kuppingercole ANALYSTS

Managed Detection and Response

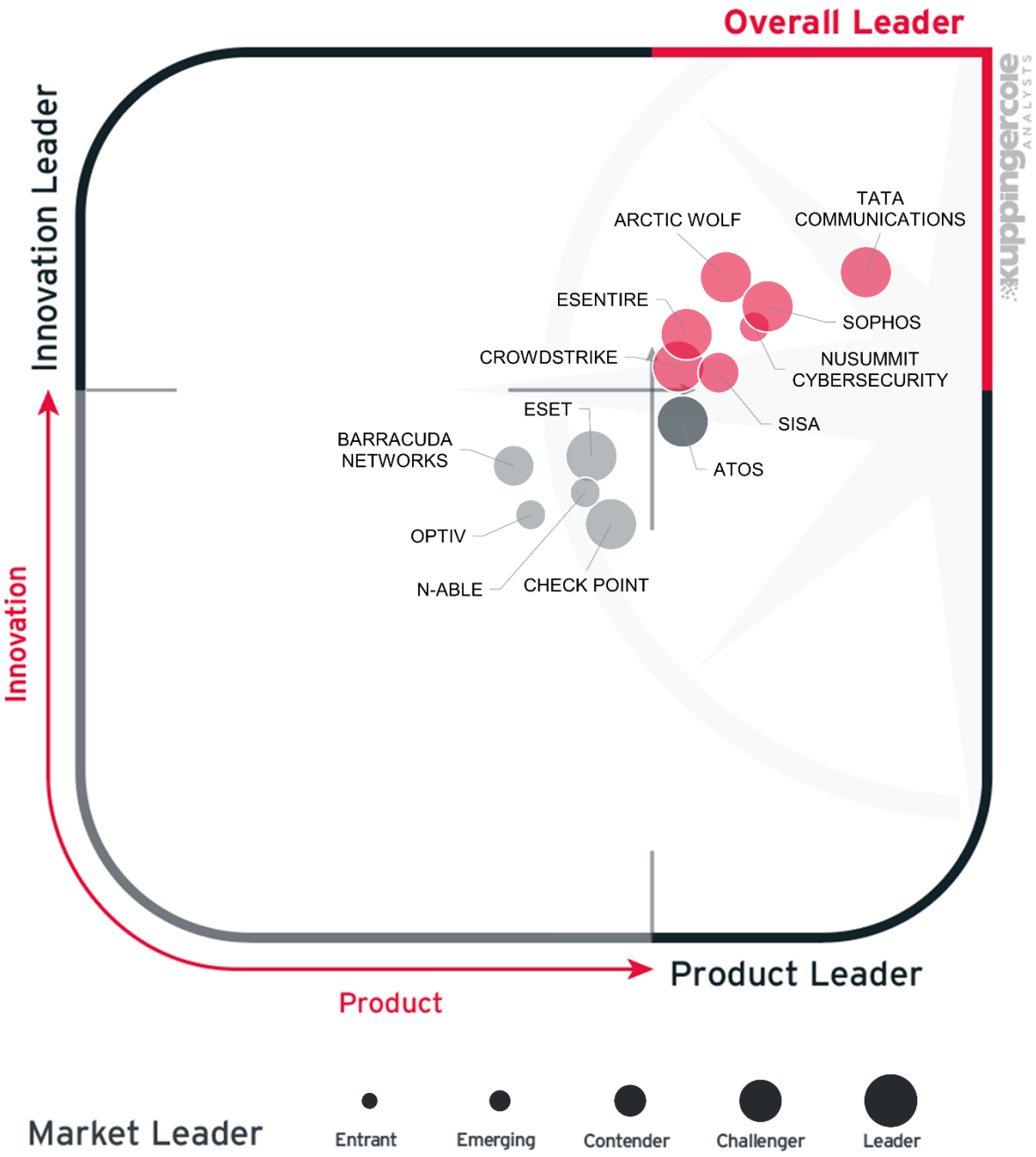
Warwick Ashford

April 29, 2026

LEADERSHIP COMPASS 2026

Leadership Compass

Managed Detection & Response 2026



This KuppingerCole Analysts Leadership Compass provides an overview of the Managed Detection and Response (MDR) market in 2026. It examines services that detect, analyze, investigate, and respond to cyber threats across diverse environments, and evaluates the ability of vendors to deliver continuous monitoring, validated detections, coordinated response actions, and measurable security outcomes.

Contents

Introduction

Organizations face persistent cyber threats that target infrastructure, applications, cloud workloads, identity systems, and connected devices. Attack techniques continue to advance, yet many organizations struggle to operate effective security operations because they lack skilled staff and cannot maintain continuous monitoring. MDR has therefore become an essential component of enterprise resilience. MDR combines advanced analytics, automation, and human expertise to detect and contain attacks quickly while supporting continuous improvement of security posture.

MDR has matured from managed alert handling into a service model that focuses on validated detections, contextual investigations, and coordinated response. Vendors deliver these outcomes through managed or co-managed operating models that span endpoint, network, identity, cloud, and application telemetry.

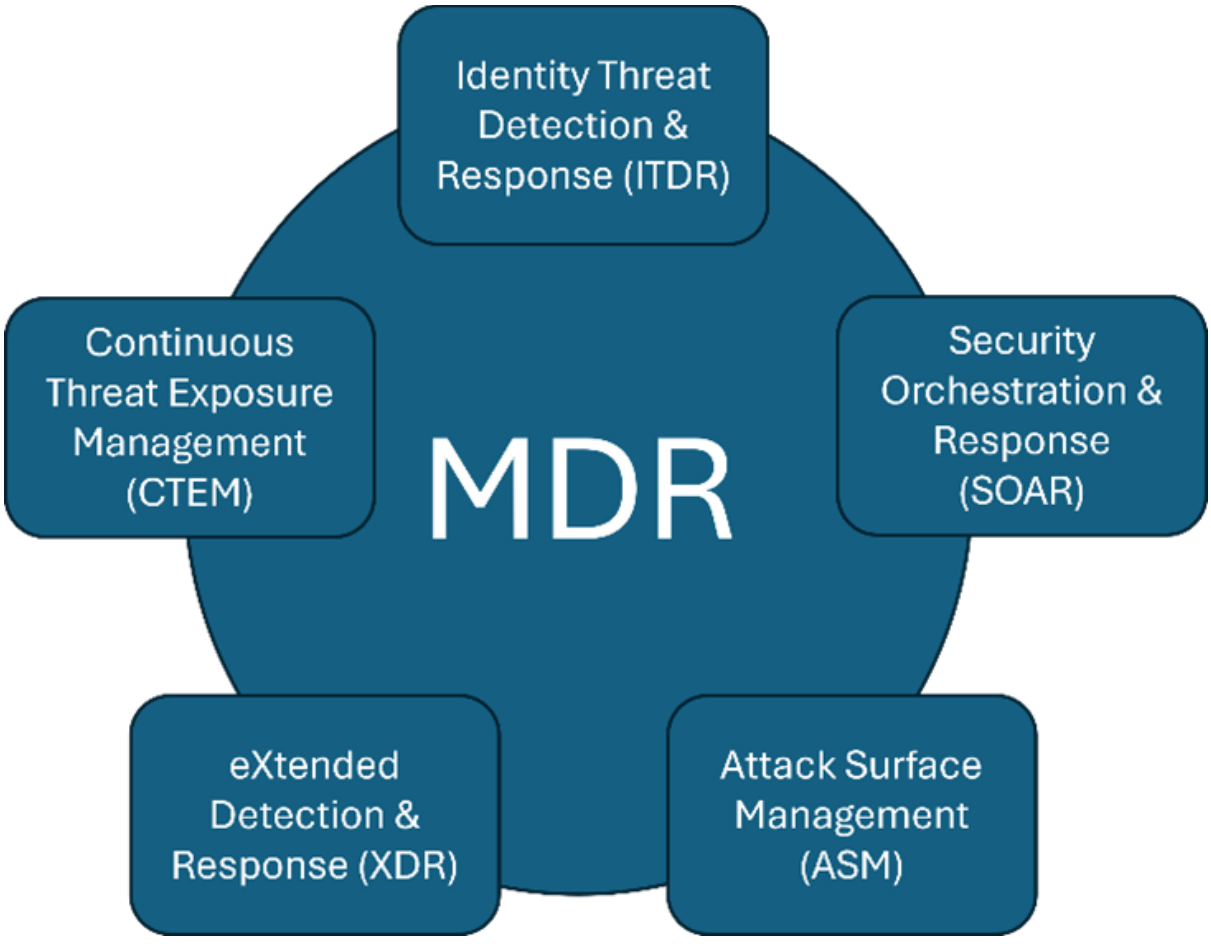


Figure 1: Integrated capabilities of modern MDR solutions

MDR now incorporates capabilities from eXtended Detection and Response (XDR), Security Orchestration, Automation, and Response (SOAR), Identity Threat Detection and Response (ITDR), Continuous Threat Exposure Management (CTEM), and Attack Surface Management (ASM), while frequently leveraging Security Information and Event

Management (SIEM) platforms as the underlying data aggregation and correlation layer. This convergence enables unified visibility and coordinated defense across all computing environments.

Organizations adopt MDR because they need continuous monitoring, fast and accurate detection, and fast and effective response. MDR providers supply human analysts, who investigate alerts, correlate activity, and determine whether incidents require containment. These services reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) by combining automated analytics with targeted human review. MDR also improves the value of existing tools because providers tune controls, refine detections, and create integrations that many customers would not have the capacity to maintain on their own. MDR services also help customers meet regulatory and security expectations under frameworks such as the European Union's Network and Information Security Directive 2 (NIS2) and the US Health Insurance Portability and Accountability Act (HIPAA), which require demonstrable monitoring and Incident Response (IR) capabilities.

MDR capabilities can also support compliance and assurance objectives under widely adopted standards and regulatory schemes, including the International Organization for Standardization's Information Security Management Systems standard (ISO 27001) and Common Criteria for Information Technology Security Evaluation (ISO 15408), the Payment Card Industry Data Security Standard (PCI DSS), the UK Cyber Essentials scheme, Germany's Cloud Computing Compliance Criteria Catalogue (C5), France's SecNumCloud certification framework, the US Federal Information Processing Standard for Advanced Encryption (FIPS 197) and for Security Requirements for Cryptographic Modules (FIPS 140-2), and the US National Institute of Standards and Technology Special Publication 800-57: Recommendation for Key Management (NIST SP 800-57).

Identity has become a primary attack vector, so MDR providers increasingly include identity-centric analytics, credential misuse detection, and monitoring for anomalous access behaviors. This aligns MDR with ITDR requirements and reflects the importance of identity in modern attacks. MDR providers also incorporate exposure management functions that identify vulnerabilities, misconfigurations, and risky behaviors before adversaries can exploit them. Many vendors integrate exposure data with detection workflows to give customers clearer insight into attack paths and priorities for remediation and improvement of defenses.

Automation plays a central role in MDR. Vendors apply Machine Learning (ML), User and Entity Behavior Analytics (UEBA), and increasingly Large Language Models (LLMs), including Generative Artificial Intelligence (GenAI), to accelerate alert triage, streamline investigations, and support analyst workflows. Detection logic remains grounded in validated telemetry correlation and behavioral models, while GenAI is primarily used to summarize incidents, assist investigations, and improve reporting efficiency.

Customers expect transparency about how AI models influence detections and recommendations, leading vendors to document model behavior, training boundaries, and decision support limitations. Response automation continues to expand, with many services offering orchestrated containment actions through established playbooks. These

automations allow MDR teams to address routine threats quickly while focusing human analysts on complex investigations and strategic tasks.

MDR supports organizations of all sizes. Smaller organizations rely on MDR as their primary security operations function due to skill shortages and the much lower cost of outsourcing compared with building and staffing an equivalent capability internally. Larger organizations use MDR to extend coverage, add expertise, or co-manage detections and IR actions with their internal teams. Co-managed MDR has become a mainstream delivery model because it gives customers shared visibility into investigations while delegating operational work to an expert provider.

Industry-specific MDR offerings continue to grow. Vendors develop tailored content packs, detections, and reporting for sectors such as healthcare, finance, and manufacturing. MDR services also extend into Operational Technology (OT), industrial automation, and connected devices. These environments require specialized telemetry, context, and response actions, so vendors invest in domain-specific expertise and integration capabilities.

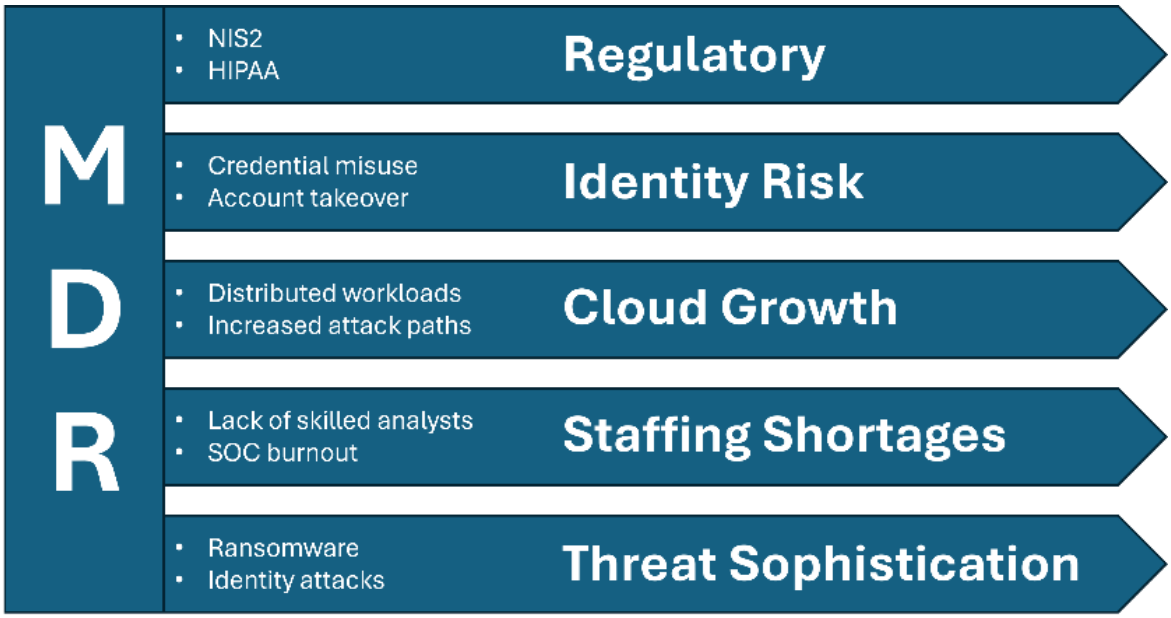


Figure 2: MDR market drivers

Customers now evaluate MDR providers based on delivered outcomes rather than tool checklists. They seek measurable improvements in detection efficiency, response speed, containment quality, and posture enhancement. Vendors that demonstrate these improvements through transparent reporting and evidence-based metrics have a competitive advantage. MDR, therefore, plays a central role in enterprise security strategy because it connects detection, analysis, response, exposure management, and compliance into a single operational function at an affordable cost.

