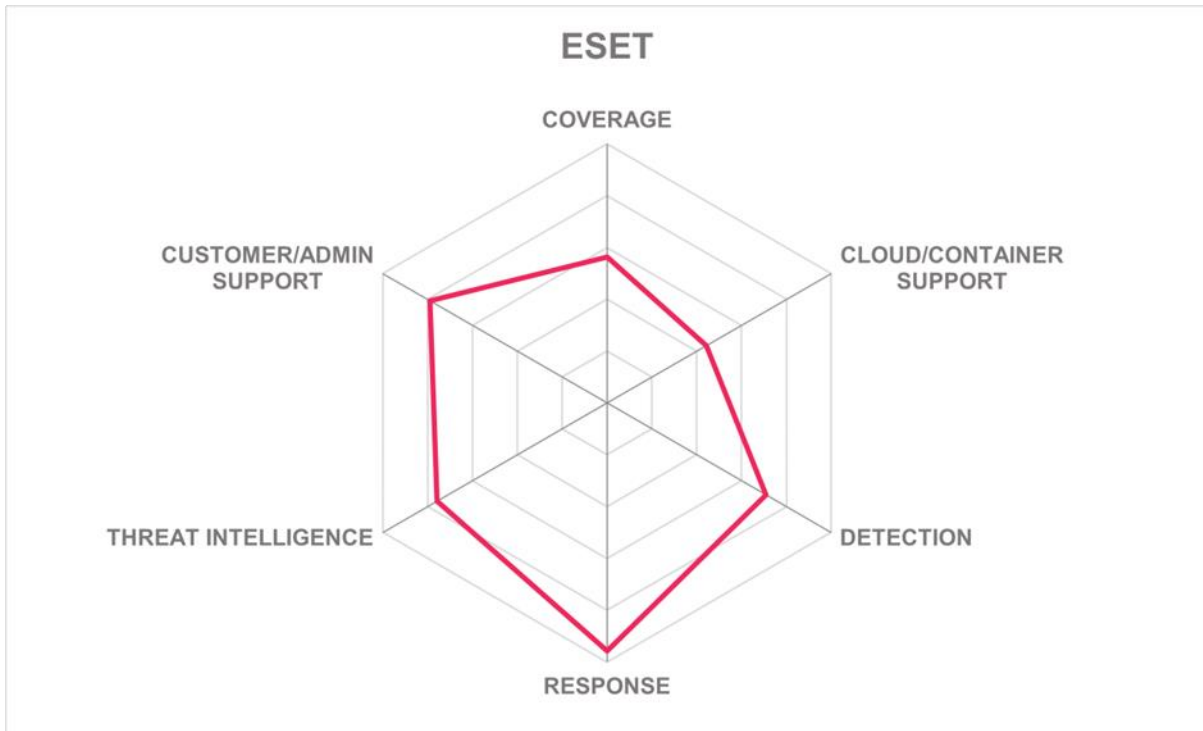
### Strengths

- Fully integrated, unified platform specifically designed for cloud-native workload security, and flexible and rapid deployment
- Simple pricing model
- New standard tier tailored to the needs of SMEs
- Cross-industry and multi-regional insights from 10 SOC locations
- Strong ransomware/extortion detection and blocking capabilities
- Very strong threat intelligence capabilities, especially within the EU
- Local language support and documentation available in most countries
- Fast response with a MTTR of 20 minutes
- NLP-based ESET AI advisor for MDR Ultimate customers
- Good support for compliance with security standards

### Challenges

- No MDR coverage of Edge computing environments
- No pre-built integrations for third-party EPDR or NDR solutions
- Does not include CSPM or CWP, but these are on the roadmap
- Few pre-built integrations with third-party SOAR solutions
- No mobile app for access to dashboards and status reports

Leader in



## Fortra – Alert Logic Managed Detection and Response

Fortra (formerly HelpSystems) is a private US cybersecurity and automation company founded in 1982 and based in Minneapolis, Minnesota, with offices across the US and in Canada, the UK, Germany, Spain, Switzerland, Australia, and Argentina. Fortra provides a growing range of cybersecurity solutions through acquisitions, including MDR, which is supported 24/7 by three SOC teams located in the US, Canada, and the UK. Most customers are in North America, followed by EMEA and fall into the mid-market category.

Alert Logic MDR uses the Fortra XDR Platform, which is in line with the company's plans to expand managed services to users, devices, servers, cloud, and SaaS. Longer term, Fortra plans to evolve the Fortra XDR Platform to integrate all security controls and XDR data sources to deliver a comprehensive range of services.

By leveraging the Fortra XDR Platform, the MDR service includes enhanced threat intelligence, dashboarding and reporting, threat hunting, and ML-based analytics to provide detection and response functionality across endpoints, networks, and cloud services in a single platform that is designed to integrate with existing security investments. In addition, the full MDR Enterprise service includes high-touch elements such as proactive tuning and detection optimization, security posture consulting, and regular security reviews.

Fortra uses a simple pricing model based on the number of nodes such as servers, clients, and network devices that the customer wants to protect. There is a once-off setup cost for new customers.

Fortra offers flexible deployment options with unlimited support on-premises, in the public cloud (AWS, Azure, or GCP), and hybrid deployments. Integrations with AWS control tower and SSM make deployment within AWS almost completely automated. Cloud-only deployments can be completed in 24 hours, but larger enterprises take 30 days on average, with most achieving basic value within 45 days, without ML training.

The solution is available directly to end-user organizations and through MSSPs and channel partners, with sales predominantly driven by the channel.

Alert Logic MDR covers Windows and Linux operating systems, but not macOS, Android, and iOS. It covers most of the main browsers.

The service provides continuous monitoring and analysis of all major business IT systems, including Edge computing environments, and provides detection and response services across several environments including remote and contract workers, but excluding IoT, IIoT, IoMT, and OT environments.

Alert Logic MDR includes pre-built integrations with relatively few third-party EPDR solutions but no NDR or SIEM solutions, relying instead on the XDR Platform's inherent capabilities.

The service provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services and can detect and respond to threats to multi-cloud

environments, but cannot identify data loss across cloud infrastructure. It also includes cloud security posture management and vulnerability scanning of customer multi-cloud environments, but does not include CWP. Alert Logic MDR can detect a limited number of threats to Kubernetes environments such as unauthorized access and compromised containers. However, it can handle logging and monitoring across multiple Kubernetes clusters and includes network traffic inspection at the individual container level. The service is able to monitor a limited number of cloud services for MDR purposes, namely Azure AD, Microsoft Office 365, and Salesforce.com.

Alert Logic MDR can detect and respond to a wide range of malicious activities, including RDP exploitation and evasive malware, but not insider threats. It also cannot detect and respond to phishing attacks in real time or detect or block malicious executables, but does include network intrusion detection capabilities, user and attacker behavior analytics, and the ability to detect and report privilege escalation. It offers OOTB integrations with third-party intrusion prevention systems (IPS) but not IDS. Alert Logic MDR comes with a 15-minute SLA for SOC incident management, covering incident creation, incident acknowledgment, data analysis and identification of IoCs, activity summary and remediation recommendations, execution of playbooks, and notification and escalation if required.

The service can take response actions regardless of what security technology customers already have, it can respond automatically to disrupt threats, it includes functionality for software patching, and it has a small range of automated response actions, namely isolating hosts/endpoints and blocking communications by IP and port. The service cannot block ransomware attacks before any data is encrypted. Although the focus of the service is on simple response playbooks for incident/threat response, if required, customers can access SOAR capabilities with custom, low-code workflows within the Fortra XDR Platform. There are no OOTB integrations with third-party SOAR products, but custom integrations are possible.

The service includes strong threat intelligence capabilities for advanced threat detection and risk mitigation, it has the support of a dedicated threat hunting team, provides regular reporting on emerging threats, and uses threat intelligence to train AI/ML models. The service offers real-time threat intelligence integration and uses a select set of third-party feeds to minimize overlaps and provide the broadest coverage, including input from Dark Web monitoring. The in-house threat intelligence capability is backed by a global team of researchers, integrates threat intelligence from across its customer base, and is able to track and profile threat actor groups through activity clustering as part of Fortra's threat hunting process.

On-site support is available for all customers, the service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, an ROI calculator, and the services of a designated team of cyber risk experts either as part of a higher-level subscription or as an optional extra. Tools for ASM are available as part of the standard subscription. There is a

mobile app that provides access to dashboards and status reports. Customer success team support is available as part of the standard subscription. Customers to the same data, tools, and reporting as Fortra. Potential customers can take advantage of a pre-sales trial period to assess if Alert Logic MDR is a good fit. The service complies with the standards and principles of ISO 27001, PCI-DSS 4.0, SSAE SOC 2 TYPE 2, HIPAA/HITRUST, UK Cyber Essentials, and TX-RAMP Level 2, and offers guaranteed data residency for the EU and US.

Alert Logic MDR supports organizations of all sizes, particularly mid-market companies with under 5,000 employees. It will especially appeal to organizations with complex IT environments and a low level of security maturity. It will also appeal to organizations seeking a single platform to manage multiple security solutions and organizations with distributed networks and serverless architectures or that fall into highly regulated industry sectors such as IT, banking and finance, manufacturing, and retail.

<b>Security</b>	Positive	
<b>Functionality</b>	Positive	
<b>Deployment</b>	Strong Positive	
<b>Interoperability</b>	Neutral	
<b>Usability</b>	Positive	

Table 10: Fortra's rating

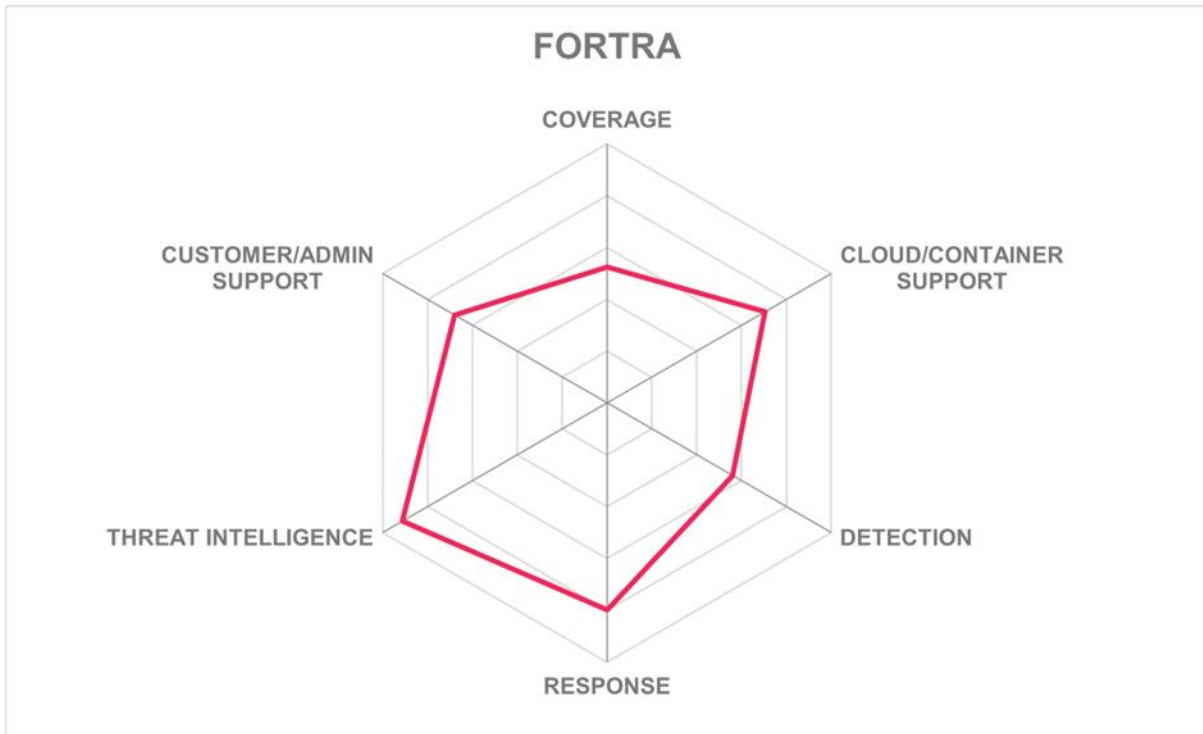
### Strengths

- Mature core MDR technology integrated into single platform
- 15-minute SLA for initial incident management
- Strong threat intelligence capability
- Good integration with existing security investments
- Enterprise MDR includes bespoke services
- Simple pricing model
- Flexible deployment options
- Fast AWS deployments due to strong integrations
- Service includes CSPM and ASM
- PCI-credited scanning vendor
- Mobile app for accessing dashboards and status reports

### Challenges

- Covers only Windows and Linux environments
- Does not cover internet-connected devices, mobile devices, and OT environments
- Does not prevent malware/ransomware execution
- Few integrations with third-party EPDR, NDR, and SIEM solutions
- Cannot identify data loss across cloud infrastructure
- Does not include CWP

- Can monitor only a few cloud services
- Limited number of automated response actions
- Support services available only in three languages and documentation available only in English.



## 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 also has an optional retainer, which can be used for a wide range of cyber risk management and preparedness services.

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 and agents installed on endpoints. Customers have the option of retaining all data on premises. Kroll can provide initial IR and monitoring capabilities within hours, with full MDR service onboarding within 28 to 42 days.

The solution is available directly to end user organizations, but also via MSSPs and channel partners. Kroll is using its partner program to provide full IR capabilities to MSP and MSSPs as well as expand to new regions, provide support in LATAM and APAC, provide regional regulatory and language support, and deliver concierge-style services.

The MDR service covers all main operating systems, including Android and iOS, and all main browsers.

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, OT, and remote workers. Kroll Responder has good visibility of email based on the high volume of business email compromise incidents it handles.

Kroll's MDR service includes pre-built integrations with most third-party EPDR solutions and NDR solutions. Any unsupported platforms can be integrated via a SIEM platform. There are also integrations with five SIEM solutions (Microsoft Sentinel, LogRhythm, Securonix, Splunk, and AT&T Alien Vault).

Kroll Responder provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also includes CWP and vulnerability scanning of customer multi-cloud environments but does not include cloud

security posture management. However, in 2024 Kroll plans leverage its partnership with Obsidian to augment its MDR support for cloud security, especially around SaaS applications. Kroll Responder can detect a wide range of threats to Kubernetes environments, and can handle logging and monitoring across multiple Kubernetes clusters. It can monitor most cloud services OOTB, but any others can be integrated via a SIEM platform.

The Kroll MDR service can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, it can detect malicious executables before they run, and includes network intrusion detection capabilities. The service also includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to detect and report privilege escalation activity.

The service can take response actions regardless of what security technology customers already have, it features a single platform that can respond automatically to disrupt threats, it includes a wide range of automated response actions, and it includes functionality for software patching. It also blocks ransomware attacks before any data is encrypted, includes automated proactive threat hunting, provides playbooks for incident response, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting. 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).

Kroll Responder includes strong threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a dedicated threat hunting team, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The service offers real-time threat intelligence integration and provides connectors for a wide range of threat intelligence sources, including Dark Web monitoring. The in-house threat intelligence capability is backed by a global team of researchers and Kroll maintains its own database of IoCs gathered from incident response activities.

On-site support is available for all customers, the service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The solution includes functionality to generate reports that map detected threats to MITRE ATT&CK tactics and techniques, and it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, an ROI calculator, and the services of a dedicated risk advisor as part of the standard subscription. Tools for ASM are available as an optional extra. There is a mobile app that provides access to dashboards and status reports. A dedicated customer success manager is available as part of the standard subscription. Customers have access to the same data, tools, and reporting as Kroll. Potential customers can take advantage of a pre-sales trial period to assess if Kroll Responder is a good fit. The service complies with the standards and principles of ISO 27001, SSAE SOC 2 Type 2, and UK Cyber Essentials, and offers guaranteed data residency for the EU and the US.



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.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Strong Positive
<b>Interoperability</b>	Positive
<b>Usability</b>	Strong Positive



Table 11: Kroll's rating

### Strengths

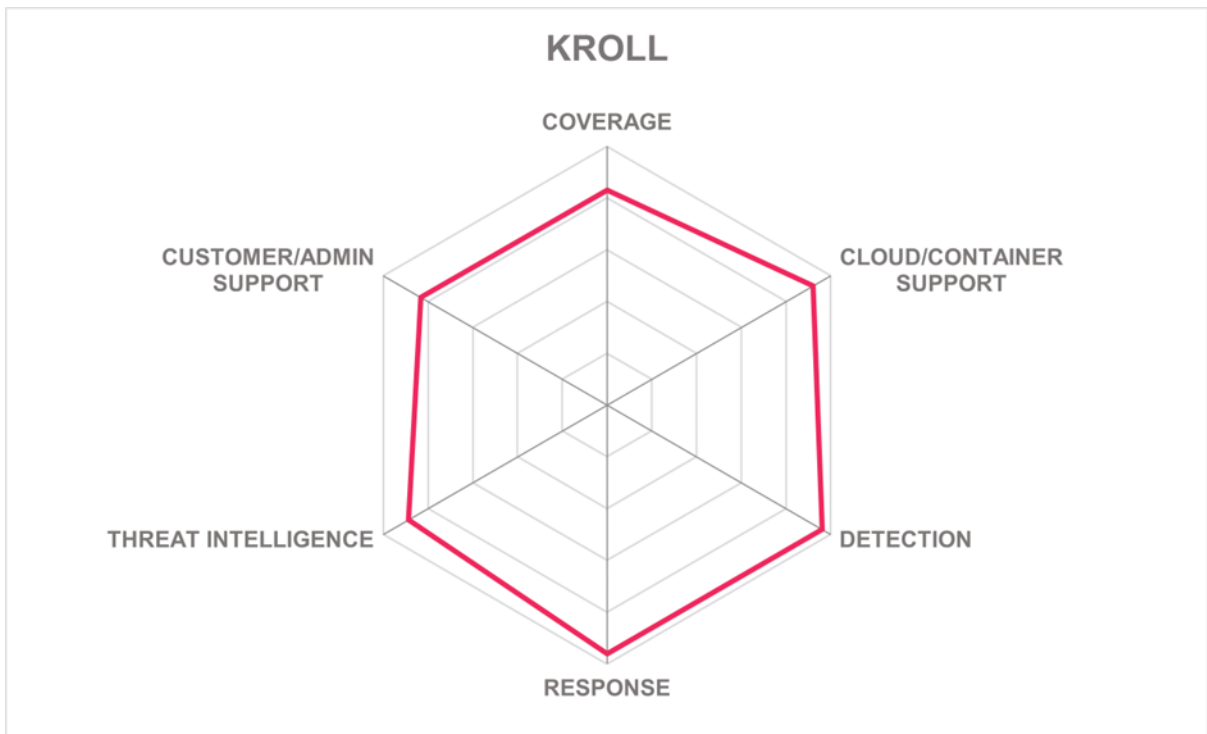
- Support for existing technology investments
- Rapid and flexible deployment options
- Comprehensive coverage of business IT environments
- Good support for cloud environments
- Comprehensive detection and response capabilities
- Strong threat intelligence capabilities
- Mobile app for access to dashboards and status reports

### Challenges

- Documentation is available only in English, but support services are available in English, Spanish, Portuguese, Italian, and Japanese
- Does not include cloud security posture management, but improved support for cloud security planned for 2024
- Does not include assistance in developing governance policies
- OOTB integrations with only five third-party SIEM solutions

Leader in





## Ontinue – ION Managed Extended Detection and Response (MXDR)

Ontinue is a private MDR services company established in 2023, with dual headquarters in Redwood City, California in the US, and Zurich, Switzerland. Originating as the MDR division of the Swiss-based cybersecurity company Open Systems, Ontinue was spun out as a separate entity to focus on specialized MDR services. Ontinue also has offices in Toronto and Vancouver, Canada; London, UK; and Delhi, India. The company's SOC operates on a follow-the-sun model, with team members working daytime shifts. Most customers are in the EMEA region followed by North America, and fall into the medium and mid-market categories.

Ontinue's ION Managed Extended Detection and Response (MXDR) is a 24/7 managed security operations service that is purpose-built for organizations that have standardized the Microsoft security stack (MS Defender and MS Sentinel). The ION MXDR service is underpinned by technology and expertise from Open Systems, Swiss-based data science company Sqooba (acquired in 2019), Microsoft services provider Born in the Cloud (acquired in 2020), and cybersecurity firm Tiberium, acquired in 2022 for its collaboration model based on Microsoft Teams. Ontinue's MXDR is built natively into MS Teams, which provides the main user interface, including all the standard MS Teams collaboration tools and channels across all devices. This eliminates the need for an additional MDR console or collaboration tools.

Pricing for Ontinue's ION services based on user and server counts. In addition to the ION MXDR service, Ontinue offers two add-on services: ION for Vulnerability Mitigation and ION for IoT Security. Microsoft Consulting Services from Ontinue are also available to help ION customers plan, deploy, and configure their Microsoft technology investments to maximize ROI.

Ontinue's MXDR is available as an agentless cloud-based managed service via MS Teams with tight integration with the MS Defender suite, which provides extended detection and response capabilities across on-premises and multi-cloud environments. Telemetry is aggregated in the customer's Microsoft Sentinel before being ingested by Ontinue's MXDR service. Ontinue's MXDR service is available directly to end user organizations and via channel partners. Customers interact with the service entirely through existing MS Teams instances, with Ontinue available as a Team. Deployment is fast, providing 24/7 coverage within one to five days and fully operational within 10 days. Ontinue runs a threat hunt for every new customer to uncover cyber hygiene issues, misconfigurations, and any threat actor activity. As part of onboarding, Ontinue conducts a Microsoft Sentinel log ingestion analysis and provides recommendations to optimize log ingestion based on a combination of security value and cost. Security posture improvement and modeling of customer environment, people, and processes also start at onboarding.

In addition to the high level of integration with Microsoft, including Windows, the service covers Linux and macOS, but it does not currently support Android and iOS.

The service provides 24/7 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 IoMT, IIoT, OT, and remote workers. Coverage of IoT and OT environments is limited, but under development.

As a dedicated Microsoft security product, the service is integrated with only one EPDR product, which is MS Defender for Endpoint. Similarly, the service is integrated only with one SIEM, which is MS Sentinel. Ontinue ION MXDR supports third-party NDR solutions through a combination of MS Sentinel's native connectors and the Advanced Security Information Model (ASIM) framework.

Ontinue MXDR provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, and can detect and respond to threats in multi-cloud environments. The Ontinue service offers limited data loss prevention (DLP) support through MS Defender for Office and MS Defender for Cloud Apps. It includes CWP and vulnerability scanning of customer multi-cloud environments, but only limited support for CSPM for Microsoft Azure, GCP, and AWS. The service can detect threats to Kubernetes using MS Defender for Cloud. Cloud services monitoring is supported using MS Defender for Cloud Apps and includes support for Microsoft O365, G Suite, Salesforce, Atlassian, Workday, ServiceNow, Dropbox, SAP, and GitHub.

The Ontinue MXDR service can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. The service includes support for network intrusion detection capabilities by integrating with third-party IDS via MS Sentinel. It can also detect and respond to phishing attacks in real time using MS Defender for Endpoint. Additional support for user-reported phishing emails is on the roadmap. The service includes user and attacker behavior analytics, and can detect and report privilege escalation.

The focus on supporting Microsoft security customers means that MS Defender is required to enable the ION MXDR service to detect threats across the entire IT estate and respond automatically to disrupt threats. Automated response actions are relatively limited, but include the ability to trigger the Automated Investigation and Response (AIR) capability of MS Defender for Endpoints, isolate hosts and endpoints, block communications by IP and port, block IoCs, mark users as compromised, restrict app execution, and run antivirus. The service does not include software patching functionality. The service can block ransomware attacks before any data is encrypted, it includes automated proactive threat hunting, it provides playbooks for incident response, and applies AI/ML for blocking anomalous or suspicious activity and identifying threats, but not for predictive threat hunting. The service does not provide its own SOAR functionality, but has a high level of integration with MS Sentinel and includes customizable automated escalation and communication paths for coordinated incident response.