This Leadership Compass is designed as a tool to help organizations 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 Analysts Research Methodology.

Key Findings

- MDR has become a unified security operations function that integrates detection, investigation, response, and exposure management across multiple telemetry domains.
- Outcome-focused service delivery drives vendor differentiation because customers require measurable improvements in detection and response efficiency.
- Identity-centric analytics strengthens MDR because identity compromise remains the leading attack vector across enterprise environments.
- ML and LLMs support triage, investigation, and reporting, improving analyst productivity and reducing operational workload.
- Exposure management, continuous assessment, and attack surface insights expanded MDR from reactive activity into ongoing posture improvement.
- All vendors in the report offer co-managed MDR adoption increased because customers want shared visibility, collaborative investigations, and control of response decisions.
- MDR providers offer specialized services for regulated sectors to support reporting requirements and tailored detection content.
- Integration and interoperability across diverse tools have become requirements because organizations need unified visibility across distributed environments.

Market Analysis

The MDR market is expanding because organizations require ongoing support to detect, investigate, and contain threats that overwhelm internal teams. MDR providers deliver this support with continuous monitoring, automated analytics, and expert review, which enables faster detection and coordinated response across complex environments.

Growth in this market reflects increased demand for accountability, measurable results, and operational resilience. Customers expect MDR providers to deliver validated detections, reduce alert noise, and support decisions with actionable insights. Vendors respond with unified analytics that correlate endpoint, network, identity, and cloud activity through advanced models and automation. Many providers now integrate exposure management, attack surface analysis, and vulnerability prioritization. These additions shift MDR toward proactive identification of weaknesses and alignment with broader cyber risk programs. Vendors also support regulatory obligations by delivering reports, documented investigations, and audit-ready evidence.

Several drivers shape the market. Organizations face staffing shortages, shrinking budgets, rising attack volumes, and greater complexity and diversity in their environments. Identity-based attacks increased significantly, so MDR now includes identity analytics and detection of credential misuse. Cloud adoption expanded attack paths, and customers expect MDR providers to support diverse workloads without increasing operational burden. Cybersecurity regulations around the world and cyber insurance requirements are increasingly requiring demonstrable monitoring and IR, which encourages investment in MDR services. Growth in OT and connected environments created new requirements for specialized telemetry, context, and response workflows. MDR vendors address these needs with domain-specific capabilities and integration.

Market evolution continues through the convergence of MDR with technologies such as XDR, CTEM, ASM, and ITDR. Vendors integrate these capabilities to deliver a single operational function with unified visibility, correlated detections, and coordinated response. AI-assisted Security Operations Center (SOC) functions increased analyst efficiency and reduced investigation time. Co-managed MDR gained momentum because customers want to retain visibility and some measure of control while delegating operational responsibilities. Open Application Programming Interfaces (APIs), standard data formats, and platform interoperability remain essential because customers need consistent data handling across distributed systems. Vendors that adopt these approaches deliver greater transparency, faster response times, and improved outcomes.

Delivery Models

The MDR market continues to support multiple delivery approaches, but these models have expanded to meet wider operational and regulatory needs. Cloud delivery remains the dominant model because it simplifies deployment, supports high data volume, and enables continuous updates. Most MDR providers now offer Software as a Service (SaaS) delivery to

streamline onboarding and maintain consistent service quality. However, many organizations require MDR to integrate with established security tools and controls, which has led providers to adopt modular architectures that support flexible deployment and telemetry collection.

Several vendors offer fully cloud-delivered MDR with lightweight agents or without agents, while others maintain options for customers that need on-premises software, collectors, or private processing environments. Certain sectors require stricter data handling controls, and some MDR providers support fully on-premises deployments, including an on-site SOC for regulated environments.

Current delivery models therefore include cloud, on-premises, and mixed deployments. The providers that offer the broadest flexibility and support for diverse operational requirements deliver the best alignment with customer expectations. Solutions that integrate with existing tools, maintain consistent visibility across environments, and allow customers to choose how detection and response functions are deployed provide the strongest operational value.

Required Capabilities

MDR solutions must support a broad set of capabilities to deliver continuous detection and coordinated response.

The following is a list of criteria for evaluation in this Leadership Compass on MDR:

- 24/7 monitoring, validated detection, and IR
- Correlation of endpoint, network, cloud, and identity telemetry
- AI-assisted analytics and investigation support
- Incident containment and isolation workflows
- Threat hunting using behavioral and intelligence-driven methods
- Automation of routine response actions through defined playbooks
- Integration with existing SIEM and SOAR tools
- Exposure management and vulnerability prioritization
- Identity-centric monitoring and detection of anomalous access activity
- Comprehensive dashboards and reporting for investigations and compliance
- Log ingestion, normalization, and correlation
- Support for diverse deployment models
- Customer communication, escalation, and collaboration processes

The following items are considered as additional and innovative capabilities:

- LLM-based analyst assistants for accelerated investigations
- CTEM and ASM
- Behavioral risk scoring based on identity activity
- Industry-specific content and reporting packages
- AI-driven threat prediction and anomaly scoring
- Support for compliance frameworks

- Open data models such as the Open Cybersecurity Schema Framework (OCSF)
- Co-managed SOC models with shared visibility
- Deception technologies for early threat detection
- AI transparency and explainability reporting
- Support for OT, Internet of Things (IoT), and industrial telemetry
- Mobile applications for real-time interaction with MDR teams
- Automated response playbook generation using AI

Leadership

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

Overall Leadership

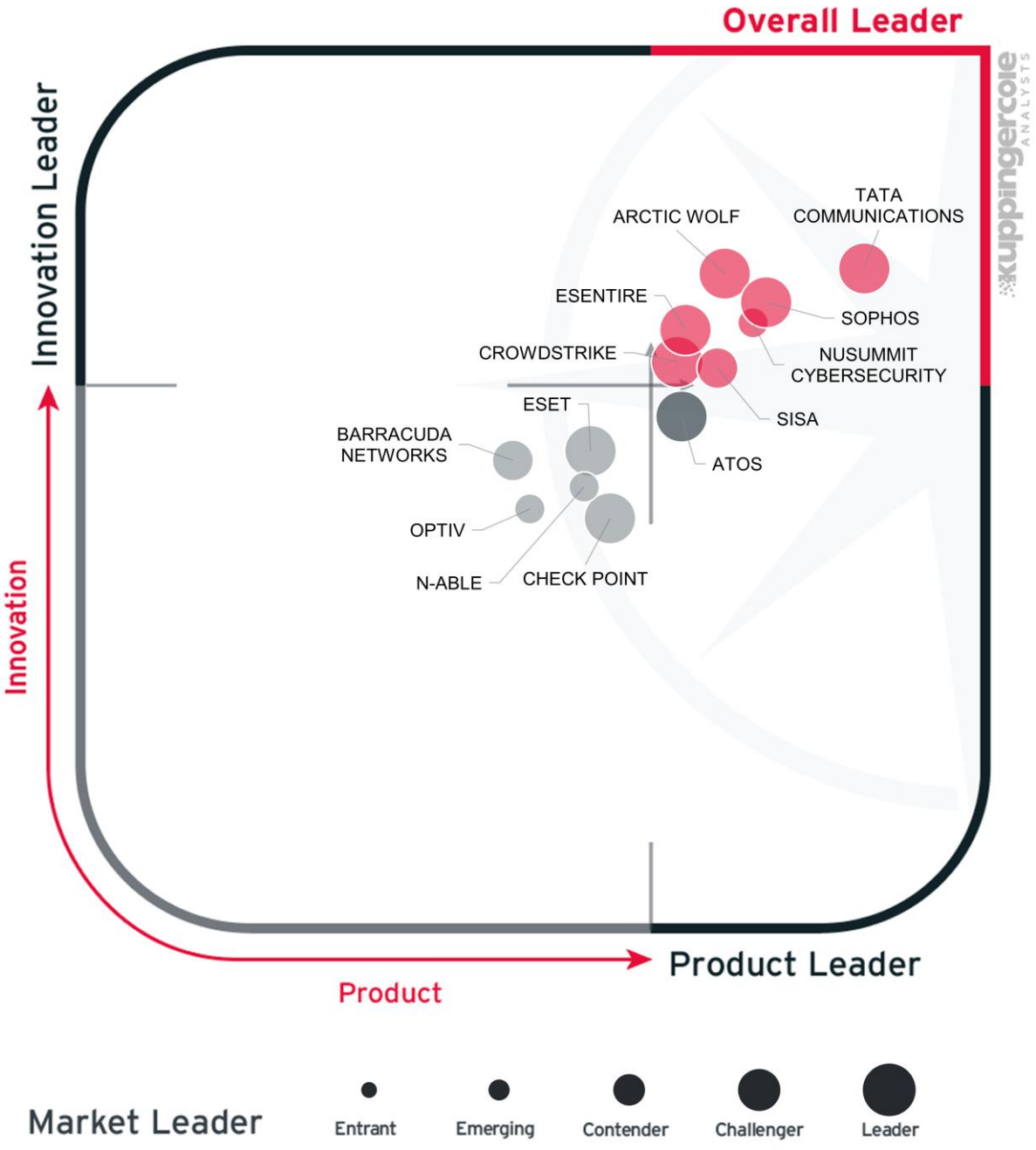
The Overall Leadership chart reflects how vendors balance product strength, innovation, and market presence. The chart evaluates vendors in this market across two dimensions. The horizontal axis measures Product Leadership, and the vertical axis measures Innovation Leadership. Overall Leaders are those in the upper right-hand quadrant, with the bubbles colored red. Vendors in this quadrant score highly in both dimensions, earning Overall Leadership status. These organizations ship mature products while maintaining strong innovation.

The bubble size reflects each vendor's relative strength in terms of Market Leadership. Further details on Market Leadership can be found in the Market Leadership section.

Product Leaders are found to the right of the vertical dividing line. The vendors in the lower right quadrant, colored black, are established vendors with full-featured products but fewer innovative differentiators. These providers demonstrate solid execution using conventional methods. Further details on Product Leadership can be found in the Product Leadership section.

Innovation Leaders are found above the horizontal dividing line. Vendors in the upper left-hand quadrant, colored black, have advanced technological approaches but less mature product offerings. These companies often introduce new technical approaches that are not yet widely adopted. Further details on Innovation Leadership can be found in the Innovation Leadership section.

Vendors in the lower left-hand quadrant, colored grey, are challengers for both product and innovation leadership. Those toward the bottom left-hand corner are mainly niche vendors with products focused on specific market segments and geographical areas.



Overall Leaders are Tata Communications, Arctic Wolf, Sophos, CrowdStrike, eSentire, NuSummit Cybersecurity, and SISA.

Tata Communications combines a mature MDR service with a high pace of innovation, supported by global scale, broad SOC coverage, and carrier-grade network visibility. It also sustains strong product depth across SIEM, SOAR, Endpoint Detection and Response (EDR), Network Detection and Response (NDR), UEBA, and cloud security, while expanding capabilities such as Edge-aligned response and agentic, human-validated investigation support across IT and OT environments.

Arctic Wolf's Aurora Platform and concierge operating model deliver consistent product strength with sustained innovation in analyst workflows, automation, and posture improvement. Its large channel-led customer base and global SOC footprint reinforce market presence while it continues to extend cloud, identity, and response coverage.

Sophos pairs mature MDR execution with ongoing innovation through Sophos X-Ops and GenAI-supported investigation workflows, backed by a broad customer base and expanded SOC scale.

CrowdStrike's Falcon Complete MDR service combines strong product leadership in endpoint-led detection and response with sustained innovation in automation and AI, supported by broad market adoption and global delivery capacity.

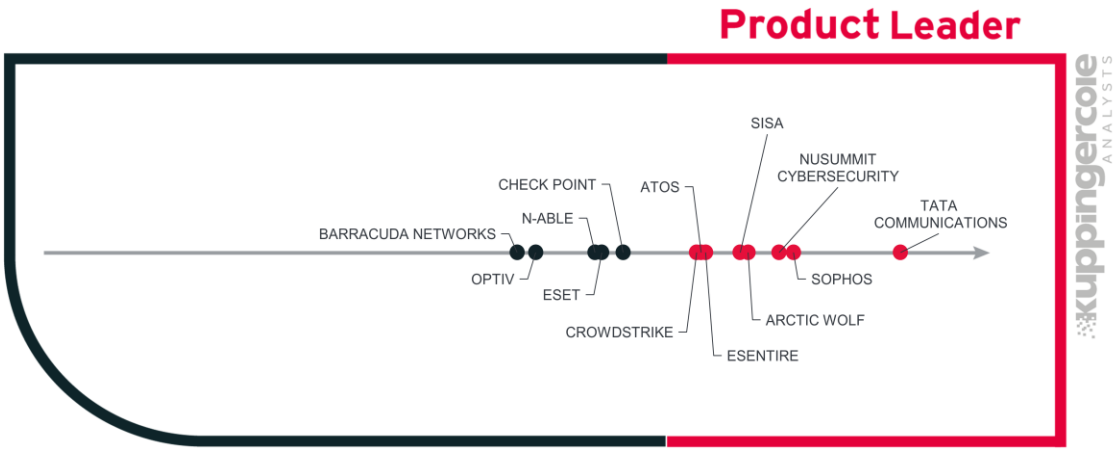
eSentire's Atlas platform and round-the-clock operations deliver strong multi-signal detection and response, while explainable, auditable AI-led investigations drive innovation and support continued market growth.