The service includes threat intelligence capabilities for advanced detection and risk mitigation and has the backing of a dedicated threat hunting team, which carries out continuous threat hunting using Ontinue's library of IoCs as well as regular structured, hypothesis-driven threat hunting based on observations in the wild. ION MXDR uses a wide range of sources to train AI/ML models, but these do not include threat intelligence feeds.

The service leverages the integrated threat intelligence feeds of the Microsoft Defender suite, and augments this with feeds from selected sources, including Recorded Future, Virus Total, and Joe Sandbox. Ontinue's Threat Intelligence team actively assesses potential gaps in intelligence and curates feeds to provide customers with regular reporting on emerging threats. The in-house threat intelligence capability is supported by a global team of researchers as well as threat intelligence from Dark Web monitoring.

All support services are remote, the service can be used to outsource the SOC function, and it enables collaboration with and support for in-house security teams at small to medium-sized organizations with less mature security operations programs. The service can also be used to augment customer SOC teams at large, mature organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and it includes customizable reporting for business executives and technical teams, but not compliance teams. It includes recommendations on improving cyber resilience and a variety of ROI tools, including an MS Sentinel cost optimization calculator, a security tool consolidation calculator, and an ION ROI report as part of the quarterly review process. At no additional cost, each customer is assigned a designated customer success manager and a cyber advisor to assist with additional security guidance and to work with customers to improve their security posture and reduce exposure proactively, based on a five-tier security posture improvement framework. Tools for ASM are available as part of the standard subscription. Because ION MXDR uses MS Teams as its primary UI, the service's dashboards, communication channels, and AI assistant are available anytime, anywhere. There is an "Engage" button in the UI that connects customers to a senior SOC analyst within 15 minutes. There is also a web-based portal as an alternative to the MS Teams interface for customers who prefer not to use Teams. ION MXDR leverages customers' existing MS Sentinel instance, which means customers retain their data at all times – including log data of every action. However, customers do not have access to the same tools as Ontinue. These are all contained within the AI-supported ION Workbench, which is designed to make Ontinue's cyber defenders as effective and efficient as possible so that the majority of incidents can be resolved without customer involvement. Ontinue does not provide potential customers with a pre-sales trial period to allow them to assess if ION MXDR is a good fit. The service complies with the standards of ISO 27001, ISO 27017, and ISO 2018, and offers guaranteed data residency for the EU and Switzerland.

ION MXDR is suitable for medium and large enterprises using MS Defender, particularly those also leveraging MS Entra and MS Sentinel, with a low to mid security maturity level, fewer than 10 internal SOC staff, and a focus on proactive, continuous security improvement. It is well-suited for organizations in industries such as manufacturing, finance, retail, technology, healthcare, and insurance.

<b>Security</b>	Positive	
<b>Functionality</b>	Positive	
<b>Deployment</b>	Positive	
<b>Interoperability</b>	Neutral	
<b>Usability</b>	Neutral	

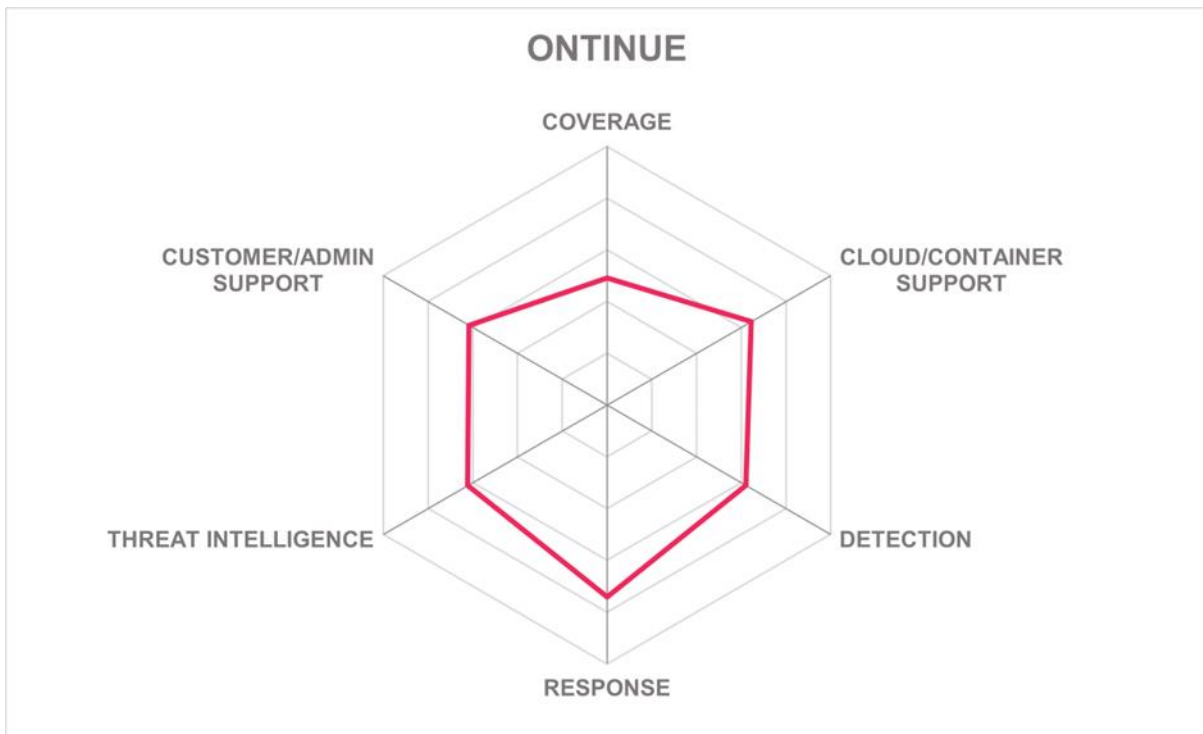
Table 12: Ontinue's rating

### Strengths

- Specialized support for the Microsoft security stack
- MS Teams is the main user interface, eliminating proprietary console
- Easy collaboration, continually improving as MS Teams evolves
- Works with MS Copilot for Office 365
- Simple pricing model aligned to Microsoft users with no hidden fees
- 24/7 coverage in one to five days and fully operational within 10 days
- High level of integration with MS Defender and MS Sentinel
- Dedicated cyber advisors and AI support highly tailored service
- Customized automation of many Tier 1 SOC responsibilities
- ION MXDR available anytime and anywhere via MS Teams or web portal

### Challenges

- No coverage of mobile devices or Android and iOS
- Limited IoT and OT coverage, but currently under further development
- Does not integrate with any non-Microsoft SIEM or EPDR solutions
- Limited DLP support across cloud infrastructure
- Limited managed CSPM support for Microsoft Azure, GCP, and AWS
- No on-site support services anywhere in the world
- Support services available only in English and German



## Optiv – Optiv MDR

Optiv is a private cybersecurity advisory and solutions company that partners with organizations to advise, deploy, and operate complete cybersecurity programs from strategy and managed security services to risk, integration, and technology services, including MDR. Founded in 2015, Optiv is headquartered in Denver, Colorado, and has offices across the US and in Mississauga, Canada, with SOCs in Leawood, Kansas in the US and Bangalore in India. Most customers are in North America and fall into the mid-market segment.

The Optiv MDR service combines the SIEM (formerly Google Chronicle) and SOAR (formerly SIEMplify) capabilities of the Google SecOps Platform with Optiv's data management layer built-in partnership with Cribl, Optiv's SOAR playbooks, processes, IT service management (ServiceNow), and Optiv's client portal. The Optiv MDR Platform is designed to enable the interoperability of customers' existing hybrid security infrastructure to correlate events, identify incidents, and to respond to and neutralize threats.

The pricing model for the core MDR service is based on the amount of data processed by the service, measured in gigabytes per day, but also includes 40 hours of Active Defense a year to bridge the gap between confirmation of an incident and engagement with an internal, Optiv, or third-party IR team. The services of dedicated threat hunter, technical management, and an IR retainer are all optional extras.

Optiv MDR is a cloud-based service with log collection mainly through APIs, but Optiv can install a virtual machine (VM) on premises for any log sources that do not support API collection. Deployment, including onboarding, assessment, and gap analysis, typically takes up to 30 days. The service is available from Optiv directly to end user organizations alongside a wide range of complementary cybersecurity services supported by a team of engineers that enables deep integration with existing cybersecurity technologies for maximum benefit.

The service covers all main operating systems, including Android and iOS.

Optiv MDR provides 24/7 monitoring and analysis of all major business IT environments and systems, including Edge computing environments, and provides detection and response services across virtual environments, company datacenters, remote workers, and contract workers, but not medical and industrial IoT devices and OT.

Optiv MDR includes prebuilt integrations with 15 third-party EPDR and 15 NDR solutions. Although the platform includes a native SIEM, the service does offer prebuilt integrations for seven third-party SIEM solutions (Micro Focus ArcSight, MS Sentinel, Exabeam, Elastic Security, FireEye Helix, IBM QRadar, and Splunk).

The service provides continuous monitoring and analysis of cloud applications and data stores, but does not provide detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. However, it does not include CSPM, CWP, or vulnerability scanning of customer multi-cloud environments. Optiv MDR can detect a wide range of threats to Kubernetes environments,



and can handle logging and monitoring across multiple Kubernetes clusters. It can monitor all major cloud services OOTB.

The service can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, it can detect malicious executables before they run, and includes network intrusion detection capabilities. The service also includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to detect and report privilege escalation.

Despite its aims to enable organizations to get the most out of existing investments, Optiv may advise adjustments to security tooling, depending on the gap analysis during onboarding. The service features a single platform that can respond automatically to disrupt threats, and it includes a range of automated response actions. It does not include functionality for software patching, but can block ransomware attacks before any data is encrypted when paired with an EDR technology. It includes automated proactive threat hunting, provides playbooks for incident response, and applies AI/ML in various ways, including predictive threat hunting, retrospective threat hunting (up to 365 days), and prevalence analysis to distinguish between common and rare events to help identify truly malicious activity. The service provides its own SOAR functionality, former called SIEMplify. There are no prebuilt integrations for any third-party SOAR solutions, but Optiv can build custom integrations if necessary.

Optiv MDR includes threat intelligence capabilities with the support of a threat hunting team, automated threat hunting, and a global threat intelligence team. It provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The service offers real-time threat intelligence integration and provides connectors for a good range of threat intelligence sources, but does not include Dark Web monitoring for threat intelligence.

Optiv MDR provides on-site support only in North America through incident response services. The MDR service can be used to outsource the SOC function, and it enables collaboration with and support from customer SOC teams at large, mature organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience and optional ROI reporting. The services of a dedicated customer success manager are part of the standard offering, but not the services of a dedicated risk advisor. This is available as an optional extra. ASM tools are also available only as an add-on. There is no mobile app, but the customer portal is web-based and has been optimized for mobile devices. Customers have access to the same data, tools, and reporting as Optiv. Highly qualified prospects can take advantage of a pre-sales trial period to assess if Optiv MDR is a good fit. The service complies with the standards and principles of ISO 27001, SSAE SOC 2 TYPE 2, PCI-DSS, HIPAA/HITRUST, US FedRAMP, UK Cyber Essentials, and Germany C5. Optiv MDR offers guaranteed data residency for the EU and the US.