NuSummit Cybersecurity's services-led CogniX MDR delivery is reinforced by a deep library of detections, automations, and integrations, while its Agentic AI roadmap and platform enhancements strengthen innovation alongside an expanding international presence.

SISA's ProACT Agentic SOC combines a forensics-led MDR model with broad telemetry coverage, integrated SIEM/SOAR capabilities, and Agentic AI-assisted investigations, supported by flexible deployment, strong compliance alignment, and growing global presence.

Product Leadership

Product leadership is the first specific category examined below. This view is based on the presence and completeness of required features as defined in the required capabilities section above. The chart is horizontal and divided into two areas, the vendors to the right of the chart and colored red are Product Leaders and those to the left and colored black are Product Leadership Challengers.

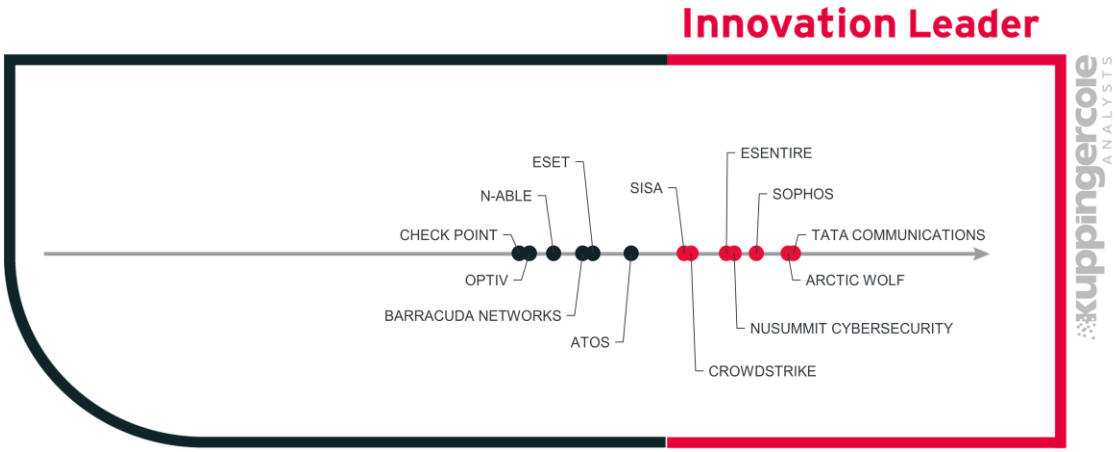


The Product Leaders in order of placement are Tata Communications, Sophos, NuSummit Cybersecurity, Arctic Wolf, SISA, eSentire, Atos, and CrowdStrike. Product leaders have the most complete mix of functionality, security, interoperability, deployment options, and usability, as defined in the required capabilities section above.

The remaining vendors are challengers in Product Leadership.

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 based on the evaluation of innovative features recently added together with the vendor's history in innovation. The chart is horizontal and divided into two areas, the vendors

to the right of the chart and colored red are Innovation Leaders and those to the left and colored black are Innovation Leadership Challengers.

Innovation Leaders are those vendors that deliver cutting-edge products, not only in response to customers' requests but also because they are driving technical changes in the market by anticipating what will be needed in the months and years ahead.

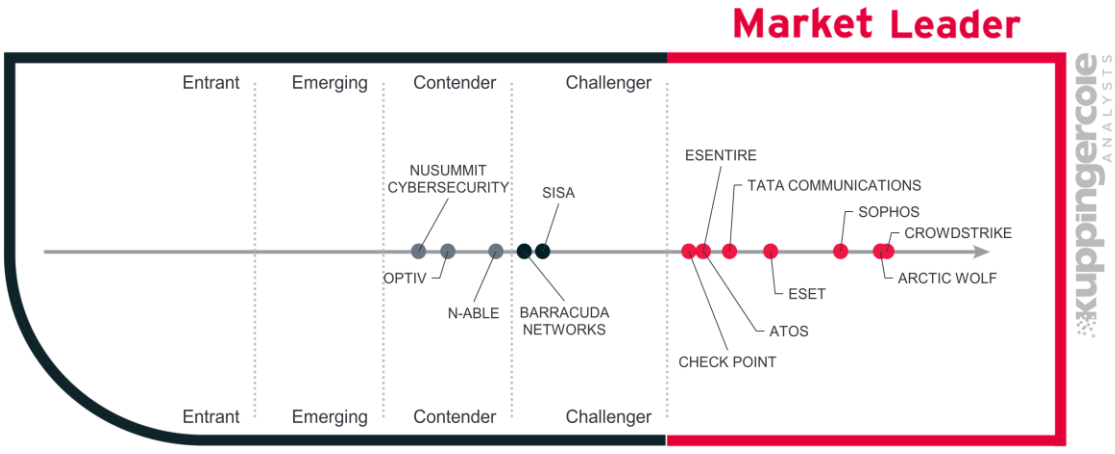
There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers. Innovative features in MDR include GenAI and Agentic AI support for analysts; coverage of IoT, OT, ICS, and SCADA environments; ransomware remediation; lateral movement detection, containment, and mapping; and automated identity protection, response actions, proactive threat hunting, patch management, and content management.

The Innovation Leaders are Tata Communications, Arctic Wolf, Sophos, NuSummit Cybersecurity, eSentire, CrowdStrike, and SISA. Tata Communications tops the list with its agent-assisted triage, extremely closely followed by Arctic Wolf with its GenAI-supported investigation automation and playbook optimization.

Other vendors placed as challengers in Innovation Leadership.

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers and their geographic distribution, 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.



CrowdStrike leads the MDR market, reflecting its broad global customer base, large scale deployments, extensive partner ecosystem, and strong financial position. Arctic Wolf follows very closely, with comparable geographic reach and a sizable installed base across mid-

market and enterprise segments. Sophos is not far behind, supported by its established channel network and wide international presence.

ESET forms the next tier, demonstrating solid global coverage and a growing MDR footprint. Tata Communications follows, benefiting from its telecommunications heritage and international service capabilities. A closely grouped set of vendors comprising Atos, eSentire, and Check Point also demonstrate meaningful market leadership, each with global customers and partner ecosystems, though at a smaller scale than the top-tier vendors.

SISA and Barracuda Networks follow as challengers, reflecting solid customer bases and growing geographic reach, but with smaller global scale, partner ecosystems, and overall deployment footprints than the Market Leaders.

N-able, Optiv, and NuSummit Cybersecurity are positioned as Contenders, reflecting more regionally concentrated customer bases and service footprints, with narrower global reach and smaller scale of MDR deployments compared with the Leaders and Challengers. The MDR market continues to grow rapidly, creating substantial opportunities for all vendors to expand their global reach, customer bases, and partner ecosystems as MDR becomes a core component of security operations.

Product and Vendor Evaluation

This section provides a structured evaluation of each product and vendor included in this KuppingerCole Analysts Leadership Compass. Each profile contains a description of the company and its offering, an analysis of relevant capabilities for this market segment, and an assessment of strengths and challenges. Where applicable, vendors are positioned as Leaders in the Product, Innovation, or Market categories.

In addition to these standard Leadership Compass categories, we provide detailed capability ratings for every vendor. These ratings are visualized in a spider chart that reflects performance across the functional and technical criteria defined for this market segment. The spider chart complements the written analysis and enables direct comparison across solutions.

For this Leadership Compass, the capability categories evaluated are described below.

Security: This covers the degree of security provided by the product or service. For products, it looks at internal security practices and controls that enable secure customer use, including authentication, access controls, and encryption. It also considers known vulnerabilities, how the vendor responds to them, and the presence of relevant security features. For services, it evaluates the security and consistency of operational processes and the presence of pertinent certifications.

Deployment: This covers how easy or difficult it is to deploy, operate, and discontinue the product or service. For products, it considers implementation effort, operational complexity, and the degree to which required components are integrated. It also looks at what is needed to manage the solution over time, including upgrades and decommissioning. For services, it evaluates the number and complexity of deployed components and the effort required to set up and run the service.

Interoperability: This covers the ability of the product or service to integrate with other vendors' products and widely used standards and technologies. It considers support for common protocols and formats, as well as the availability of secure and well-documented APIs for programmatic access. For service providers, it also evaluates the ability to deliver solutions that integrate into customer applications, infrastructure, and operational workflows.

Usability: This covers how easy the product or service is to use and administer. For products, it looks at whether user interfaces are logical and intuitive and whether the experience is consistent across the vendor's components. It also considers administrative efficiency and the clarity of configuration and reporting workflows. For services delivered by system integrators or managed service providers, it evaluates customer experience through the quality of service delivery, communications, and day-to-day operational interactions.

Coverage: This covers the breadth of the solutions' coverage in terms of monitoring and analysis of data movement across applications, systems, endpoints, protocols, groups, networks, and locations. It also evaluates integrations with other security technologies.

Cloud/container support: This covers 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 (CSPM), Cloud Workload Protection (CWP), and vulnerability scanning.

Detection: This covers the threat detection coverage and capabilities of the solutions 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.

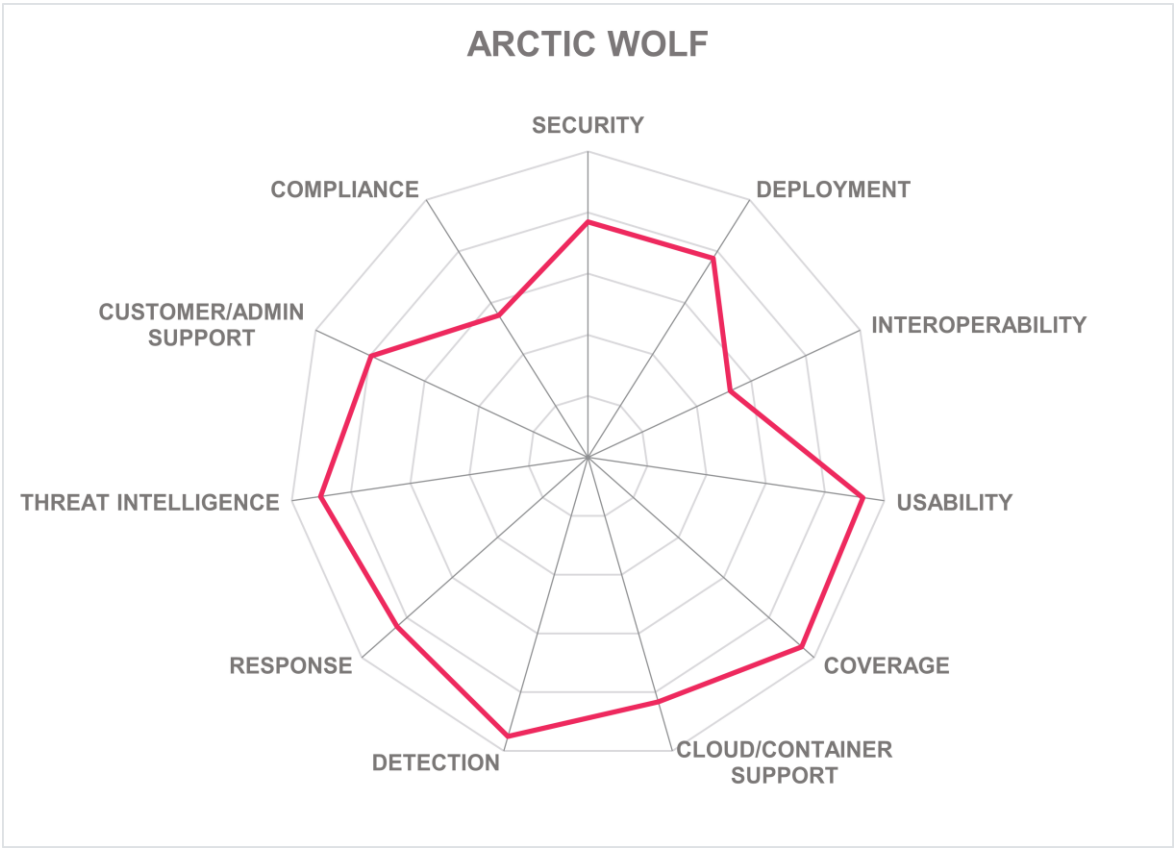
Response: This covers the ability of the solutions to respond to threat detections, including automated response actions, software patching capabilities, response times, SOC capabilities, ransomware blocking, SOAR capabilities, and provision of IR playbooks.

Threat intelligence: This covers a solution's threat intelligence and threat hunting capabilities, including the provision of ASM, threat exposure management, automated threat hunting, reporting on emerging threats, real-time threat intelligence integration, and support for threat intelligence exchange standards.

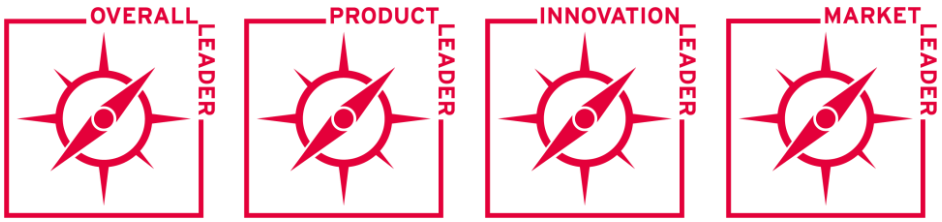
Compliance: This covers the vendors' compliance with key standards and ability of their solutions to produce detailed, audit-ready logs and reports aligned with the relevant cybersecurity regulations and industry standards.

Customer/admin support: This covers the support provided by the solution to customers in terms of services, mapping of threats to standard frameworks, cyber insurance support, dashboards, collaboration, reporting, forensic services, continuous improvement, risk management, and industry-sector and language support.

Arctic Wolf – Arctic Wolf MDR



Leadership



Arctic Wolf is a private cybersecurity company founded in 2012 and headquartered in Eden Prairie, Minnesota, in the US. The company specializes in security operations, with MDR and Security Operations Center as a Service (SOCaaS) as its core offerings. Arctic Wolf serves organizations of all sizes, with most customers in the medium-sized and mid-market segments, followed by large enterprises and small businesses. Customers are primarily located in North America (NA), with a strong presence in Europe, Middle East, and Africa (EMEA) and growing adoption in Asia-Pacific (APAC). Arctic Wolf MDR is delivered as a

SaaS offering through a 100% channel partner model, with licensing based on users, appliances, and servers under fixed-price contracts.