Optiv MDR supports organizations of all sizes and most verticals, particularly manufacturing, insurance, and finance. It will appeal to organizations looking for integrated complementary

security technologies such as EDR and managed services for privileged access management (PAM), SIEM, vulnerability management, and endpoint management.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Positive	
<b>Deployment</b>	Positive	
<b>Interoperability</b>	Strong Positive	
<b>Usability</b>	Positive	

Table 13: Optiv's rating

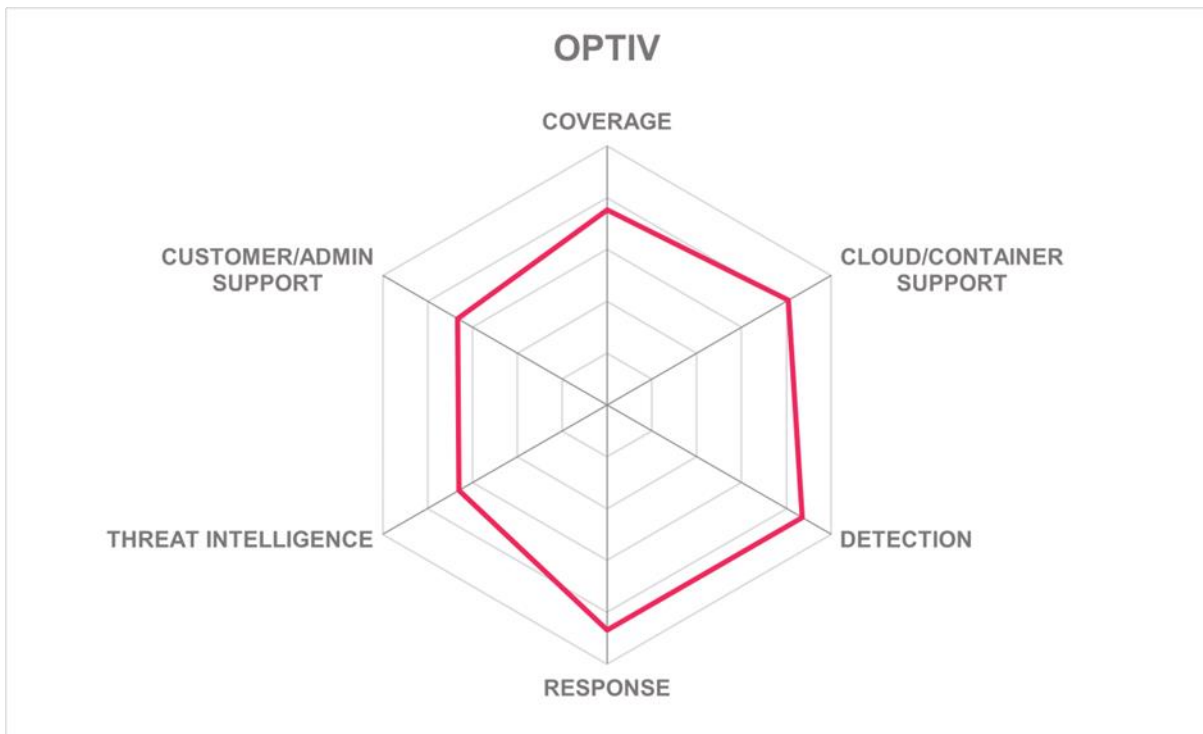
### Strengths

- Based on Google SecOps Platform
- Simple pricing model based on the amount of data processed by the service
- Service designed to work with existing cybersecurity investments
- Active Defense to provide emergency initial response to incidents
- Good integration with third-party security solutions
- Excellent coverage of cloud services and Kubernetes environments
- Strong SIEM and AI capabilities derived from Google SecOps Platform.
- Global threat intelligence team
- Strong support for compliance with security standards

### Challenges

- Does not cover medical and industrial IoT devices and OT
- Does not include CSPM, CWP, or multi-cloud vulnerability scanning
- No functionality for software patching
- No prebuilt integrations with any third-party SOAR solutions
- Support and documentation available only in English





## Proficio – ProSOC MDR

Proficio is a private cybersecurity services company founded in 2010 and headquartered in Carlsbad, California, specializes in providing MDR, managed security services (MSS), and SOC services. It has SOCs in Carlsbad (US), Barcelona (Spain), and Singapore. Most customers are in North America, and fall into the mid-market and enterprise segments.

Proficio provides two models for delivering MDR including a hosted cloud-based ProSOC MDR platform and a Managed SIEM and SOC Services model supporting a customer owned Splunk or Microsoft Sentinel platform. The latest version of Proficio’s ProSOC MDR hosted model is a next generation SIEM/XDR platform built on Elastic Search and ServiceNow. ProSOC MDR 3.0 includes AI-assisted threat discovery, and an AI assistant for response, remediation, trend analysis, and reporting. It also provides enhanced timeline and kill chain visibility.

Proficio’s pricing can be per user, per node, or based on volume of log ingestion depending on the combination of services provided with MDR, with a fixed annual cost on a contract basis. Proficio’s Active Defense XDR automated response, vulnerability management, cyber exposure monitoring, breach and attack simulation, 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 is entirely cloud based for rapid and easy scaling, and does not use any sensors or agents. Proficio collects and analyzes data from hundreds of log source types including network, endpoint, identity, SaaS, cloud via API, and syslog. If, however, 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 deployments typically take 30 days. The service is available directly to end user organizations, but also via MSSPs and channel partners.

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

The service provides 24/7 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, OT, and remote workers.

ProSOC MDR includes prebuilt integrations with most third-party EPDR solutions and many NDR products, with custom integrations available for an additional fee. There are also OOTB integrations for a select set of SIEM solutions (Micro Focus ArcSight, MS Sentinel, Elastic Security, and Splunk).

The service provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also includes CSPM,

CWP, and vulnerability scanning of customer multi-cloud environments. ProSOC MDR can detect a wide range of threats to Kubernetes environments, excluding misconfigurations, and can handle logging and monitoring across multiple Kubernetes clusters. It can monitor most cloud services OOTB, but custom integration is available for all others for a fee.

ProSOC MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, and includes network intrusion capabilities. The service includes user and attacker behavior analytics, supported by ML and threat intelligence, integrations with third-party IDS, and the ability to detect and report privilege escalation.

The service features a single platform that can respond automatically to disrupt threats, it includes a fairly wide range of automated response actions, and it includes functionality for software patching. Proficio claims response times of under three minutes. ProSOC MDR blocks ransomware attacks before any data is encrypted, includes automated proactive threat hunting, provides playbooks for incident response, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting. The service provides its own SOAR functionality as well as OOTB integrations with six third-party SOAR solutions (Fortinet FortiSOAR, MS Sentinel, Palo Alto XSOAR, ServiceNow, Splunk, and ThreatConnect). Custom integrations are available for a fee.

ProSOC MDR includes threat intelligence capabilities for advanced threat detection and risk mitigation, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The service offers real-time threat intelligence integration and provides connectors for several threat intelligence sources. Additional threat feeds in STIX/TAXII format can be integrated for a fee. ProSOC MDR is supported by a global team of threat intelligence researchers and includes Dark Web monitoring or cyber threat intelligence. Customers have the option to enhance ProSOC MDR with Proficio's Cyber Exposure Monitoring service, which includes digital risk monitoring, external ASM, and Dark Web risk monitoring.

On-site support services are available in North America, EMEA, and APAC. The service can be used to outsource the SOC function, essentially providing SOCaaS. It enables collaboration with and support for customer SOC teams at large organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, an ROI calculator, risk score benchmarking, and the services of a dedicated risk advisor as part of the standard subscription. Tools for ASM are available as an add-on. A dedicated customer success manager is available as part of the standard subscription. Customers have access to the same data, tools, and reporting as Proficio. They do not offer potential customers a pre-sales trial period to assess if ProSOC is a good fit. The service complies with the standards and principles of ISO 27001 and SSAE SOC 2 TYPE 2. Proficio is licensed by Singapore's Cyber Security Agency and offers guaranteed data residency for the US, EU, Singapore, and Australia.

Proficio’s ProSOC MDR supports organizations of all sizes and verticals, especially those that want to outsource their SOC and are seeking flexible, scalable, and highly tailored MDR services with rapid and proactive automated threat response capabilities.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Deployment</b>	Positive	
<b>Interoperability</b>	Strong Positive	
<b>Usability</b>	Strong Positive	

Table 14: Proficio’s rating

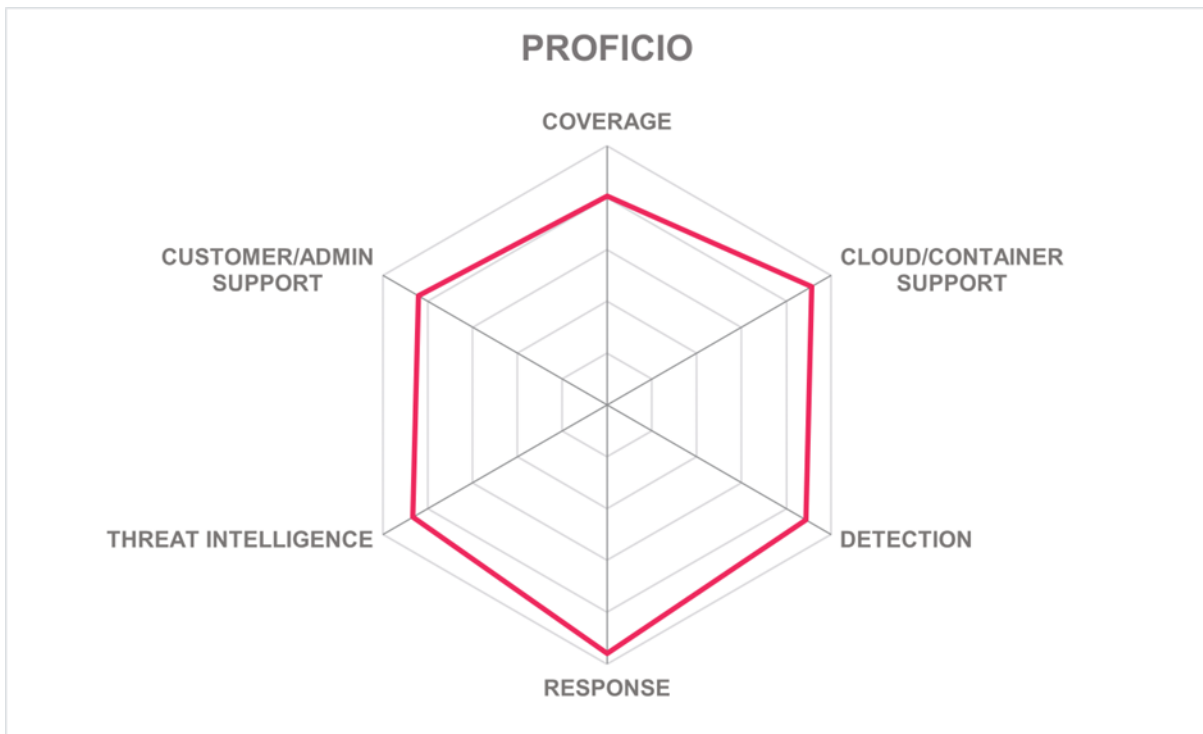
**Strengths**

- Rapid and easy scalability
- No additional sensors or agents needed beyond current EPDR/NDR/XDR
- Good MDR coverage of cloud and container environments
- Fast response to threat detections
- Proactive and automated threat containment
- On-site support available in North America, EMEA, and APAC
- Good and extensible threat intelligence capabilities
- Strong support for cloud computing environments

**Challenges**

- Limited number of OOTB third-party SIEM integrations
- Support services available only in English, Spanish, and Chinese
- Documentation available only in English and Spanish
- No pre-sales trial period





## ReliaQuest – ReliaQuest GreyMatter

ReliaQuest, a privately held US-based cybersecurity technology company, was founded in 2007 and is headquartered in Tampa, Florida. It has security operations across six technical operations centers located in Tampa, Florida; Las Vegas, Nevada; Salt Lake City, Utah (US); Dublin, Ireland; London, UK, and Pune, India. ReliaQuest serves companies of all sizes, with a focus on mid-sized and large businesses. The majority of its customers are based in North America, particularly the US, followed by the EMEA region.

ReliaQuest's MDR services are enabled by GreyMatter, a cloud-based, AI-supported security operations platform, built on an open XDR architecture. Pricing for the GreyMatter platform and services is determined by the number of endpoints and cloud workloads. Customers can use any supported technology they own for detection, investigations, and response actions through GreyMatter at no additional cost. Additional capabilities like the new Phishing Analyzer and Digital Risk Protection services will scale based on the number of inboxes and users, respectively.

Deployment options are either fully cloud-based or hybrid, with some on-premises components, such as software installed on enterprise hardware or virtual appliances. ReliaQuest offers a four-phase onboarding process, typically completed within one to six weeks. Customers gain access to the GreyMatter platform and ReliaQuest's threat intelligence summaries within the first 24 hours of deployment. The service is available directly to end user organizations, but also via channel partners.

The MDR service covers all main operating systems, including Android and iOS, and all main browsers.

The service provides 24/7 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, OT, and remote workers.

ReliaQuest's MDR service includes integrations with most third-party EPDR and NDR solutions, either directly or via a log platform. There are also integrations with nine SIEM solutions, including Microsoft Sentinel, Exabeam, LogRhythm, Splunk, and Sumo Logic.

GreyMatter provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also integrates with CSPM, CWP, and vulnerability scanning tools in multi-cloud environments. GreyMatter can detect a wide range of threats to Kubernetes environments, and can handle logging and monitoring across multiple Kubernetes clusters. The platform can monitor most cloud services OOTB and integrates with multiple cloud security tools such as Wiz, Prisma, Defender for Cloud, and Orca.

GreyMatter can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and



respond to phishing attacks in real time, it can detect malicious executables before they run, and includes network intrusion detection capabilities through third parties. The service includes user and attacker behavior analytics, and can integrate with a wide range of EUBA and related technologies due to its open-XDR approach. It also includes integrations with third-party IDS, and the ability to detect and report privilege escalation. ReliaQuest claims a MTTC of under five minutes, crediting this achievement to the use of automation and the integration of AI, utilizing Retrieval-Augmented Generation (RAG) models for greater accuracy, alongside automation and an enhanced 'analyst experience' through the introduction of advanced AI-enabled support tools and a streamlined user interface (UI).

The service can take response actions regardless of what security technology customers already have, it features a single platform that can respond automatically to disrupt threats, and it includes a wide range of automated response actions, automated proactive threat hunting, and playbooks for incident response. However, it does not include functionality for software patching or predictive threat hunting, and it cannot block ransomware attacks before any data is encrypted.

GreyMatter provides its own SOAR functionality and has built-in capabilities for alert enrichment, response workflows, and security incident management. It also comes with integrations for six third-party SOAR solutions (Exabeam, LogRhythm, Palo Alto Networks XSOAR, ServiceNow, Splunk, and Swimlane). ReliaQuest follows a bi-directional API integration approach to speed up ingestion of data for analysis and for triggering response actions from within the GreyMatter Platform.

GreyMatter includes strong threat intelligence capabilities for advanced threat detection and risk mitigation, boosted by the 2022 acquisition of digital risk protection firm Digital Shadows. This capability is supported by a dedicated threat hunting team that carries out proactive hunts, retroactive hunts, and ad-hoc hunts based on emerging threats. The service provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The service offers real-time threat intelligence integration and provides connectors for at least 10 threat intelligence sources. It is able to consume any other threat intelligence service that provides an API. The in-house threat intelligence capability is backed by a diverse global team of researchers who can cover more than 20 languages.

The solution includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations for improving cyber resilience, an ROI calculator, and the services of a dedicated risk advisor and customer success manager as part of the standard subscription. Tools for ASM are available as an add-on. There is a mobile app that provides the ability to review alerts, run response actions, and access dashboards and status reports. ReliaQuest reports an increasing use of the mobile app as end users seek to improve response times. Customers have access to the same data, tools, and reporting as ReliaQuest. Potential customers can take advantage of a pre-sales trial period to assess if GreyMatter is a good fit. The service complies with the principles and standards of ISO 27001, PCI DSS, SOC 2 type 2, and HIPAA/HITRUST. It offers guaranteed data residency for the EU, US, and Canada.

ReliaQuest's MDR service supports organizations of all sizes, from small businesses to large enterprises, across various industries, with a particular focus on finance and government. The solution is ideal for organizations needing seamless integration with legacy security tools or seeking to maximize the ROI on their existing security technology investments.

<b>Security</b>	Strong Positive
<b>Functionality</b>	Strong Positive
<b>Deployment</b>	Positive
<b>Interoperability</b>	Strong Positive
<b>Usability</b>	Strong Positive



Table 15: ReliaQuest's rating

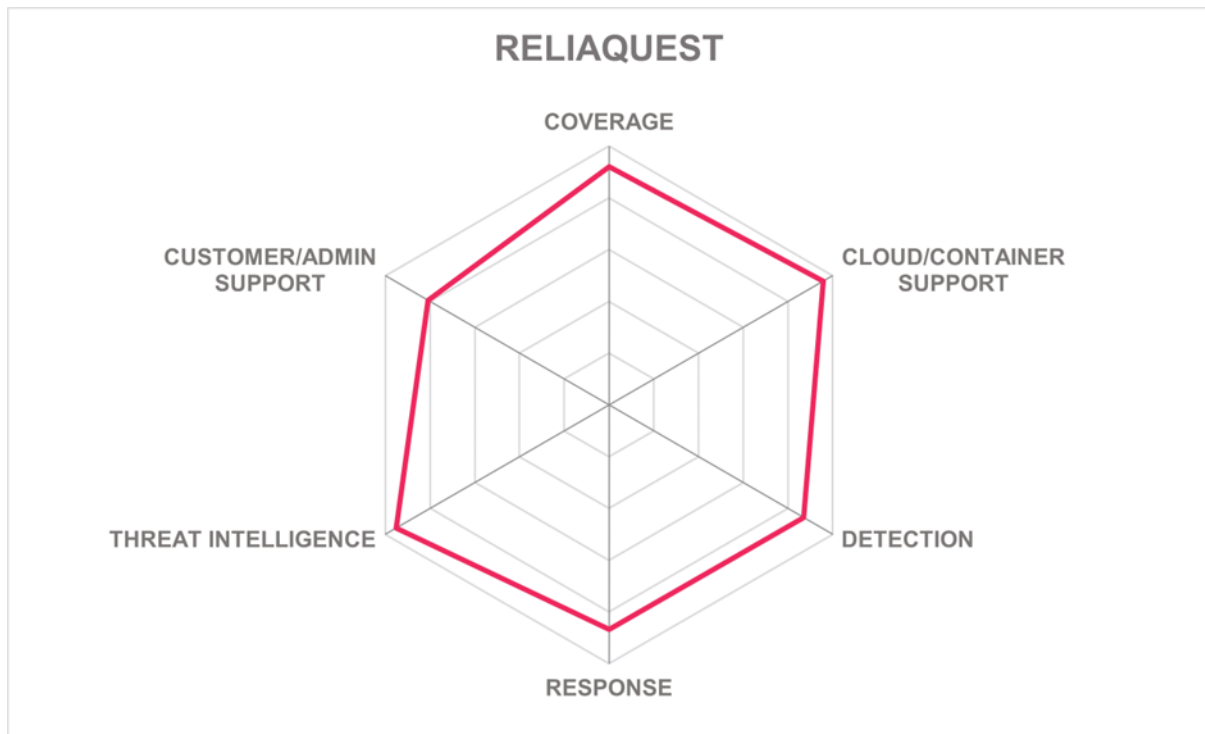
### Strengths

- Good coverage of all main business IT environments
- Prebuilt integrations for EPDR, NDR, and SIEM solutions
- Excellent MDR coverage of cloud and container environments
- Can detect and respond to a wide range of malicious activity
- Provides its own SOAR functionality
- MTTC of less than five minutes
- Bi-directional API integration
- Good threat detection capabilities
- Includes the services of a dedicated risk advisor and customer success manager
- Mobile app for access to dashboards and status reports

### Challenges

- Does not include functionality for software patching
- Cannot block ransomware attacks before any data is encrypted
- Does not include predictive threat hunting
- Provides support services only in English and Spanish
- Documentation available only in English





## 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, Germany, 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 has revised and simplified its MDR services with two MDR service packages: Sophos MDR Essentials and Sophos MDR Complete. Both packages offer 24/7 threat monitoring and response, weekly and monthly reporting, monthly intelligence briefings, threat hunting, and threat containment. In addition, MDR Complete offers root cause analysis, a \$1M breach protection warranty, and unlimited full-scale incident response, including a dedicated incident response lead. However, MDR Essentials customers can also get full incident response with a 12-month or multi-year IR services retainer, including an initial vulnerability scan across external assets and an incident readiness report. For both packages, there is an optional Managed Risk add-on service in partnership with Tenable. This is a new service aimed at threat prevention through risk management based on detections of vulnerabilities. The service is aimed at increasing attack surface visibility, providing continuous risk monitoring, vulnerability prioritization, and fast risk identification.

Sophos MDR is licensed based on the number of users and servers (physical and virtual) in an organization. Deployment is mainly as a cloud-based service on top of the core Sophos Central SaaS Platform, with the XDR component deployed as an agent on endpoints and servers in the customer's environment. The agent can run alongside third-party EPDR systems to gain visibility into non-Sophos-managed systems and enable MDR analysts to run real-time investigations and take actions to contain threats.

Sophos MDR provides third-party integrations that use either a REST API connector, or a VM that acts as a log collector, depending on the integrated product. API-based integrations with Microsoft solutions, Google Workspace, and third-party endpoint security products, are included at no additional cost. Sophos NDR requires an appliance that connects to a SPAN port to capture packet data; typical NDR implementations take between a week and a month.

The service is available directly to end user organizations, but also through MSSPs and channel partners, and provides coverage of all main operating systems, including Android, iOS, and ChromeOS via the Sophos Chrome Security extension. It also covers all main browsers.

Sophos MDR provides 24/7 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, OT, and remote workers. In the past year, Sophos has added new integrations for firewall, network security, email security, productivity, and identity solutions and introduced integrations for many backup and recovery solutions. Sophos has also focused on leveraging the Microsoft Management Activity API and Graph Security API to provide additional support to customers

with Microsoft licenses, especially BEC detection capabilities, which are available to holders of all types of Microsoft licenses. Customers with MS business premium licenses and above also benefit from Sophos detections for account takeover (ATO) and identity threats.

Sophos MDR includes pre-built integrations with all major third-party EPDR solutions, but only two non-Sophos NDR solutions: Darktrace and Vectra Cognito. There are no pre-built integrations for SIEM solutions, but the Sophos open API enables third-party SIEMs to ingest alerts from the Sophos Central SaaS Platform.

The service provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also includes CSPM, CWP, and vulnerability scanning of customer multi-cloud environments, but it is not able to detect any specific threats to Kubernetes environments and cannot handle logging and monitoring across multiple Kubernetes clusters. The service can monitor Microsoft Office 365, Microsoft Defender for Cloud Apps, Microsoft Entra ID Protection, and Google Workspace. The service can also ingest activity logs from Amazon Web Services, Microsoft Azure, and Google Cloud Platform environments

Sophos MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect and respond to phishing attacks in real time, it can detect malicious executables before they run, it includes network intrusion detection capabilities and OOTB integration with third-party IDS, and can detect and report privilege escalation. It also includes attacker behavior analytics, which is used to improve detections, but does not include user behavior analytics.

Sophos MDR can take response actions regardless of what security technology customers already have, it features a single platform that can respond automatically to disrupt threats, it includes a good range of automated response actions, and it includes vulnerability management services. It also blocks ransomware attacks before any data is encrypted, includes automated proactive threat hunting, provides playbooks for incident response, and applies AI/ML for detecting anomalous behavior, identifying threats, and for predictive threat hunting. The solution provides its own SOAR functionality, and consequently does not come with integrations for any third-party SOAR solutions.

Sophos MDR includes threat intelligence capabilities for advanced detection and risk mitigation, includes the support of a dedicated threat hunting team, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The service offers real-time threat intelligence integration and provides connectors for a wide range of intelligence sources. The service is backed by a global team of threat intelligence researchers and includes SophosLabs Intelix, a cloud-based threat intelligence and threat analysis platform. The MDR SecOps team uses threat intelligence from intelligence sharing communities and other open-source information, but the service does not include Dark Web monitoring for threat intelligence.