Arctic Wolf MDR is delivered through the Arctic Wolf Aurora Platform, which is built on an open XDR architecture and ingests telemetry from a customer's existing security technology stack. The service combines continuous monitoring by the Arctic Wolf concierge SOC (cSOC) with proactive security posture improvement delivered by the Concierge Security Team. Arctic Wolf offers its MDR service in three packages: Security Operations Core, Plus, and Total. All packages include MDR, log retention, data search, and access to the concierge team. Higher tiers add managed risk services, security awareness, and an IR retainer. Engagement levels are further differentiated through Silver, Gold, and Platinum concierge tiers, which define the frequency and depth of proactive engagements.

Arctic Wolf's concierge operating model is a key feature, which treats MDR as an ongoing service rather than an isolated response function. Arctic Wolf assigns named security experts to each customer, who provide recurring in-depth security posture reviews and guidance on risk reduction. Experienced analysts review tickets before delivery to ensure context-rich and actionable information. Arctic Wolf refreshed the user interface in the past year to support a unified view across detection, investigation, and posture management, and includes attack path mapping and guided remediation. Areas for improvement include limited visibility of shadow IT activity and the absence of native integrations with third-party vulnerability and exposure management platforms.

Arctic Wolf MDR provides round-the-clock monitoring and response across endpoints, servers, email systems, identity platforms, Edge environments, IoT devices, mobile devices, and remote users. It supports all major operating systems and browsers and includes ITDR capabilities. The service analyzes network and application-layer traffic, including Domain Name System (DNS), Hypertext Transfer Protocol Secure (HTTPS), Remote Desktop Protocol (RDP), Secure Shell (SSH), Internet Protocol Security (IPsec), and Voice-over-Internet Protocol (VoIP) communications. It also supports selected IoT and industrial protocols including Modbus, Message Queuing Telemetry Transport (MQTT), and Distributed Network Protocol 3 (DNP3). Arctic Wolf provides integrations for a wide but not exhaustive range of third-party Endpoint Protection, Detection, and Response (EPDR) and XDR tools such as the CrowdStrike Falcon Platform and Palo Alto Networks Cortex XDR, and for a range of NDR tools such as Check Point Horizon NDR. The service can ingest syslog from third-party SIEMs, but it does not offer connectors for third-party SIEM platforms. Arctic Wolf MDR also provides connectors for a small range of Data Loss Prevention (DLP) and Data Security Posture Management (DSPM) tools such as Microsoft Purview DLP, for identity platforms such as Microsoft Entra ID, and for Secure Access Service Edge (SASE) platforms such as Netskope Intelligent SSE. The solution can discover but not monitor shadow IT. Arctic Wolf supports the OCSF.

The service delivers continuous monitoring and response across cloud infrastructure and SaaS applications. It includes CSPM, CWP, and vulnerability scanning for customer environments. Arctic Wolf MDR analyzes telemetry from container platforms and serverless workloads, including Kubernetes, Amazon Elastic Kubernetes Service (EKS), AWS Lambda, Microsoft Azure Functions, and Google Cloud Platform (GCP) services. It correlates events

from cloud DNS, gateways, and API gateways to detect exfiltration and command-and-control activity. Arctic Wolf provides native monitoring for a small range of cloud services, including Microsoft Entra ID, Microsoft 365, Microsoft Defender for Cloud Apps, and Google Workspace, and offers several out-of-the-box (OOTB) Microsoft 365 integrations, but not including Microsoft Teams. The solution also has connectors for a narrow range of third-party CSPM platforms, including Microsoft Defender for Cloud. AWS GuardDuty and Microsoft Azure integrations are expected to add support for Wiz CNAPP (Cloud Native Application Protection Platform) and Palo Alto Networks Prisma Cloud in the second half of 2026.

Arctic Wolf MDR detects a broad range of threats across endpoint, network, cloud, and identity data. Detection capabilities include account compromise, credential misuse, lateral movement, privilege escalation, and Multifactor Authentication (MFA) bypass. Network detections include east-west traffic analysis and on-demand packet capture. Analytics correlate identity, device, and network telemetry to identify anomalous access patterns. File Integrity Monitoring (FIM) supports baseline and periodic scans of endpoints. User Behavior Analytics (UBA) is fully managed by Arctic Wolf analysts, with no requirement for customer tuning or management.

The solution supports a wide range of response actions, including host isolation, session termination, DNS redirection, rollback of configuration changes, and Just-in-Time (JIT) privilege revocation through identity integrations. Automated containment is available when approved by customer policy. Arctic Wolf MDR can block ransomware before encryption and isolate affected systems if execution occurs. The platform includes native SOAR capabilities and more than 50 response playbooks. On-site assistance and post-remediation validation are available if required, but the solution does not include automated software patching.

Arctic Wolf MDR includes integrated threat intelligence and proactive threat hunting delivered by a dedicated team. The service draws intelligence from customer deployments, technology partners, and external sources, and applies real-time feeds for enrichment and correlation. Threat exposure management and vulnerability assessment are included as part of MDR, with targeted advisories issued to affected customers. Arctic Wolf analysts perform automated and manual threat hunting on a continuous basis, and regular reporting covers emerging threats and hunting outcomes. Arctic Wolf operationalizes intelligence across the customer base to improve detections for newly observed threats.

Innovation within Arctic Wolf MDR focuses on analyst effectiveness and proactive security improvement. The company has invested heavily in ML and GenAI to improve usability, detection quality, and response workflows. Recent additions include an AI Security Assistant for query generation and investigation support, dynamic optimization of response playbooks, and automation of early investigation tasks. Activity recording and playback support forensic analysis, while decoy credentials and ransomware simulation tools enhance detection and preparedness. Structured human-in-the-loop processes maintain human oversight.

Arctic Wolf MDR supports customer compliance with ISO 27001 and SOC 2 Type II and aligns detections and reporting with the MITRE ATT&CK® framework. The service provides reporting to support regulatory requirements such as the EU’s NIS2, Digital Operational

Resilience Act (DORA), and General Data Protection Regulation (GDPR). Arctic Wolf is preparing the service for alignment with FIPS 197 in the US. Guaranteed data and metadata residency is available for the US, the EU, and Australia. The service cannot be deployed inside infrastructure that the customer owns or directly controls for data sovereignty or residency purposes.

On-site support is available in NA, EMEA, and APAC. Arctic Wolf provides support and documentation only in English and German. Customers can fully outsource security operations or engage in co-managed models. Arctic Wolf assigns each customer a dedicated analyst, risk advisor, and customer success manager. Dashboards, attack path mapping, insurer-ready incident reports, and a Return on Investment (ROI) calculator are included. Arctic Wolf offers cyber insurance coverage, and forensic services can be delivered remotely or on site when needed.

Arctic Wolf MDR is suitable for organizations of all sizes and for Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) seeking an MDR service backed by a large global SOC. Organizations across multiple industries use the solution, with strong adoption in finance, healthcare, manufacturing, and chemical and pharmaceutical sectors. It is particularly relevant for organizations that want continuous monitoring combined with proactive security posture improvement and guided risk reduction without building or expanding an internal SOC.

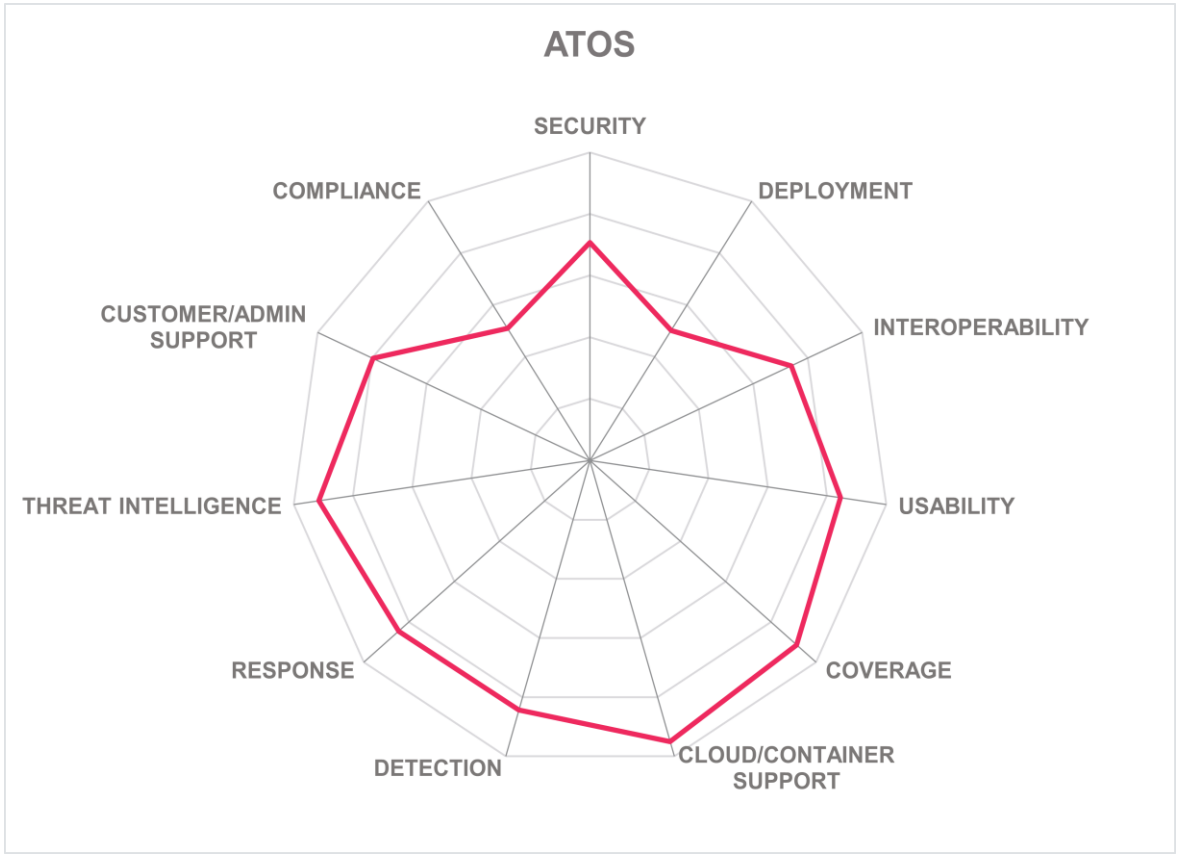
Strengths

- Concierge security team with scheduled posture reviews
- Open XDR platform with broad telemetry ingestion
- 24/7 monitoring with global SOC coverage
- Fixed price contracts with unlimited log ingestion
- Strong ITDR coverage
- Native SOAR workflows and guided remediation support
- Cloud, container, and serverless monitoring support
- Real-time threat intelligence enrichment and correlation
- Dedicated customer analyst and risk advisor support

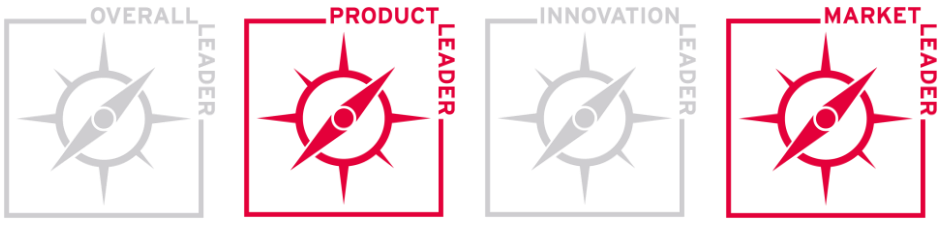
Challenges

- Limited shadow IT monitoring capabilities
- No native third-party SIEM connectors
- Limited native third-party EPDR, XDR, and NDR connectors
- Does not support automated patching, but this is on the roadmap
- Narrow third-party CSPM integration coverage
- Cannot run in customer-controlled environments

Atos – Atos MDR/AIsaac



Leadership



Atos is a publicly listed cybersecurity and digital services company founded in 1997, with global headquarters in Bezons, France. North American headquarters are in Irving, Texas, in the US. Atos operates in 61 countries and serves mainly mid-market organizations, followed by medium-sized and large enterprises. Atos delivers Atos MDR as a managed service through managed security service providers and channel partners. Atos prices the service as an integrated offering based on estimated alert volumes and data ingestion and deploys it primarily on cloud infrastructure, with support for on-premises and private cloud projects.

Atos MDR is the core of the Atos Threat Detection, Investigation and Response (TDIR) capability and combines the Atos AIsaac AI-based platform with partner technologies. The service supports a core SIEM and EDR function using AIsaac, Microsoft Sentinel, Google Chronicle, or combinations of these. It includes built-in SOAR, integrations with third-party EPDR and NDR platforms, Atos-developed algorithms for identity detection and ML models for threat hunting and alert triage, a GenAI assistant for security operations, and global threat intelligence and digital risk protection services.

A key strength is the Atos global delivery model with 17 SOCs sharing detection logic, threat intelligence, and investigation expertise across regions. The Atos Enterprise Security Dashboard provides consolidated visibility, supports faster decision making, and simplifies reporting and audit preparation. Atos has long-standing experience in AI for security operations, boosted by its strategic partnership and integration with AI technology firm Qevlar. Atos was early in applying ML to threat detection and alert triage. Areas for improvement include the lack of self-service dashboard creation for customers and limited native support for customer-managed orchestration workflows.

The service provides round-the-clock monitoring and response across managed and unmanaged assets, including endpoints, networks, identity systems, mobile devices, Edge environments, IoT, and OT systems. It supports most major operating systems and browsers, except Apple Safari, and analyzes encrypted and unencrypted traffic across common IT, OT, and industrial protocols. ITDR is included. The platform integrates with a broad range of SIEM, XDR, EPDR, NDR, DLP, identity, SASE, and exposure management platforms, including Microsoft Sentinel, CrowdStrike Falcon Platform, Fortinet FortiNDR, Palo Alto Networks Cortex XSOAR, Okta Workforce Identity, and Microsoft Entra ID. Shadow IT can be discovered through scans using Tenable or Qualys and related activity can be monitored through ingested telemetry. Atos supports the OCSF.