On-site support is available for all customers if necessary. The service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and includes customizable reporting for business executives and technical teams, but not compliance teams. It includes recommendations on improving cyber resilience, and an ROI calculator. The services of a dedicated risk advisor and ASM functionality are available only as optional extras. There is no mobile app to access dashboards and status reports. A dedicated customer success manager is available only under the MDR Complete package. Customers have access to the same data, tools, and reporting as Sophos. Potential customers can take advantage of a pre-sales trial to assess if Sophos MDR is a good fit. The service complies with the standards and principles of ISO 27001, PCI-DSS, SSAE SOC 2 TYPE 2, and HIPAA/HITRUST. It also offers guaranteed data residency for the EU and the US.

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 and is designed to work with existing security tools, especially those organizations lacking security expertise and dedicated SecOps teams.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Deployment</b>	Strong Positive	
<b>Interoperability</b>	Positive	
<b>Usability</b>	Strong Positive	

Table 16: Sophos's rating

### Strengths

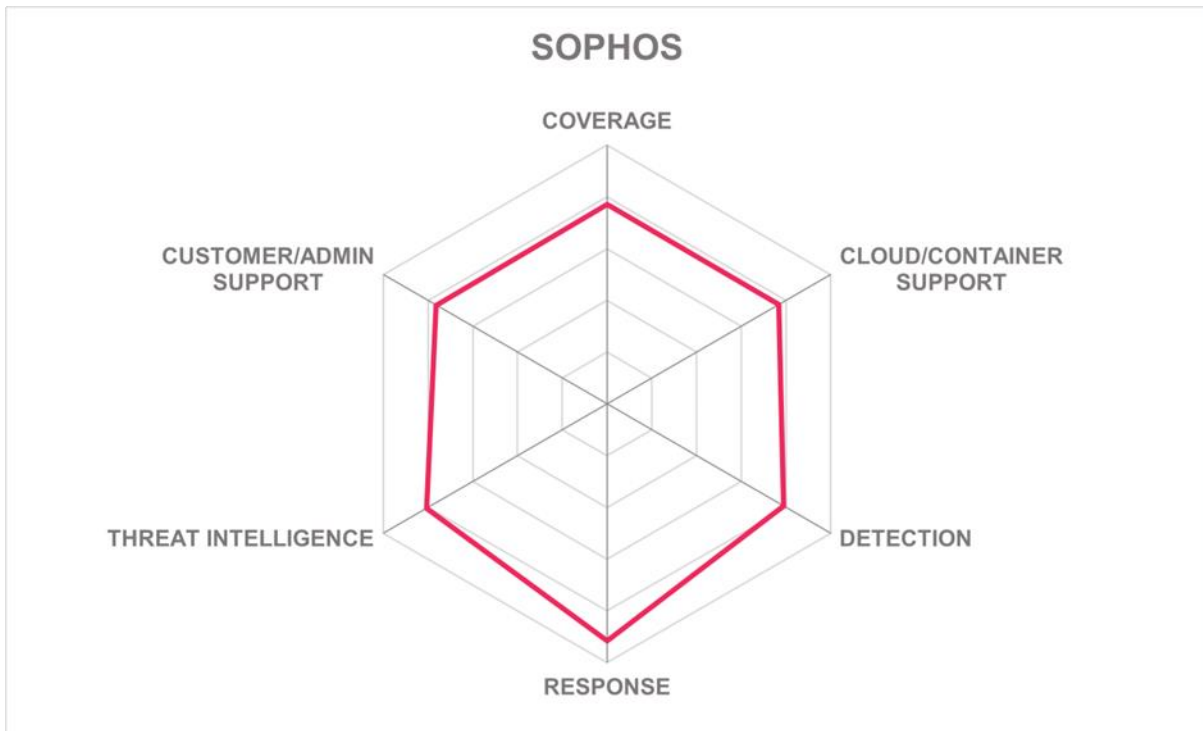
- Simple pricing model based on the number of users and servers
- Good MDR coverage of main operating systems and browsers
- Strong BEC capabilities especially for Microsoft environments
- New managed risk service available as an optional extra
- Large number of OOTB third-party integrations
- Offers vulnerability management services
- Strong threat intelligence capabilities and support
- Remote and on-site support for customers worldwide
- Excellent language support for services and documentation

### Challenges

- Limited pre-built integrations with third-party NDR solutions and none for third-party SIEM solutions
- Not able to detect any specific threats to Kubernetes environments

- Includes attacker behavior analytics but not user behavior analytics
- Does not include integrations for any third-party SOAR solutions
- Does not include software patching functionality
- Does not include customizable reporting for compliance teams
- No mobile app to access dashboards and status reports

Leader in



## Tata Communications – Managed Detection and Response (MDR)

Tata Communications is a global public communication and digital services company that operates in more than 190 countries, providing a range of communication services, network services, SASE, cloud services, and cybersecurity, including MDR. It was founded in 2002 and is headquartered in Mumbai, India, with SOCs in India (Pune and Chennai) and Dubai, with new SOCs planned for the US, Europe, and Singapore. Most customers are in the APAC region, followed by EMEA and fall into the enterprise and mid-market segments.

Tata Communications MDR is part of the company's cyber threat detection and response portfolio and combines several security platforms (SIEM, native SOAR, EDR, NDR, UEBA, cyber threat intelligence, and TC<sup>x</sup> that unifies visibility). 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. Tata Communications also offers on-premises dedicated SOCs for highly regulated sectors. Standard deployments can be completed within two weeks. In addition to the core MDR services, there is a wide range of add-on services such as brand monitoring, red team assessment, breach attack simulation, advanced threat hunting, ASM, EDR, NDR, and forensics.

There is a simple and flexible pricing model. Pricing is mainly based on EPS or messages per second (MPS), but pricing models based on data ingested or based on the number of devices and users in an organization are also available. The solution is available directly to end user organizations or via OEMs, other MSSPs, and partners. The company has increased its focus on supporting regionalized services via local partners by allowing them to white label Tata Communications MSSP services.

The solution covers all operating systems, including Android and iOS, and all major 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 several environments, including medical and industrial IoT devices, OT, and remote workers, but not all on-premises applications.

Tata Communications MDR includes pre-built integrations with most third-party NDR solutions, eight SIEM solutions, and five third-party EPDR products (CrowdStrike Falcon Endpoint Protection, Microsoft Defender for Endpoint, SentinelOne Singularity Platform, Kaspersky, and TrendMicro), but others can be integrated if APIs are available.

The solution provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also includes CSPM, CWP, and vulnerability scanning of customer multi-cloud environments. Tata Communications MDR can detect a wide range of threats to Kubernetes environments, and can handle logging and monitoring across multiple Kubernetes clusters. It can also monitor most cloud services OOTB.



Tata Communications MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, and insider threats. It can detect and respond to phishing attacks in real time, it can also detect malicious executables before they run, and it includes network intrusion detection capabilities. It includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to detect and report privilege escalation.

The solution can take response actions regardless of what security technology customers already have, it features a single platform that can respond automatically to disrupt threats, it includes a range of automated response actions, and it includes functionality for software patching. It also blocks ransomware attacks before any data is encrypted, includes automated proactive threat hunting, and applies AI/ML for detecting anomalous behavior and identifying threats, and for predictive threat hunting. Situational and customized threat hunting is also available. Tata Communications MDR includes its own SOAR functionality that includes a set of playbooks to improve MTTR as well as providing integrations for a wide range of third-party SOAR solutions. Custom playbook development is also available.

Tata Communications MDR includes threat intelligence capabilities for advanced threat detection and risk mitigation, includes the support of a threat intelligence platform that uses more than 65 threat feeds and dedicated threat hunting team, provides regular reporting on emerging threats, and uses threat intelligence feeds to train AI/ML models. The solution offers real-time threat intelligence integration and provides connectors for four additional third-party threat intelligence sources: Threat Abuse IPDB, LogRhythm, Recorded Future, and Cyble. The in-house threat intelligence capability is not backed by a global team of researchers, but Tata Communications generates threat intelligence from the visibility it has of 30% of the world's internet traffic as a tier 1 internet service provider (ISP). It also monitors the Dark Web for threat intelligence.

Tata Communications provides on-site support in the APAC region. The MDR service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The solution includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and it includes customizable reporting for business executives, technical teams, and compliance teams. It also includes recommendations on improving cyber resilience, but does not include an ROI calculator or the services of a dedicated risk advisor. However, the solution does include the services of a dedicated customer success manager. Tools for ASM are available as an add-on. There is no mobile app to provide access to dashboards and status reports, but this is in development as part of a planned revamp of the UI. Potential customers can take advantage of a pre-sales trial period to assess if Tata Communications MDR is a good fit. The solution complies with the standards and principles of ISO 27001, PCI-DSS, SSAE SOC 2 TYPE 2, HIPAA/HITRUST, UK Cyber Essentials, Germany C5, and France's SecNumCloud. It offers guaranteed data residency for the UAE and India.

Tata Communications MDR supports organizations of all sizes, but is particularly suited to medium to large enterprises in highly regulated sectors such as banking, financial services, insurance, healthcare, manufacturing, and automotive who are looking for a flexible and modular MDR service with a wide range of integrated add-on services.

<b>Security</b>	Strong Positive	
<b>Functionality</b>	Strong Positive	
<b>Deployment</b>	Positive	
<b>Interoperability</b>	Strong Positive	
<b>Usability</b>	Positive	

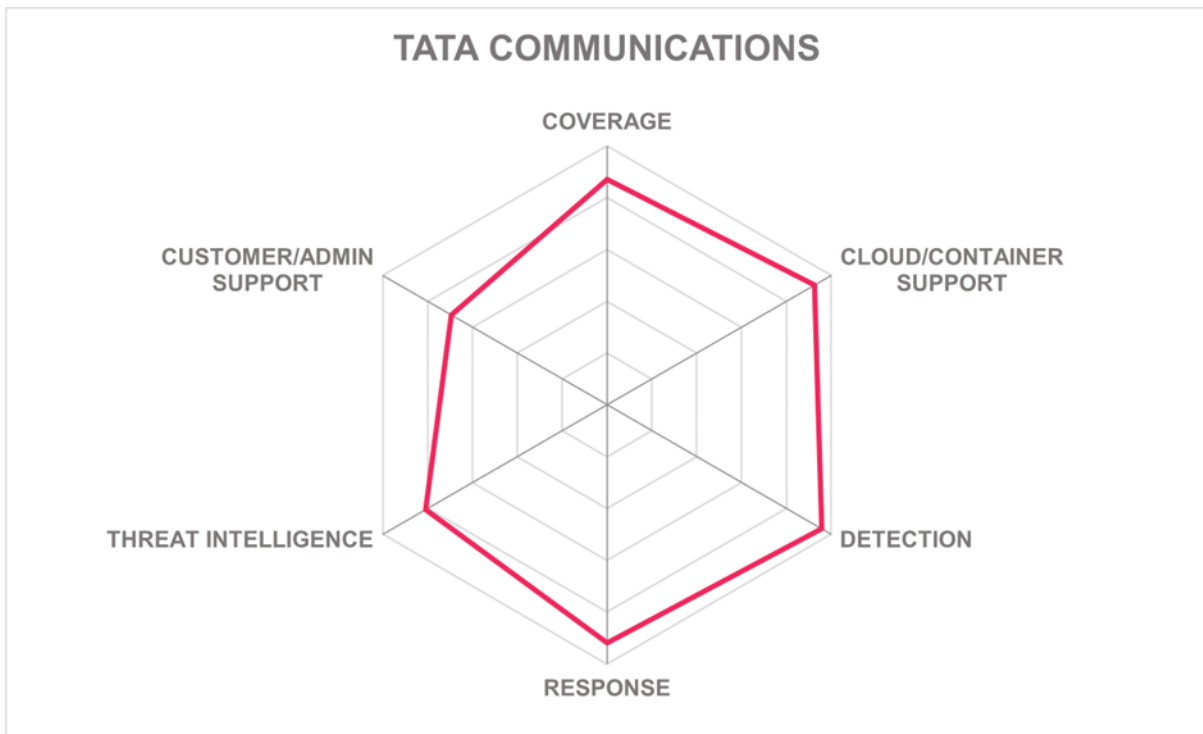
Table 17: Tata Communications' rating

### Strengths

- Rapid and flexible deployment options
- Simple and flexible pricing model
- Strong support for main international security standards
- Designed to interoperate with a wide range of security technologies
- Wide range of pre-integrated add-on services
- Strong threat intelligence, data analytics, and threat hunting capabilities
- Built in SOAR functionality and a wide range of SOAR integrations
- Good support for customer admins

### Challenges

- Provides connectors for limited number of threat intelligence sources
- On-site support services available only in the APAC region
- Does not include a dedicated risk advisor
- No mobile app, but this is on the roadmap
- Support services and documentation provided only in English
- Limited coverage of OT and IoT environments but enhancements of the roadmap



## ThreatLocker – Cyber Hero MDR

ThreatLocker is a private US-based cybersecurity company specializing in endpoint security solutions. Founded in 2017, ThreatLocker is headquartered in Orlando, Florida, where its global SOC is located. The company also has offices in Dublin, Ireland; Sydney, Australia; and Abu Dhabi, UAE, with datacenters in the US, Canada, Ireland, Australia, and the UAE. ThreatLocker's largest market is North America, followed by APAC and EMEA. Many of their customers fall into the medium-sized business category.