Atos MDR delivers continuous monitoring and response across public and private cloud services and SaaS platforms. It includes CSPM, CWP, and vulnerability scanning across multi-cloud environments. The service monitors Kubernetes clusters, serverless functions, and container workloads, and correlates events from cloud control planes, gateways, and DNS services to identify anomalous access and exfiltration attempts. The platform provides extensive OOTB integrations for Microsoft 365, including Exchange Online, SharePoint, and Teams, as well as leading CSPM platforms such as Tenable and other exposure management tools. The platform also integrates with Amazon Web Services (AWS), Microsoft Azure, and GCP services, including Kubernetes and serverless services. A dedicated MDR connector team develops additional integrations on request to support customer specific cloud services, SaaS applications, and security technologies.

Detection capabilities span identity, endpoint, network, and cloud telemetry across data centers, public cloud platforms, and remote users. The service detects account compromise, credential misuse, privilege escalation, lateral movement, and MFA bypass, including RDP anomalies, suspicious east-west traffic patterns, and malware beaconing. It supports UBA and attacker behavior analytics that are fully managed by Atos and not self-managed by customers. Network based detections include traffic analysis but not on-demand full packet

capture. AI models and real-time threat intelligence enrich and correlate alerts, resulting in an average detection time of two minutes across the monitored estate.

Response actions include automated and guided containment such as session termination, JIT privilege revocation, configuration rollback, prevention of unauthorized configuration changes, and DNS-based controls including traffic redirection and blocking. The platform supports fully automated containment when policy approval and governance controls allow it. The service can block ransomware before encryption starts through managed EDR integration and can isolate compromised hosts or disable risky user sessions. There is no native patching capability, but this is on the roadmap. Remediation and patch coordination, including policy-based automated patching for Atos managed systems, are available through Atos vulnerability services. Built-in SOAR features include structured playbooks, evidence collection, post incident validation, and defined Service Level Objectives (SLOs) for response times.

Threat intelligence is provided by Atos global platforms and the Atos Threat Research Center. The MDR service includes automated and manual threat hunting, regular reporting on emerging threats, and exposure-based prioritization. Intelligence is sourced from customer environments, technology partners, and commercial feeds and is used to train detection models and enrich investigations. Atos offers asset discovery and ASM as optional services. The platform supports all major threat intelligence exchange standards.

Innovation is evidenced by investment in ML and other forms of AI across detection, triage, and analyst workflows. The service includes an AI-based investigation assistant and search assistant powered by LLMs to support analysts with alert summarization, contextual enrichment, and natural language query creation, as well as code and configuration generation. It also supports simulation of ransomware attacks and selected threat scenarios to validate defenses. Customers can develop their own connectors and threat hunting models within the platform. There is no native deception technology or forensic activity replay, although these can be implemented through existing third-party customer tools and optional BAS services from Atos.

Atos has SOC 2 Type I and Type II attestations and maintains ISO 27001 certification for its information security management systems (ISMS) across its global operations. It aligns detection and reporting to the ATT&CK framework and maps incidents to tactics and techniques. The solution does not provide regulatory compliance reports, but compliance assessments for NIS2, DORA, and GDPR are available through Atos advisory services. The platform supports data and metadata residency across multiple jurisdictions, including the EU, the US, the UK, France, Germany, and India.

Customer and administrator support includes round-the-clock service delivered through global SOCs, with on-site support available in major regions. Atos provides support in 11 languages, while it provides documentation only in English. Customers can fully outsource their SOC or choose co-managed models. Atos assigns a dedicated customer success manager and primary analyst to each customer. The company collaborates with cyber insurance providers and can produce insurer-ready incident reports, but insurance is not included. Atos offers digital forensics and IR services as optional extras.

Atos MDR is suited to managed service providers, managed security service providers, and organizations from small enterprises through large global organizations. It is particularly relevant for sectors such as manufacturing, finance, government, retail, insurance, and energy that require global coverage, deep operational expertise, and integration with existing security investments.

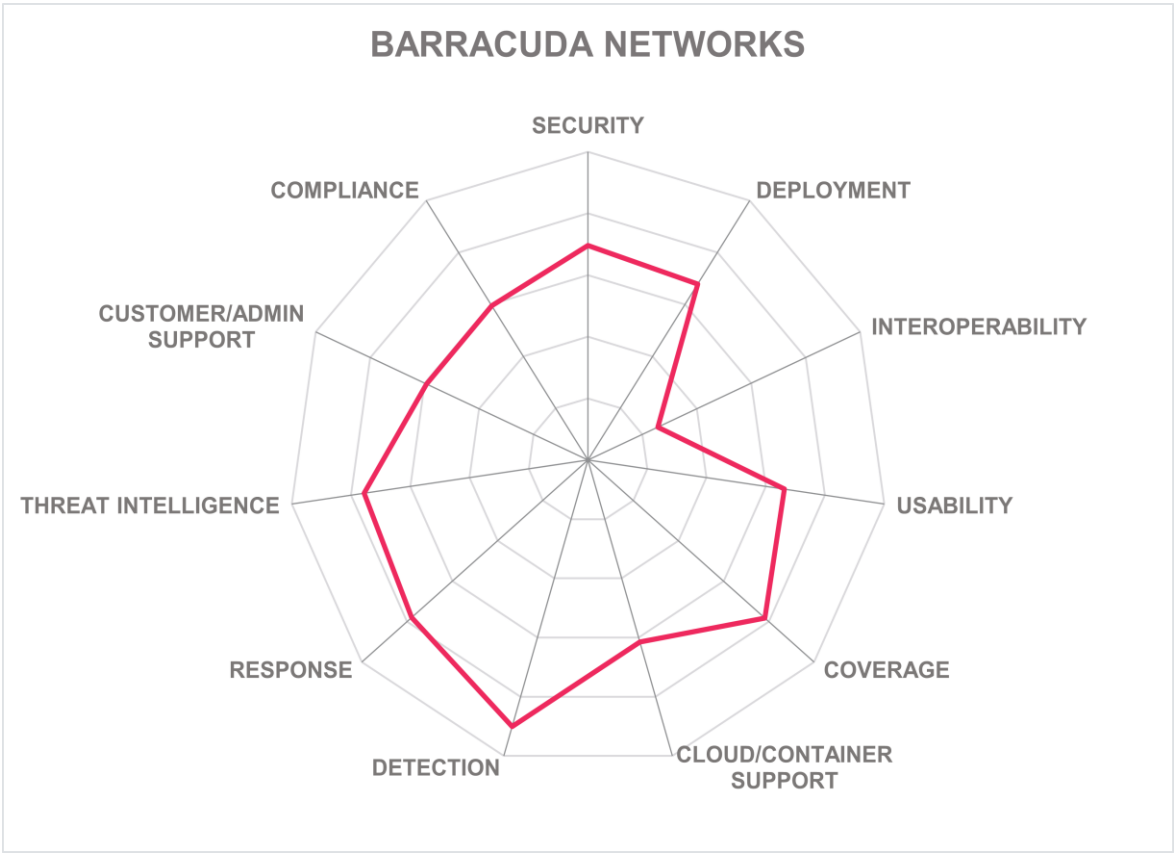
Strengths

- Global delivery model with 17 interconnected SOCs
- Technology agnostic MDR integrating multiple SIEM and XDR platforms
- Deep threat intelligence sharing across global SOC network
- Mature AI for alert triage and detection
- Broad coverage across managed and unmanaged assets
- Strong identity threat detection and response capabilities
- Integrated Enterprise Security Dashboard for operational visibility
- Predictable service-based pricing aligned to alert volumes

Challenges

- No third-party SOAR integrations by default
- Limited customer self-service for dashboard creation
- No built-in software patching within MDR service, but on the product roadmap
- Documentation available only in English

Barracuda Networks – Barracuda Managed XDR



Barracuda Networks was founded in 2003 and is headquartered in Campbell, California, in the US. The company is privately owned by equity firm KKR. Barracuda delivers its MDR capability through its Managed XDR (MXDR) offering and targets organizations of all sizes, with most customers in the medium segment, followed by small businesses. Most customers are in NA, followed by APAC and EMEA. Barracuda delivers the service as a SaaS offering exclusively through MSPs, MSSPs, and channel partners. Deployment supports log collectors that can run on-site or self-hosted, with data residency options for the US, EU, Canada, Ireland, Germany, and India.

Barracuda MXDR is sold as a modular service that allows customers to select only the security domains they wish to cover. The portfolio includes cloud security, email security, endpoint security, server security, network security, and vulnerability security. These services combine threat detection and response capabilities with risk detection through vulnerability scanning, which is based on Rapid7 technology and delivered as a managed

service. Customers can choose any combination of these services. Pricing is based on the number of protected assets within each domain, such as users for cloud and email, endpoints for endpoint security, servers for server security, and firewalls or network devices for network security. Customers can obtain endpoint security either as a fully managed service, including a SentinelOne license, or as a monitored service using a customer-supplied EDR license. Barracuda delivers the solution under a SaaS model via MSPs, MSSPs, and channel partners. Barracuda Networks is developing bundled “good, better, and best” packages to simplify procurement through a per-user model and potentially combine MXDR with other Barracuda services.

A key strength of the service is the breadth of automated threat responses across endpoints, cloud services, and network devices, including Microsoft 365 and Google Workspace. Customers can respond to alerts directly within the dashboard and provide structured feedback that supports detection tuning. Automated containment can occur within seconds without manual intervention. The dashboards are clear and metric-rich, with strong reporting and threat statistics. The interface has a slightly retro feel and would benefit from modernization. There is no support for the OCSF, and integrations with third-party SIEM, NDR, and SOAR platforms remain limited.

Barracuda MXDR provides round-the-clock monitoring across endpoints, servers, email, identity systems, IoT, Edge environments, and remote workers, but excludes mobile devices. It supports Windows, Linux, and macOS, as well as all major browsers including Safari. The solution analyzes encrypted and unencrypted network and application-layer traffic, including DNS, HTTPS, RDP, SSH, IPsec, and VoIP communications. The platform supports EtherNet/IP but does not support other Industrial Control System (ICS) protocols. Integrations include selected EPDR/XDR and identity products such as Microsoft Defender for Endpoint, Sophos Intercept X with XDR, Microsoft Entra ID, Okta Workforce Identity, and Cisco Duo. There are no native connectors for third-party DLP, DSPM, or most SASE platforms.

The service delivers 24/7 monitoring across cloud services and SaaS applications. It includes CSPM and CWP capabilities but does not perform vulnerability scanning across multi-cloud estates. It monitors unusual administrative activity, suspicious logins, and anomalous resource sharing. The platform analyzes telemetry from Amazon EKS, AWS Lambda, Azure Functions, and GCP services. The platform correlates events from cloud DNS and API gateways to detect exfiltration and command-and-control attempts. Kubernetes environments are not monitored. Microsoft 365 integrations are extensive, including Teams.

Detection capabilities include identification of account compromise, credential misuse, lateral movement, MFA bypass, and token theft. Network detections capture east-west traffic and support on-demand packet inspection. The solution correlates identity, device, and network telemetry and performs FIM. The provider can manage UBA fully or co-manage it with customers. The platform detects privilege escalation, abnormal data access, unusual uploads and downloads, and potentially unwanted programs (PUPs). Integration with third-party IDS and IPS is available. Barracuda reports an average detection time of two minutes.

Response capabilities include automated containment, DNS redirects, configuration rollback, and prevention of unauthorized changes. Privileged Access Management (PAM) and Identity Provider (IdP) integrations enable JIT privilege revocation and session termination. The platform can deprovision users through System for Cross-domain Identity Management (SCIM) or other APIs, while the platform allows federated authentication via Security Assertion Markup Language (SAML). Software patching is not included. Ransomware can be blocked before encryption. SOAR functionality is native to the platform. Post remediation validation is included. There is no on-site assistance, but remote forensic services are available. SLAs apply to MXDR operations.

The service draws threat intelligence from commercial feeds, open-source data, technology partners, and telemetry from hundreds of thousands of customers across the company's broader portfolio. The platform uses real-time feeds for enrichment and correlation. The service supports most intelligence exchange standards except OpenIOC. Continuous vulnerability assessment and CTEM services are included, with prioritized remediation guidance. The solution includes both automated and manual threat hunting, supported by a dedicated team. There is no built-in ASM capability.

The solution integrates AI, mainly in the form of ML, across detection, usability, abnormal activity identification, insider threat detection, and broader threat analysis. The platform also uses ML to optimize response playbooks dynamically and simulate potential threats. GenAI facilitates log search, Structured Query Language (SQL) query generation, alert and investigation summarization through LLM assistance, dashboard interaction, and code and configuration creation. It does not leverage GenAI for policy authoring or compliance reporting. The platform includes user and attacker behavior analytics, advanced SOC-customized endpoint detections, automated remediation, decoy hosts and data artifacts, and support for BAS. There is no ransomware simulation and no activity recording or playback for forensic reconstruction.

Barracuda MXDR holds SOC 2 Type I and Type II attestations. It aligns detections and reporting with the ATT&CK framework and maps incidents to tactics and techniques. It does not provide compliance reporting for NIS2, DORA, or GDPR. The platform provides data residency in several jurisdictions including the US, EU, Canada, Ireland, Germany, and India. The solution can operate within customer-controlled environments to address sovereignty requirements.

The service can fully outsource the SOC function or operate in co-managed mode. Barracuda provides support and documentation only in English. The platform includes an ROI calculator. Attack path mapping is available to select customers, but Barracuda plans to broaden access to all customers. The platform can generate insurer-ready reports after incidents, but cyber insurance is not bundled. The service supports remote forensic evidence gathering. On-site support and tailored industry-specific services are not available.

Barracuda MXDR is suitable for MSPs and MSSPs and for organizations from small businesses to large enterprises. It is particularly relevant for manufacturing, retail, healthcare, multi-location organizations, and government organizations that require managed protection across endpoint, network, email, and cloud environments. The service

appeals to resource-constrained security teams seeking strong automation and consolidated security services delivered through channel partners.