The company's core product is ThreatLocker Protect, a Zero Trust solution that uses allowlisting to block any unwanted software from running, Ringfencing™ to control software's behavior, and Network Control, a host-based firewall that opens and closes ports dynamically.

ThreatLocker also offers Elevation Control (PAM), Storage Control, Configuration Management, and ThreatLocker Detect, a policy-based endpoint detection and response (EDR) solution. ThreatLocker Detect uses the telemetry data ThreatLocker collects, and augments it with Event log data. This allows organizations to alert on and respond automatically to anomalous events or suspicious behavior on their endpoints. This information gives insights into an organization's security, enabling customers to identify and remediate possible cyber threats, in many cases before they happen.

Cyber Hero MDR, which provides managed services from the ThreatLocker Cyber Hero team, is an add-on to ThreatLocker Detect. The team monitors and responds to alerts generated in MDR customer environments. In the event of a cyber incident or attempted attack, the MDR team will follow customers' runbooks to notify and/or carry out response actions such as isolating or locking down affected devices.

ThreatLocker has a simple pricing model based on the number of endpoints protected, with a different base rate depending on what combination of products is chosen by the customer.

ThreatLocker MDR is available as a cloud service supported by round-the-clock support from its US-based SOC, using agents installed on every endpoint. Deployment of ThreatLocker's MDR offering typically takes a single day and is available directly to end user organizations and via MSSPs and channel partners.

The service is available for organizations using MS Windows, macOS, and Linux. The service provides round-the-clock monitoring and analysis of all major business IT environments and systems, virtual environments, datacenters, and remote and contract workers, but not Edge computing environments.

ThreatLocker MDR is designed to be vendor agnostic and can integrate with existing EPDR, NDR, SIEM, and security analytics products.

The solution provides round-the-clock monitoring and analysis of cloud applications and cloud data stores, and detection and response across multiple cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. The

solution includes CWP and vulnerability scanning of customer multi-cloud environments, but does not include cloud security posture management. ThreatLocker MDR does not detect any specific threats to Kubernetes environments and cannot handle logging and monitoring across multiple Kubernetes clusters. Although only Microsoft cloud services are covered currently, support for additional providers such as Google is planned.

ThreatLocker MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, Living Off The Land (LOTL) attacks, and insider threats. Although ThreatLocker provides Network (Access) Control, it does not include network intrusion capabilities. The solution includes user and attacker behavior analytics, integrations with third-party IDS, and the ability to control, detect, and report on privilege escalation activity.

The solution can take response actions regardless of what security technology customers already have, with a strong capability to isolate and lockdown computers on customer networks. It features a single platform that can respond automatically to disrupt threats, and includes a wide range of automated response actions, excluding the ability to initiate full packet capture and rollback registry/configuration changes. The solution does not include software patching functionality, but it can typically stop ransomware attacks before any data is exfiltrated or encrypted. The solution does not provide its own SOAR functionality, but can integrate with any third-party systems. The solution includes automated proactive threat hunting and provides playbooks for incident response, and does not use AI/ML for predictive threat hunting. However, customers can create their own policies, which the MDR will monitor and take response actions to any violations according to customer playbooks.

ThreatLocker MDR offers threat intelligence capabilities for advanced threat detection and risk mitigation, supported by a dedicated threat hunting team. However, it does not include regular reporting on emerging threats. Additionally, the solution lacks real-time threat integration, connectors to external threat intelligence sources, and Dark Web monitoring for cyber threat intelligence.

ThreatLocker provides customers with round-the-clock support and claims to have a US-based human support agent answer virtually all chats within 60 seconds and resolve most issues within minutes.

The service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large, mature organizations. The solution includes customizable reporting for business executives, technical teams, and compliance teams. The solution also includes recommendations on improving cyber resilience and an ROI calculator, but does not include the services of a dedicated risk advisor. Tools for ASM are available as part of the standard subscription. There is a mobile app that provides the same functionality as the management portal. A dedicated solution engineer and customer success manager is available as part of the standard subscription. Customers have access to the same data, tools, and reporting as ThreatLocker. Potential customers can take advantage of a pre-sales trial period to assess if ThreatLocker Cyber Hero MDR is a good fit. The solution complies with the SSAE SOC 2 TYPE 2 framework and offers guaranteed data residency for the US, Canada, EU, UAE, and Australia.

ThreatLocker Cyber Hero MDR, including ThreatLocker Detect, supports organizations of all sizes and verticals. Its core capability of blocking all unintended actions makes it particularly attractive to the government sector and other highly regulated industries seeking monitoring, alerting, and response capabilities, along with robust policy-based security controls. However, it lacks some advanced features such as cloud security posture management, AI/ML-driven predictive threat hunting, and native SOAR capabilities, which may limit its appeal to organizations requiring comprehensive automation and advanced threat intelligence integration.


<b>Security</b>	Neutral	
<b>Functionality</b>	Neutral	
<b>Deployment</b>	Neutral	
<b>Interoperability</b>	Positive	
<b>Usability</b>	Positive	

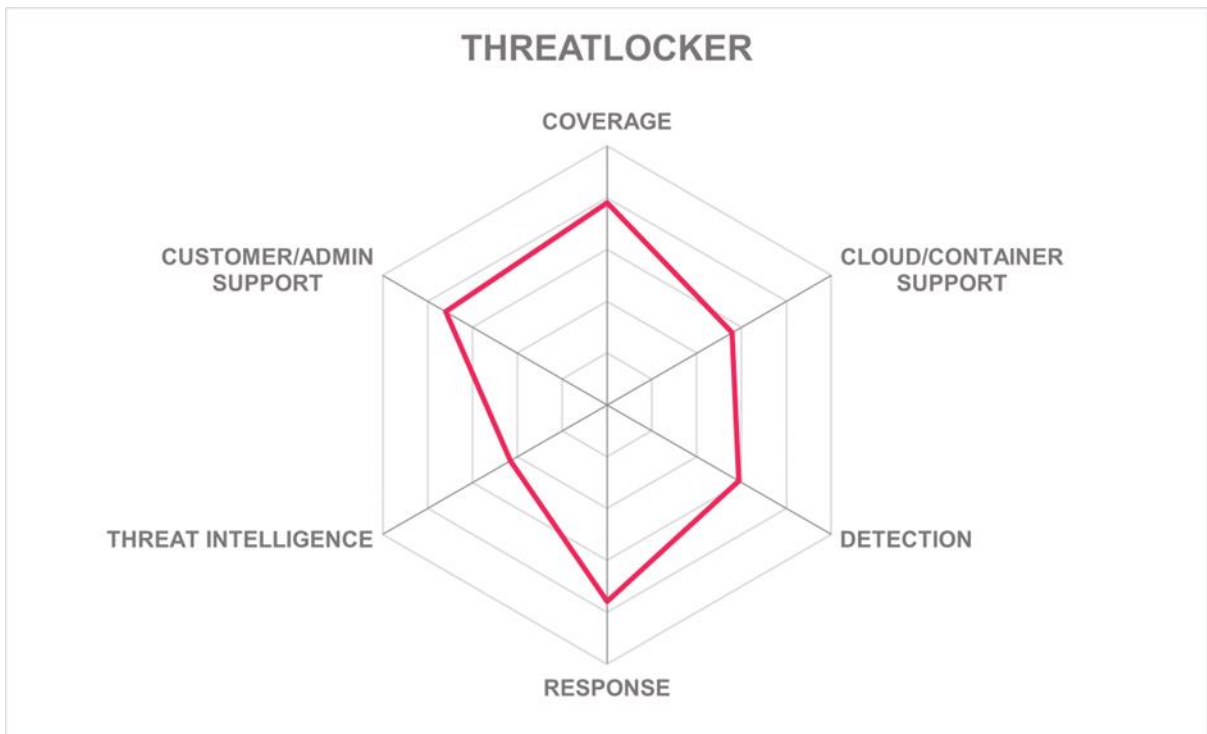
Table 18: ThreatLocker's rating

### Strengths

- ThreatLocker's EDR and MDR are complementary to its core platform
- Support customers' existing technology stacks
- Simple pricing model
- Good coverage of major business IT environments and systems
- Rapid customer and incident response
- Rapid deployment
- Guaranteed data residency for the US, Canada, EU, UAE, and Australia
- Mobile app to support cyber defenders wherever they are

### Challenges

- Covers only Windows, macOS, and Linux environments, not Android and iOS
- Does not cover mobile devices and only some IoT, IIoT, IoMT, OT
- No coverage of Edge computing environments
- Does not include CSPM
- Does not include software patching capabilities
- No specific support for Kubernetes environments
- Can monitor a limited number of cloud services for MDR purposes
- Does not apply AI/ML for predictive threat hunting
- ThreatLocker does not provide risk advisory services, but product research informs organizations about software risks
- Support services and documentation available only in English



## Uptycs – Uptycs MDR

Founded in 2016, and headquartered in Waltham, Massachusetts in the US, Uptycs is a venture capital-backed private cybersecurity company that specializes in providing a unified cloud-native security analytics platform. The company offers a range of services focused on endpoint security, cloud security, compliance management, unified security analytics, and MDR, with a virtual global SOC based on the follow-the-sun model with SOC analysts in Australia, India, and the US. Most customers are North America followed by EMEA and fall into the Enterprise segment.

Uptycs MDR is essentially an add-on service to the Uptycs Cloud-Native Application Protection Platform (CNAPP), which provides a unified approach to security across multi-cloud environments, endpoints, containers, Kubernetes, and connected developer environments. For more information on the Uptycs CNAPP, see the [KuppingerCole Leadership Compass: Cloud-Native Application Protection Platforms](#).

Uptycs MDR covers all endpoints, services, and workloads protected by the Uptycs CNAPP Platform, and pricing is based on the assets protected and the level of service. Customers can choose between three levels of MDR.

With Managed Onboarding, the Uptycs MDR team assists customers for the first 60 days by triaging initial alerts, fine-tuning those alerts, and developing custom exceptions to align with the customer's infrastructure. This level does not include IR or forensic services.

The Managed Monitoring level involves continuous monitoring of all workloads and endpoints for potential threat actors. The MDR team performs threat hunting, triages alerts, notifies customers of high-confidence threats, and helps develop custom alerts. Additionally, the team alerts customers to any new vulnerabilities found in their systems, and notifies them of high-risk vulnerabilities that are being exploited in the wild.

At the highest level, Managed PROTECT, the MDR team not only monitors and alerts but also actively responds to threats. They block high-risk events, suspected threat activity, and assist in incident investigations. Although Uptycs can perform technical remediation on an asset to make changes to it, this level does not include recovery services.

Uptycs MDR is deployed mainly as a cloud-based service with on-prem elements where required, allowing for rapid deployment. The service is available exclusively through channel partners.

The service covers all major operating systems, but not Android and iOS. However, it also provides coverage for Kubernetes, AWS, Azure, GCP, GitHub, and Okta. The MDR service also supports all main browsers.

Uptycs MDR provides 24/7 monitoring and analysis of all business IT environments protected by Uptycs, excluding internet traffic, corporate networks, and Edge computing environments. The service provides detection and response across most environments, including remote workers, excluding IoMT, IIoT, and OT.



As an add-on to the Uptycs CNAPP Platform, the MDR service does not pull in data from third-party security solutions, and therefore does not provide prebuilt integrations with third-party EPDR and NDR. However, it does include integrations with eight SIEM solutions (Elastic Security, Fortinet FortiSIEM, Logpoint, LogRhythm, IBM QRadar, Rapid7, Splunk, and SumoLogic), and it supports Webhook and API integrations.

Uptycs MDR provides continuous monitoring and analysis of cloud applications and cloud data stores, and detection and response across all cloud services and applications. It includes connectors to cloud services, it can identify data loss across cloud infrastructure, and it can detect and respond to threats to multi-cloud environments. It also includes CSPM, CWP, and vulnerability scanning of customer multi-cloud environments. The service can detect a wide range of threats to Kubernetes environments, including misconfigurations and container vulnerabilities, and can handle logging and monitoring across multiple Kubernetes clusters. It can monitor five cloud services for MDR purposes (Azure AD, MS Office 365, Google Workspace, Google Drive, and GitHub).

Uptycs MDR can detect and respond to a wide range of malicious activities, including RDP exploitation, ransomware attacks, evasive malware, and insider threats. It can detect malicious executables before they run, it can detect and respond to phishing attacks in real time, but it does not include network intrusion detection capabilities or integrations with IDS. The service can detect and report privilege escalation and includes user behavior analytics, but not attacker behavior analytics.

The service can take response actions as long as the asset impacted has an Uptycs agent, it can respond automatically to disrupt threats, and includes a fairly wide range of automated response actions. It does not include functionality for software patching, but it can block ransomware attacks before any data is encrypted. It also includes proactive threat hunting. The service does not provide playbooks for incident response and does not apply AI/ML for predictive threat hunting. Uptycs MDR includes its own SOAR functionality but integrating with third-party SOAR solutions would require coding to APIs.

Uptycs MDR includes threat intelligence capabilities for advanced threat detection, backed by an internal threat intelligence team and a global team of researchers. It includes automated and manual threat hunting, and provides regular reporting on emerging threats. It supports a bring-your-own-license model for customers to plug in third-party threat intelligence feeds but does not use threat intelligence feeds to train AI/ML models.

On-site support is available for all customers, the service can be used to outsource the SOC function, and it enables collaboration with and support for customer SOC teams at large organizations. The service includes functionality to generate reports that map detected threats to ATT&CK tactics and techniques, and includes customizable reporting for business executives, technical teams, and compliance teams. It does not include recommendations for improving cyber resilience, an ROI calculator, the services of a dedicated risk advisor, ASM tools, or a mobile app for access to dashboards and status reports. However, Uptycs MDR does include the services of a dedicated customer success manager. Customers have access to the same data, tools, and reporting as Uptycs. The service complies with the standards and principles of ISO 27001, PCI-DSS, HIPAA/HITRUST, and SSAE SOC 2

TYPE 2, and offers guaranteed data residency in US, EU, and UAE. For countries with specific data residency requirements, Uptycs can create a cloud stack within their region.

Uptycs MDR supports customers of all sizes and across various industries, whether they handle incident recovery internally or through third-party services. It is particularly well-suited for organizations with complex IT environments that seek to enhance visibility and security across multi-cloud environments, Kubernetes infrastructure, and software supply chain security, all while reducing headcount by outsourcing their SOC operations

<b>Security</b>	Positive
<b>Functionality</b>	Neutral
<b>Deployment</b>	Positive
<b>Interoperability</b>	Neutral
<b>Usability</b>	Positive



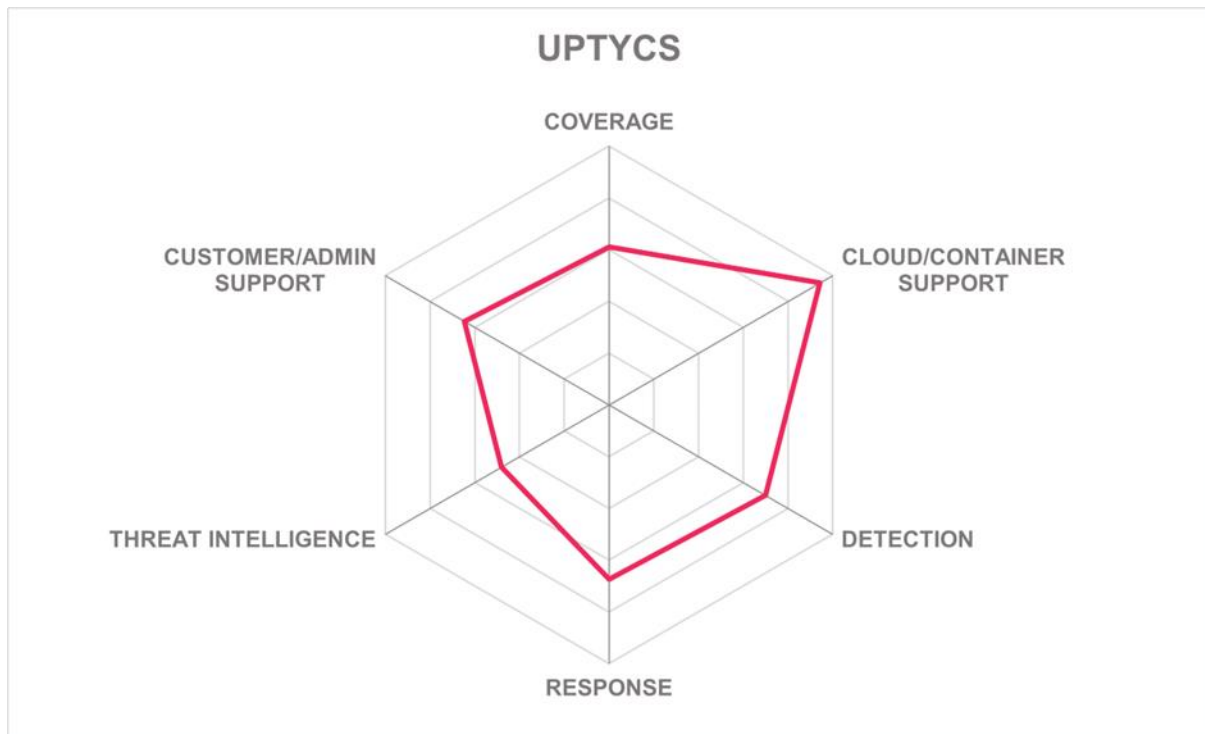
Table 19: Uptycs’s rating

### Strengths

- Integrated with Uptycs CNAPP
- Cloud-based service, allowing rapid deployment
- Good security coverage of hybrid, multi-cloud environments
- Specialized coverage of cloud and Kubernetes environments
- Strong focus on endpoint security
- Customizable MDR levels to meet varying needs

### Challenges

- Requires Uptycs CNAPP
- Does not directly monitor internet traffic or corporate networks
- Full MDR service does not include recovery
- Support and documentation available only in English



## Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space.

### Barracuda Networks

Barracuda Networks was founded in 2003 and is headquartered in Campbell, California in the US. They are owned by global investment firm, KKR. Barracuda offers products and services for email, data, network, and application security. Barracuda's XDR offering is composed of the products listed above. The solution is primarily offered as a Managed XDR solution. The XDR console is hosted as SaaS by Barracuda Networks.

**Why worth watching:** Barracuda has a long history of helping small to mid-size businesses with email and data protection. Barracuda offers SLAs with >99.99% availability. They have expanded their portfolio of services, and have built out a Managed XDR solution that SMBs and mid-market companies should consider when launching RFPs.

### Cybereason

Cybereason is a private cybersecurity technology company founded in 2012 and headquartered in Boston, Massachusetts in the US. Cybereason MDR is based on the company's Open XDR Defense Platform, and 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.

**Why worth watching:** 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.

### Expel

Expel is a private security operations provider based in the US, founded in 2016, and headquartered in Herndon, Virginia in the US. 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.

**Why worth watching:** 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.

## ForeNova Technologies

ForeNova Technologies is a private cybersecurity company founded in 2021 and headquartered in Amsterdam in the Netherlands. ForeNova is focused on small and mid-market enterprises in Europe, but it also has customers in Malaysia and Hong Kong.

**Why worth watching:** NovaMDR 360° supports organizations of all sizes but is best suited to small and mid-market enterprises 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.

## Fortinet

Fortinet is a public, US-based cybersecurity company founded in 2000 and headquartered in Sunnyvale, California. Fortinet Managed Detection and Response (MDR) is a cloud-based service that leverages FortiEDR and FortiXDR technologies.

**Why worth watching:** Fortinet MDR supports all but the smallest of businesses and is best suited to medium and mid-market enterprises that have internal SOCs 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.

## IBM Security

IBM Corporation is a multinational technology and consulting company founded in 1911 and headquartered in Armonk, New York, in the US. IBM MDR is deployed as a managed service based on the IBM MDR platform hosted in IBM facilities that can support customer technology on premises, in the cloud or in a hybrid fashion.

**Why worth watching:** IBM Security MDR 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.

## Red Canary

Red Canary is a private, American managed detection and response company founded in 2014 and based in Denver, Colorado. Red Canary MDR is a cloud-based service, offering coverage for endpoint, network, and cloud.

**Why worth watching:** 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.

## SentinelOne

Founded in 2013, SentinelOne is a US-based cybersecurity company that is headquartered in Mountain View, California, and specializes in providing advanced endpoint protection and response solutions. SentinelOne's Singularity MDR service is based on its AI-supported Singularity platform, which integrates endpoint protection (EPP), EDR, and XDR.

**Why worth watching:** SentinelOne's Singularity MDR is suited to organizations looking for a rapid response service that integrates AI and human expertise, is transparent in operations and findings, offers optional forensic services, and extends beyond endpoints to include cloud, identity, email, and network protection.

## SecurityHQ

SecurityHQ is a privately held global Managed Security Services Provider (MSSP), founded in 2003 with headquarters in London. SecurityHQ's MDR is a cloud-based service that was established in 2008, and is underpinned by the company's Response Platform.

**Why worth watching:** 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.

## WithSecure

Formerly F-Secure Business founded in 1988, WithSecure is headquartered in Helsinki, Finland. It offers two MDR services: WithSecure Managed Detection and Response, and Countercept MDR. The WithSecure MDR service uses the company's Elements EDR's Broad Context Detections (BCD), telemetry, and response capabilities, providing 24/7 monitoring and incident response. Countercept MDR, uses a proprietary EDR agent and log collectors that feed into an XDR detection platform.

**Why worth watching:** WithSecure has long-standing expertise in cybersecurity and offers a Europe-only Countercept MDR option, addressing data sovereignty concerns.

## Xcitium

Headquartered in Bloomfield, New York, 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 offers four MDR packages designed to meet different use cases and market segments.

**Why worth watching:** 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 with patch management, vulnerability management, and unlimited incident response.

## Related Research

[Leadership Compass: Identity Threat Detection and Response \(ITDR\)](#)  
[Leadership Compass: Managed Detection and Response \(MDR\) 2023](#)  
[Leadership Compass: Network Detection and Response \(NDR\) 2024](#)  
[Leadership Compass: Endpoint Protection, Detection and Response 2024](#)  
[Market Compass: Security Operations Center as a Service \(SOCaaS\)](#)  
[Buyer's Compass: NIS2 – EU Network and Information Security Directive](#)  
[Blog: Threat Detection and Incident Response](#)

## Copyright

©2024 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden without prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing in-depth analysis, positions presented in this document will be subject to refinement or even major changes. KuppingerCole disclaims 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 does 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](mailto:clients@kuppingercole.com).