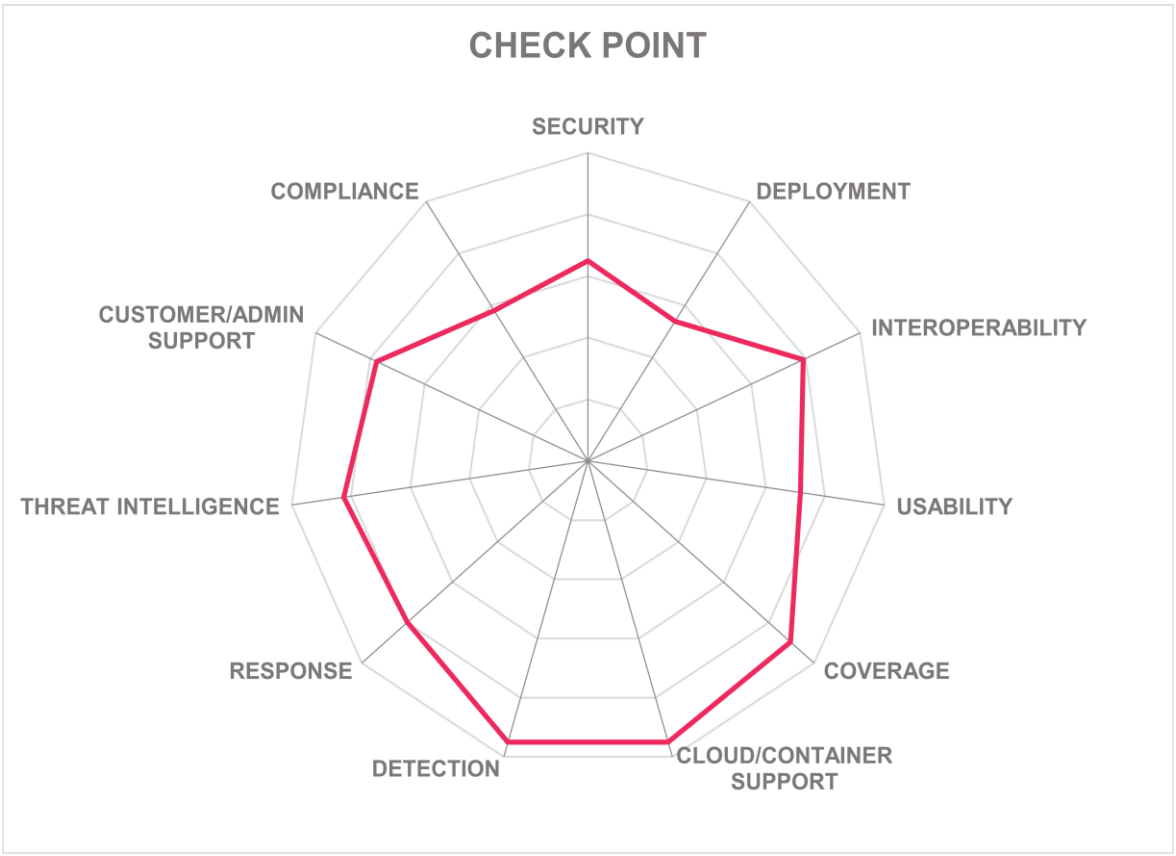
Strengths

- Broad automated threat response coverage
- Integrated SIEM and native SOAR
- Strong Microsoft 365 integrations
- Google Workspace automated containment support
- Rapid average threat detection time
- Extensive cross portfolio threat intelligence
- Flexible asset-based licensing model
- Global 24/7 SOC operations
- Managed vulnerability assessment integration
- Includes some deception techniques

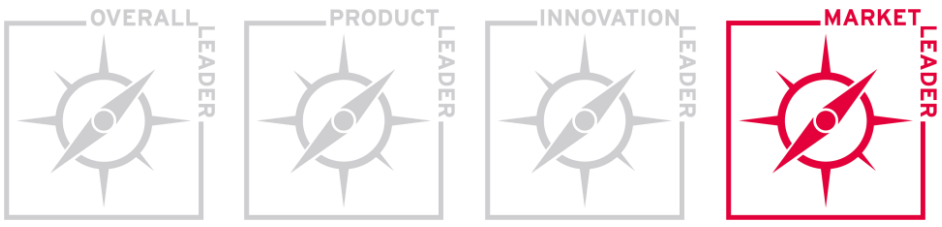
Challenges

- Limited third-party NDR, SIEM, and SOAR integrations
- No mobile device coverage, but this is on the roadmap
- No on-site support services
- Dashboard modernization required
- Limited Kubernetes monitoring support
- Lacks compliance reporting

Check Point – Check Point MDR for Workspace/MDR 360°



Leadership



Check Point was founded in 1993 and is headquartered in Tel Aviv, Israel. It operates in 182 countries and provides network, endpoint, cloud, exposure management, and security capabilities for AI applications and usage through its Infinity platform. Check Point delivers Check Point MDR as a SaaS-based managed service within Check Point Services. Customers range from small businesses to large enterprises, with most in the medium-sized

business segment across EMEA and NA. Check Point offers the service directly and through MSSPs and channel partners in two packages: MDR for Workspace and MDR 360°.

Check Point MDR is built on the Infinity platform and provides 24/7 monitoring, detection, and response through a global follow-the-sun SOC. MDR for Workspace targets smaller organizations, while MDR 360° addresses mid-market and enterprise requirements with a modular structure and optional add-ons. The service is agentless and vendor-agnostic, integrating alerts through API connections and, where required, a co-managed Microsoft Sentinel SIEM layer. Pricing is per user per year, with volume tiers for MDR 360°. Optional add-ons include identity threat detection, advanced data sources, and cyber resilience service hours for red teaming, compromise assessment, and consulting.

The primary user interface is the Check Point Infinity Portal, which offers intuitive, menu-driven navigation and a clear executive dashboard. The platform synchronizes incidents bidirectionally with Microsoft Sentinel and Microsoft Defender, enabling customers to work within their preferred console. Check Point has enhanced reporting to provide deeper visibility into detection sources and tuning opportunities. The portal could benefit from modernization, but a “major” user interface update is planned for mid-2026 to introduce a more analyst-centric workflow and greater investigation transparency. The base MDR services do not include ITDR, but customers can add it as an optional extra.

Check Point MDR provides full alert resolution where required and can discover and monitor shadow IT. It covers Windows, Linux, macOS, Android, iOS, and Chrome OS, as well as all common browsers. Monitoring extends to endpoints, servers, email, identity systems, Edge environments, IoT, ICS, and Supervisory Control and Data Acquisition (SCADA) environments, and remote workers. It analyzes encrypted and unencrypted network and application-layer traffic, including DNS, HTTPS, RDP, SSH, IPsec, and VoIP communications, as well as OT protocols including Modbus, MQTT, and DNP3. It integrates with a wide range of third-party EPDR and XDR platforms such as SentinelOne Singularity Platform, a wide range of NDR solutions including Fortinet FortiNDR and Check Point Horizon NDR, SIEM platforms such as Microsoft Sentinel, SOAR platforms including Palo Alto Networks Cortex XSOAR, DLP solutions such as Microsoft Purview DLP, identity and access platforms including Microsoft Entra ID, SASE platforms such as Netskope Intelligent Security Service Edge, and exposure management tools including Tenable One Cloud Security. It supports the OCSF.

The service delivers 24/7 monitoring and response across cloud services and SaaS applications. It includes CWP, CSPM, and vulnerability scanning for multi-cloud environments. It monitors unusual administrative activity, suspicious logins, abnormal resource sharing, and changes to virtual private clouds, and analyzes workload telemetry from Kubernetes, container platforms, and serverless functions such as Amazon EKS, AWS Lambda, and Microsoft Azure Functions. The platform correlates events from cloud DNS, gateways, and API gateways to detect exfiltration and command-and-control detection. OOTB integrations include Microsoft 365, Microsoft Teams, Microsoft Defender for Cloud Apps, Google Workspace, and connectors to third-party CSPM platforms such as Wiz CNAPP and CSPM.

Detection capabilities span identity, endpoint, and network telemetry. The service can detect account compromise, credential misuse, lateral movement, MFA bypass, and token theft. Network detections include east-west traffic analysis, on-demand full packet capture, and investigation of unknown signals. Check Point states an average detection time of one minute. The platform supports user and attacker behavior analytics in managed, self-managed, or co-managed modes. The service detects privilege escalation, abnormal access to sensitive data, unusual file transfers, and PUPs, and integrates with third-party IDS and IPS.

Check Point MDR offers a wide range of automated response actions, including configuration rollback, DNS redirection, session termination, and JIT privilege revocation through privileged access management or identity provider integration. It can automatically deprovision users through SCIM or API calls, it supports authentication through SAML, and it supports automated containment when approved by policy. Software patching is available with automated scanning and customizable policies. The service blocks ransomware before encryption, responds to phishing in real time, and addresses cloud misconfigurations and living-off-the-land techniques. It includes its own SOAR capability and provides post remediation validation. Check Point offers an SLA, and forensic support is available.

Threat intelligence is powered by Check Point Threat Cloud and global research teams. The service includes continuous vulnerability assessment, CTEM, and prioritized remediation guidance. The MDR team conducts automated and manual threat hunting, and regular reporting covers posture and emerging threats. Threat intelligence feeds and open-source data train ML models, and the platform operationalizes intelligence from customer deployments and partners in real time. The platform supports major threat intelligence exchange standards, except OpenIOC. ASM and BAS are available as optional add-ons rather than standard components.

Innovation centers on its Open Garden MDR 360° approach, which refers to an agentless, vendor-agnostic integration model. The modular, integration-first design is aimed at enabling customers to retain existing investments, avoid vendor lock-in, and tailor the service to their own technology stack. The acquisition of Lakera in 2025 adds dedicated security for AI capabilities, enabling MDR to detect misuse of AI applications, prompt injection attempts, shadow AI usage, and data leakage from AI interactions as part of its monitoring and response scope. Innovation also includes expanded third-party integrations and analyst workflow enhancements.

The platform uses ML for usability improvements, anomaly detection, insider threat detection, and predictive threat hunting. The service includes user and attacker behavior analytics, decoy credentials, and DNS sinkhole deception, as well as activity recording and playback for forensic analysis. It does not use GenAI for policy creation, compliance reporting, or dynamic playbook generation, but LLM support for analyst summarization is on the roadmap. Check Point MDR aligns with the ATT&CK framework and generates reports mapping detected threats to tactics and techniques. It supports regulatory reporting for NIS2, DORA, and GDPR. The service offers guaranteed data residency for the US, Canada, EU, UK, UAE, Australia, and India. It can also operate within customer-controlled environments. It has SOC2 Type II attestation but is not certified for ISO 27001.

Check Point delivers general MDR support only remotely and only in English, with documentation also only in English. Customers can fully outsource the SOC function or adopt a co-managed model. Check Point assigns each customer a dedicated analyst and a customer success manager. Regular risk assessment reporting, attack path mapping, and policy development assistance are included. The platform can generate insurer-ready reports after incidents. Dedicated risk advisor services are optional, and there is no cyber insurance bundled with the service. Check Point offers pre-sales trials and can deliver forensic services remotely or on site.

Check Point MDR is suitable for organizations of all sizes and for MSPs and MSSPs seeking an agentless, vendor-agnostic service integrated with the Infinity platform. It is widely used in government, manufacturing, chemical and pharmaceutical, aerospace and defense, and other regulated sectors. Organizations that require deep Microsoft integration, AI security capabilities, and modular service selection will find MDR 360° of particular interest.

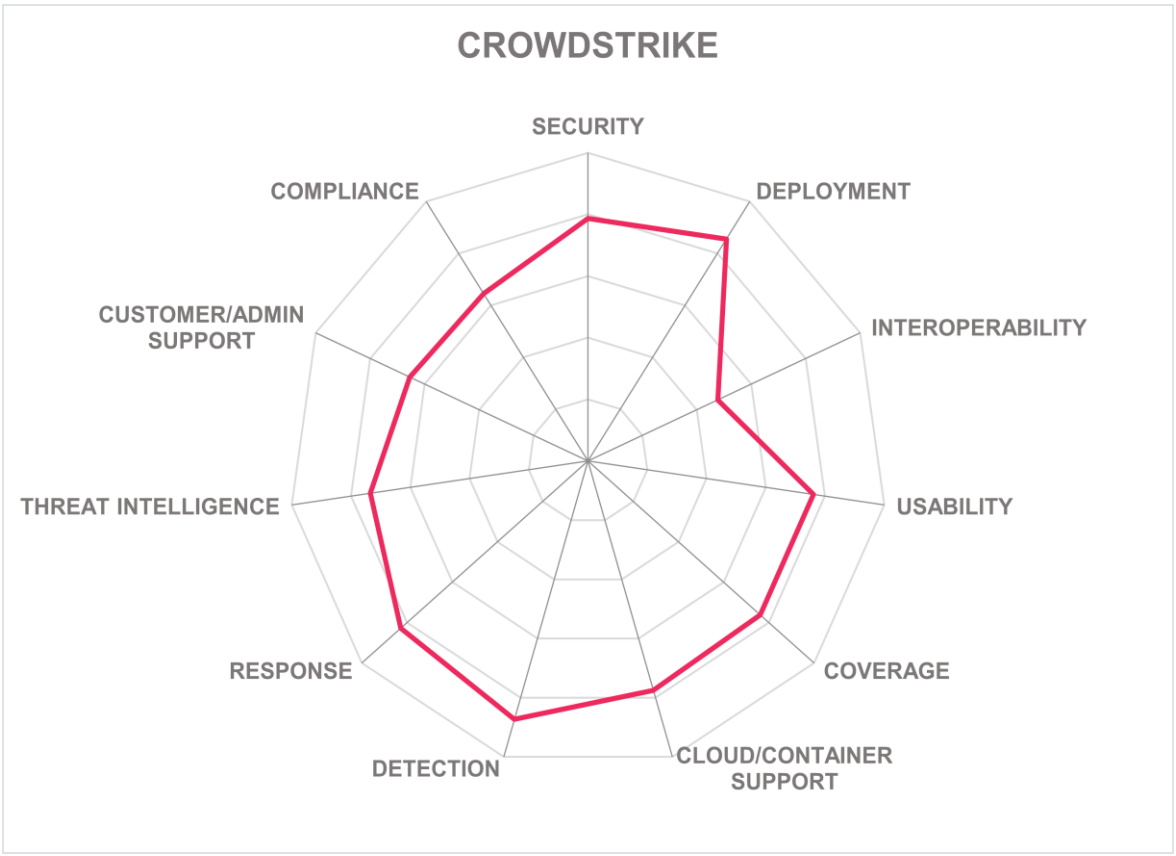
Strengths

- Agentless vendor-agnostic MDR architecture
- Many integrations for DLP, EPDR, NDR, SASE, and other security solutions
- Can detect AI misuse, shadow AI usage, prompt injection, and data leakage from AI applications
- Strong global threat intelligence resources
- Modular pricing
- Software patching functionality
- Encrypted Traffic Analysis
- Support for OT/ICS environments
- Activity recording and forensic playback
- Guaranteed data residency for multiple geographic regions

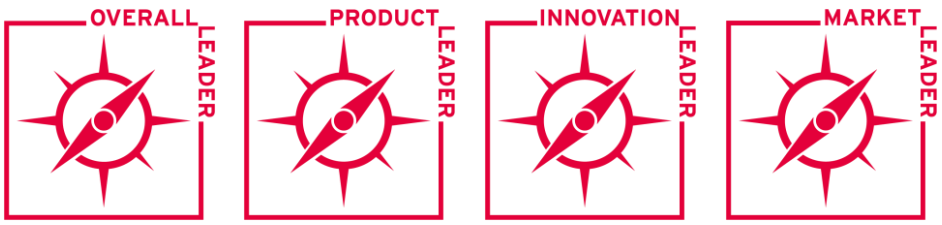
Challenges

- Not ISO 27001 certified
- No on-site support included
- English-only support and documentation
- No bundled cyber insurance offering
- ITDR, ASM, and BAS are add-ons

CrowdStrike – Falcon Complete MDR



Leadership



CrowdStrike is a publicly traded cybersecurity company founded in 2011 and headquartered in Austin, Texas, in the US. The company specializes in threat prevention, detection, and response delivered through the Falcon platform. Falcon Complete MDR serves organizations from small businesses to large enterprises, with most customers in medium-sized and mid-market segments. Customers are mainly based in NA, followed by EMEA, APAC, and Latin America (LATAM). The service is delivered as a SaaS offering, licensed

annually and deployed through a lightweight endpoint sensor, with delivery available directly or through MSSPs and channel partners.

Falcon Complete MDR delivers continuous human-led monitoring, investigation, and response across endpoints, identities, cloud workloads, and third-party data sources. The service operates on the Falcon platform and uses Falcon Next-Gen SIEM to correlate telemetry across security domains. Licensing for Falcon Complete MDR is modular and based primarily on the number of protected endpoints, with additional components licensed separately by identities, cloud workloads, and data ingestion volumes for Falcon Next-Gen SIEM. Customers receive full-cycle response, including containment and remediation, without managing the underlying tooling. CrowdStrike offers the service as a bundled MDR subscription, with optional add-ons for Identity Protection, Falcon Cloud Security, and Falcon Next-Gen SIEM. Falcon Flex provides an alternative procurement model that allows organizations to commit to an agreed level of spend and allocate that spend across Falcon modules, including Falcon Complete MDR, over time. Customers can activate, expand, or change enabled capabilities during the contract term without initiating new procurement cycles. This approach supports phased platform adoption, reduces administrative overhead, and provides predictable costs while allowing security capabilities to evolve in line with operational and risk requirements.

CrowdStrike's flat "Fire Team" operating model removes tiered analyst handoffs and allows a single team to investigate, contain, and remediate incidents from initial detection through to resolution. The Falcon Complete Hub provides a unified browser-based interface that brings together alerts, escalations, dashboards, action items, and analyst communication for a unified view of all MDR activities. AI-supported investigation using CrowdStrike's Charlotte AI accelerates triage and analysis through a combination of GenAI and Agentic AI built on a multi-model architecture of LLMs and smaller task-specific models. The service is designed to investigate, contain, and remediate threats directly, instead of simply raising alerts and handing off the work. CrowdStrike reports a median time to contain of one minute. Areas for improvement include support for OT/ICS environments and features such as breach simulation.

Falcon Complete MDR provides continuous monitoring and response across endpoints, servers, email systems, identity platforms, Edge environments, IoT-connected assets, and remote users. It supports Windows, Linux, and macOS, but not Android, iOS, or Chrome OS. It covers all common browsers except Opera. The service can analyze encrypted and unencrypted network and application-layer traffic, including DNS, HTTPS, RDP, SSH, and VoIP communications, but does not analyze industrial protocols. Integrations via Falcon Next-Gen SIEM include Microsoft Defender for Endpoint and Trend Micro Vision One for EPDR and XDR telemetry, Arista NDR, ExtraHop RevealX, Darktrace DETECT and RESPOND, and Cisco Secure Network Analytics for NDR, Microsoft Sentinel for SIEM ingestion, Microsoft Entra ID for identity telemetry, and Netskope Intelligent SSE for SASE visibility. Native Falcon Fusion SOAR is included. Shadow IT can be discovered but not monitored. CrowdStrike supports the OCSF.

The service provides round-the-clock monitoring and response across cloud services and SaaS applications. It includes CWP, but not CSPM within the standard MDR subscription.

The platform analyzes telemetry from container and serverless environments including Amazon EKS, AWS Lambda, Microsoft Azure Functions, and GCP services. The service monitors Kubernetes clusters and correlates events from cloud DNS, gateways, and application programming interfaces for command-and-control or exfiltration attempts. Integrations include Microsoft Defender for Cloud and AWS Security Hub for CSPM data ingestion, and extensive Microsoft 365 integrations including Teams. The platform extends monitoring to Google Drive, Microsoft Defender for Cloud Apps, and Google Workspace, with telemetry correlated in Falcon Next-Gen SIEM for cross-domain detection and response.

Falcon Complete MDR detects account compromise, credential misuse, lateral movement, MFA bypass, and token theft through identity and endpoint telemetry correlation. It detects privilege escalation, abnormal data access, suspicious file transfers, and PUPs. Network detections include east-west traffic analysis and unknown signal investigation, but not on-demand packet capture. Analytics correlate identity, device, and network data to identify anomalous access. FIM is not included by default. UBA can be provider-managed, customer-managed, or co-managed. The service integrates with third-party IDS and IPS.

The service provides automated and analyst-driven response actions such as host isolation, process termination, rollback of configuration changes, and JIT privilege revocation through identity integrations. Security teams can enable automated containment through predefined security postures. Falcon Complete MDR can block ransomware prior to encryption and remove adversary persistence without reimaging. The service includes native SOAR capabilities and predefined response playbooks, but not software patching. The standard MDR service does not include on-site response and forensic services, but these are available at an additional cost if required.

Falcon Complete MDR includes proactive threat hunting backed by CrowdStrike intelligence teams that track hundreds of adversary groups. The service derives threat intelligence from global telemetry, external intelligence feeds, and customer environments, with real-time enrichment during investigations. CrowdStrike analysts perform automated and manual threat hunting continuously, and customers receive regular reporting on emerging threats. Vulnerability assessment, exposure management, and ASM are not included in the MDR service, although CrowdStrike exposure insights are used to inform analyst investigations and advisory guidance.

CrowdStrike continues to invest heavily in AI and automation within Falcon Complete MDR. Charlotte AI supports analysts by explaining command lines, summarizing investigations, and accelerating triage. ML models support detection, predictive threat hunting, and insider threat identification. Recent innovations include the Falcon Complete Hub interface and software agent-assisted investigation workflows. CrowdStrike uses AI mainly for detection and response efficiency rather than policy generation or compliance automation. Deception technologies, BAS, and ransomware simulation are not part of the offering.

CrowdStrike has obtained a SOC 2 Type II attestation, it has achieved US Federal Risk and Authorization Management Program (FedRAMP) High authorization, it has ISO 27001 certification, it has attained Security, Trust, Assurance, and Risk (STAR) Level 1 and STAR

Level 2, it is compliant with UK Cyber Essentials, and it has Germany's C5 attestation. The service aligns detections and reporting with the ATT&CK framework and provides reports mapped to tactics and techniques. Regulatory reporting support is available for NIS2, DORA, and GDPR. CrowdStrike offers guaranteed data residency in the US and the EU. The service does not operate within customer-controlled environments.

CrowdStrike provides follow-the-sun 24/7 operations with support available globally. Support services and documentation are available in English and Japanese, and CrowdStrike has a global ecosystem of partners for additional local language requirements. CrowdStrike assigns customers to Fire Teams rather than individual analysts, which provides continuity and shared expertise. Dashboards, attack path visualization, and insurer-ready incident reports are included. The service includes a warranty of up to $2M. The service does not include cyber insurance or pre-sales trial access.

Falcon Complete MDR is suitable for organizations of all sizes that require continuous monitoring and hands-on response without building an internal SOC. It is also relevant for MSSPs through the Falcon Complete for Service Providers program. The service is used across many industries, with strong adoption in healthcare, finance, government, manufacturing, and retail. It is particularly relevant for organizations with complex attack surfaces that want unified detection and response delivered through a single platform and human-led operations.

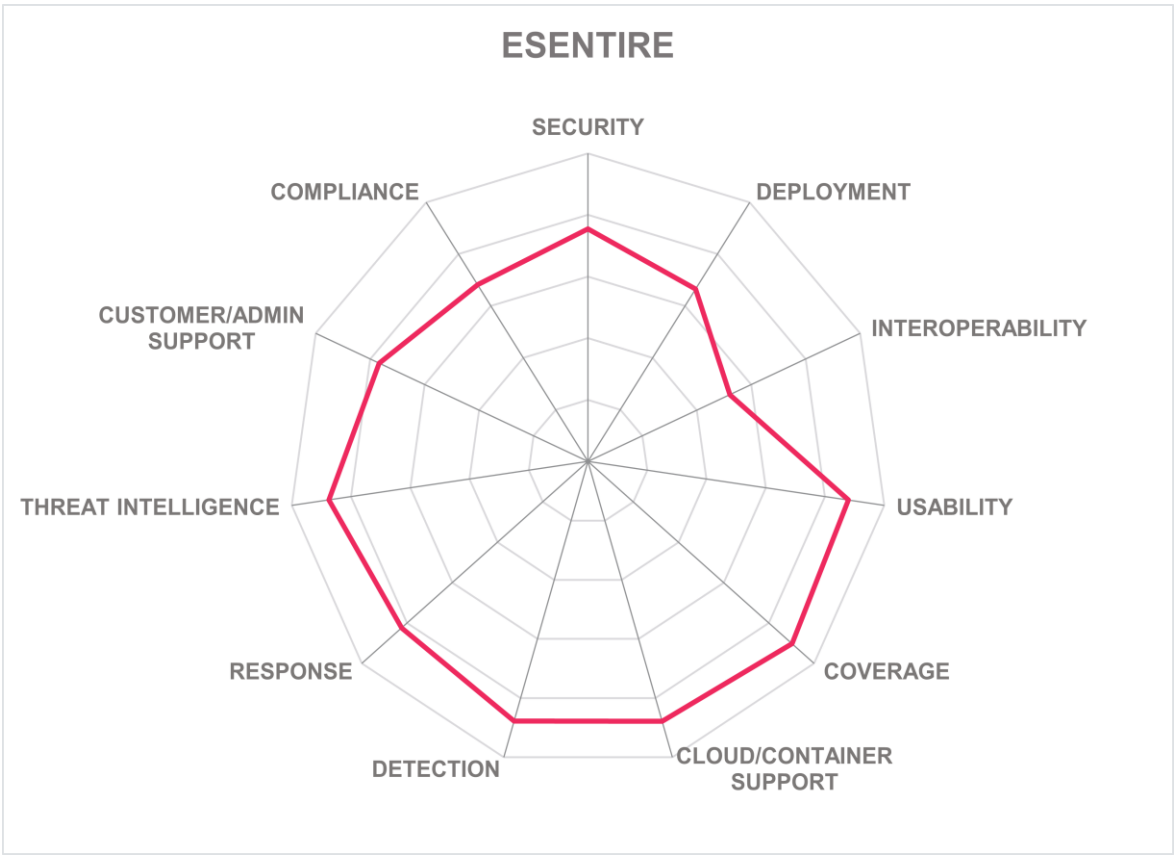
Strengths

- Flat Fire Team model with consistent analyst ownership
- Native SOAR and fast automated containment capabilities
- AI-assisted investigation and triage through Charlotte AI
- Unified Falcon Complete Hub user interface
- Strong identity threat detection and response coverage
- Global follow-the-sun SOC operations
- Many security certifications

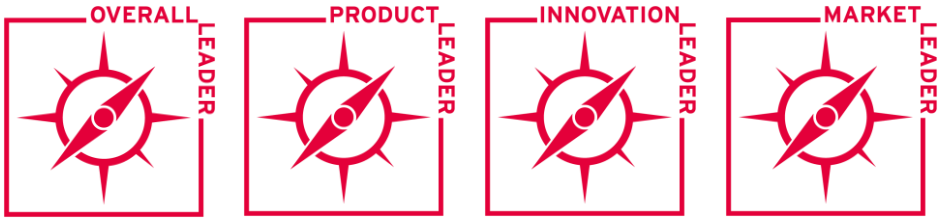
Challenges

- Limited on-site response in the cost of the standard MDR service
- No deception or breach simulation capabilities
- No support for OT/ICS protocols
- Data residency limited to selected regions

eSentire – eSentire MDR



Leadership



eSentire is a private global MDR provider founded in 2001 in Canada, with headquarters and a SOC in Waterloo, Ontario, and an additional SOC in Cork, Ireland. The company serves customers in 80 countries. Most customers are medium-sized organizations, followed by mid-market enterprises, with a smaller proportion in the small business and large enterprise segments. The majority are in NA, followed by EMEA and APAC. eSentire MDR is delivered as a SaaS-based service built on the company's Atlas platform, with seat-based licensing.

The platform provides cloud-hosted management and analytics combined with on-premises components for network, endpoint, and log data collection.

eSentire MDR combines its Atlas XDR platform with multi-signal telemetry ingestion and 24/7 SOC operations. Atlas AI operates as a multi-agent system embedded across the platform, performing AI-led investigations with transparent evidence, tool calls, and confidence scoring. SOC analysts review and validate findings, enrich and tailor investigations, and escalate to the eSentire Threat Response Unit (TRU) or IR team when required. There are also configurable response options to enable autonomous response based on AI investigations where speed is important. eSentire MDR is available in three packages: Essentials, Advanced, and Complete, ranging from foundational MDR with unlimited logging to a full service with vulnerability management, IR support, and a named cyber risk advisor.

The Atlas AI Supervisor Architecture spawns dedicated investigator, critic, and reporter agents for each incident to replicate analyst workflows. The “Findings” capability provides full visibility into investigation paths, timelines, evidence, and human validation status in a clear, clean interface. Dynamic dashboards and natural language query generation allow customers to build role-based views aligned to operational priorities. Areas for improvement include limited native bidirectional SOAR integrations and the absence of automated software patching.

eSentire MDR delivers round-the-clock coverage across endpoints, servers, email, identity systems, Edge environments, IoT devices, mobile platforms, and remote users. It supports Windows, Linux, macOS, Android, iOS, and Chrome OS, and analyzes network and application-layer traffic including DNS, HTTPS, RDP, SSH, IPsec, and VoIP communications, as well as selected OT protocols such as Modbus and EtherNet/IP. Integrations include selected EPDR and XDR solutions such as the CrowdStrike Falcon Platform, Microsoft Defender for Endpoint, SentinelOne Singularity, Palo Alto Networks Cortex XDR, and Deep Instinct, as well as NDR solutions including Fortinet FortiNDR and Check Point Horizon NDR.

SIEM integrations include Microsoft Sentinel, Splunk Enterprise Security, and Sumo Logic Cloud SIEM. The platform also integrates with Microsoft Purview DLP, Netskope Intelligent SSE, Zscaler Data Protection, Microsoft Entra ID, Okta Workforce Identity, Prisma SASE, Tenable One, and Wiz. The Atlas platform can connect to any security control or product that exposes data or response controls via REST APIs. A REST API exposes Findings and ticketing for integration with IT service management (ITSM) and SOAR tools. Shadow IT can be discovered and monitored. The Atlas data schema is not based on the OCSF, but the platform can ingest OCSF-formatted data and map it to its internal data model.

The service provides continuous monitoring across cloud services and SaaS applications and includes CSPM and CWP with vulnerability scanning. It monitors suspicious logins, unusual administrative activity, and configuration changes across environments including Microsoft 365, and Google Workspace. Atlas analyzes telemetry from Amazon EKS, AWS Lambda, Azure Functions, and GCP services; correlates DNS and API gateway activity; and

monitors Kubernetes. The platform provides connectors for selected third-party CSPM and CNAPP tools.

The solution provides detection across endpoint, network, identity, cloud, and email telemetry, correlating multi-signal data to identify anomalous activity and active threats. It can detect account compromise, credential misuse, lateral movement, privilege escalation, abnormal access to sensitive data, unusual file uploads or downloads, and identity credential abuse, including MFA bypass and token theft. Network-based detections include east-west traffic analysis for insider threat and advanced persistent threat activity, on-demand full packet capture, and investigation of unknown signals.

The platform correlates identity, device, and network telemetry with TRU intelligence to deliver contextualized findings. User and attacker behavior analytics are included, with profiling and ML models to identify deviations such as impossible travel or suspicious PowerShell activity. eSentire reports an average detection time of one minute across customer environments. The platform does not provide FIM.

The solution provides a broad set of automated and analyst-driven response capabilities across endpoint, network, identity, and cloud environments. Automated actions include host isolation, DNS redirects, rollback of configuration changes, prevention of unauthorized configuration updates, and initiation of on-demand full packet capture on selected segments or endpoints. The platform can enforce JIT privilege revocation and session termination through PAM and IdP integrations. It supports authentication via SAML and can automatically deprovision users or disable risky sessions using SCIM or API-based controls.

Atlas includes built-in SOAR functionality with prescribed orchestration runbooks and dynamically generated playbooks created by Atlas AI for each investigation. While the service does not include software patching, it scans for outdated software and provides remediation guidance. The platform supports fully automated containment when approved by policy. Post-remediation validation ensures that threats have been neutralized and have not resurfaced, and on-site IR assistance is available if required under the defined SLA.

Threat intelligence is driven by eSentire’s TRU, which conducts proactive threat hunts, threat sweeps, and structured research across more than 37 commercial, open source, and industry intelligence feeds, as well as intelligence derived from customer investigations and technology partners. The TRU curates intelligence into proprietary eSentire feeds and operationalizes it across the global customer base in near real time. eSentire reports that 99% of the indicators delivered in these feeds are confirmed to correspond to malicious activity in customer environments, resulting in a very low false-positive rate.

eSentire also reports that many of these indicators are identified and operationalized before they appear in widely used commercial threat intelligence feeds. The TRU operationalizes findings into new detections, runbooks, and ML models, and delivers regular advisories and monthly briefings. The service supports STIX, TAXII, and MISP. eSentire provides risk-based remediation guidance for managing threat exposure based on vulnerability data and analyst assessments. However, dedicated functionality for continuous discovery of external-facing assets for ASM purposes is not included.

Innovation centers on Atlas AI and its explainable, auditable investigation framework. The platform logs every AI decision and supports human validation and AI auditing through an internal quality assurance process. GenAI facilitates query creation, playbook development, compliance reporting, and investigation summaries. ML enables anomaly detection, attacker behavior analytics, predictive hunting, and SOC quality assurance. The Supervisor Architecture coordinates multiple AI agents per investigation to replicate analyst workflows with transparent evidence and confidence scoring.

eSentire MDR aligns with the ATT&CK framework and generates reports mapping detected threats to tactics and techniques, with detections continuously updated against the ATT&CK knowledge base. The service provides compliance reports for NIS2, DORA, and GDPR and holds SOC 2 Type II attestation and ISO 27001 certification, with support for customer compliance with PCI DSS, HIPAA, FIPS 197, and NIST 800-57. eSentire offers data residency in the US and EU through regional Atlas deployment on AWS, and Atlas can also be deployed as a single customer stack in any AWS region where all required AWS services are available.

Support includes 24/7 SOC services, a dedicated customer success manager, and optional cyber risk advisors at higher tiers, with customers able to choose pooled or dedicated service models based on maturity and need. eSentire provides on-site support in NA, EMEA, and APAC, and delivers services in English and French, with documentation in English, French, and Spanish. Customers can outsource the SOC entirely or adopt a co-managed model. The solution includes regular risk assessment reporting, assistance with security and governance policy development, insurer-ready incident reports, ROI calculation, and remote or on-site forensic services, but cyber insurance is not included.

eSentire MDR is suitable for organizations of all sizes and for MSPs and MSSPs seeking a managed, AI-driven security operations capability. It is particularly relevant for finance, legal, healthcare, manufacturing, and business services organizations that require rapid containment, proactive threat hunting, and continuous exposure management, and that value explainable AI combined with human-led response.

Strengths

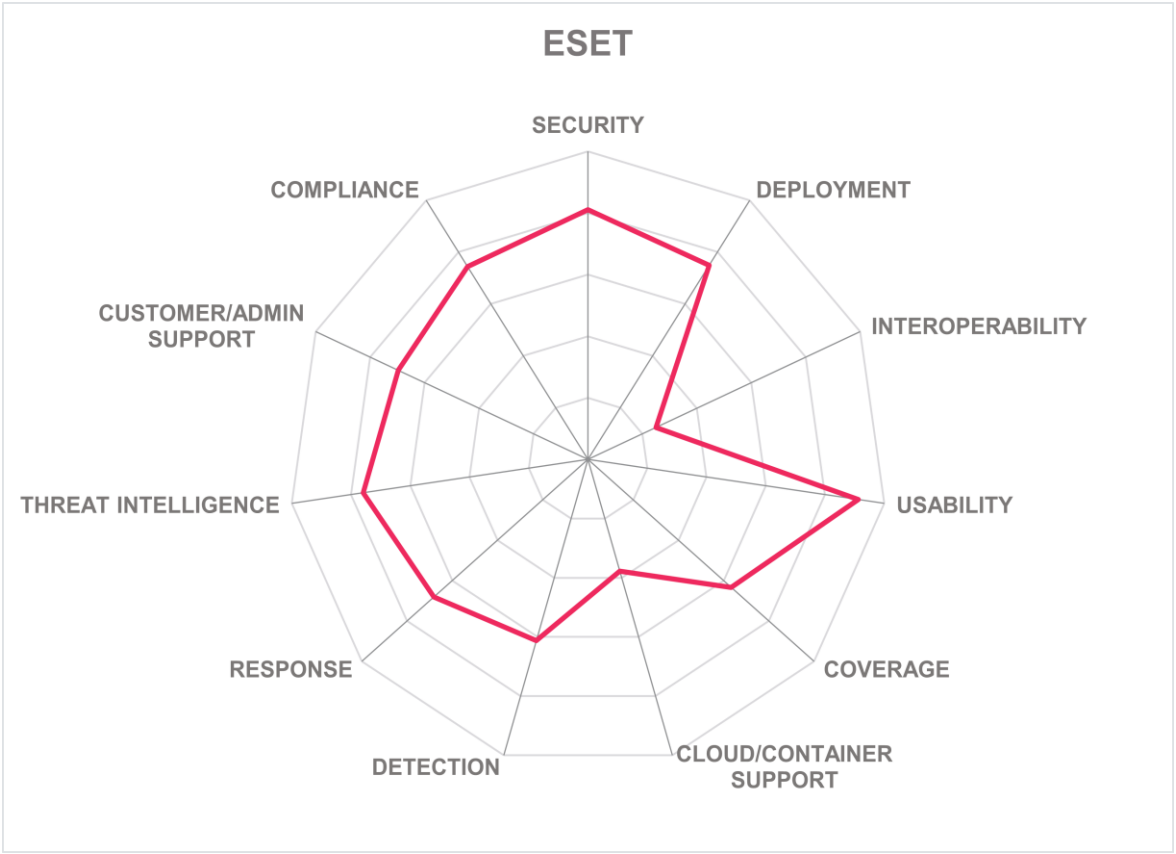
- Explainable multi-agent Atlas AI investigations
- Human validated AI-led findings
- Transparent and auditable investigation timelines
- Strong threat intelligence capability
- Analyzes key OT protocols
- Continuous proactive threat hunting
- Broad multi-signal telemetry ingestion
- Built-in SOAR with dynamic playbooks
- Flexible, tiered MDR service packages
- Extensive API-driven platform interoperability

Challenges

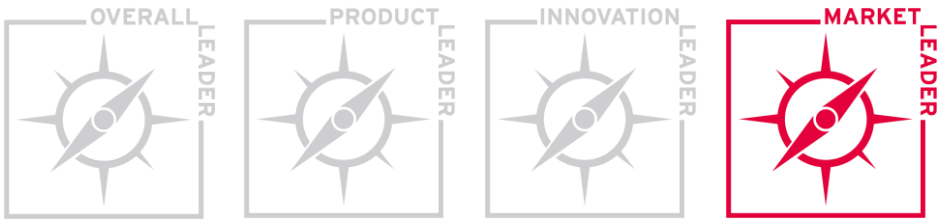
- Limited native third-party SOAR integrations

- No external ASM capability
- No baseline FIM
- Does not include automated software patching

ESET – ESET PROTECT MDR



Leadership



ESET is a private cybersecurity company founded in 1992 and headquartered in Bratislava, Slovakia. ESET PROTECT MDR is aimed mainly at small businesses with fewer than 50 employees, followed by medium-sized organizations with up to 1,000 employees. Most customers are in EMEA, followed by APAC, NA, and LATAM. ESET licenses the service per protected asset with a minimum commitment of 25 assets. Customers can deploy the service as a SaaS offering with optional on-premises elements, and it is sold directly as well as through MSPs and channel partners. MSSP delivery is planned.

ESET PROTECT MDR is delivered through the ESET PROTECT Platform, which combines endpoint protection, XDR, SIEM, and SOAR capabilities with continuous SOC supervision. ESET offers the service in two tiers: ESET PROTECT MDR and ESET PROTECT MDR Ultimate. Both provide 24/7 monitoring, threat triage, rapid containment, threat hunting, and tailored weekly and monthly reporting. MDR Ultimate adds guided deployment, deeper investigations, customized historical hunting, digital forensics assistance, and a dedicated IR lead.

The ESET PROTECT Console provides customers with clear visibility into incidents, response actions, and analyst commentary. The user interface is clean and well-structured with clear dashboards, incident timelines, configurable notifications, and direct visibility into SOC actions. ESET response actions are supported by automation and experienced SOC teams. The inclusion of ESET's AI Advisor by default in MDR Ultimate lowers the skills barrier for smaller organizations. Areas for improvement include expanding third party telemetry integrations and further strengthening identity focused detection and response capabilities.

ESET PROTECT MDR provides monitoring and response coverage across endpoints, servers, and email systems, supporting Windows, Linux, macOS, Android, iOS, and Chrome OS, as well as all common browsers including Safari. It can analyze common encrypted protocols such as DNS, HTTPS, and RDP, but offers limited support for industrial protocols, with EtherNet/IP as the primary exception. The platform provides integrations for a narrow set of SIEM and security analytics platforms including Microsoft Sentinel, Splunk, IBM Security QRadar SIEM, Wazuh, and Elastic Security, with log export via syslog and open API support for custom integrations. There are a limited number of connectors for third-party EPDR/XDR and NDR platforms, including Cisco XDR, and Stellar Cyber, but no native integrations with DLP or SASE solutions. There are no integrations with identity security tools, but it can integrate with Microsoft Entra ID and Active Directory repositories. The solution can discover and monitor shadow IT. ESET offers BAS as an optional extra. ESET does not natively support OCSF, but its Open XDR data model is based on the Elastic Common Schema (ECS). ECS-modeled data can be mapped to OCSF where required, although this may require transformation.

The service provides monitoring, analysis, and response across cloud services and SaaS applications. It does not include multi-cloud vulnerability scanning but includes CWP, with CSPM on the roadmap. There are no native connectors to cloud service providers or third-party CSPM platforms, and telemetry from containers, Kubernetes, and serverless environments such as Amazon EKS or Azure Functions is not yet supported, although enhancements are on the roadmap. ESET provides strong OOTB integration with Microsoft 365 and Google Workspace, but monitoring of other major SaaS services such as Salesforce, Zoom, Box, GitHub, Jira, and Workday is not included.

Detection capabilities span ransomware, phishing, privilege escalation, insider threats, and abnormal access to sensitive data. The platform includes UBA and attacker behavior analytics, enabling detection of anomalous user activity, credential misuse, lateral movement, unusual file uploads or downloads, and suspicious command execution patterns across endpoints. It supports custom rule creation for FIM use cases and can alert on

unauthorized modification of specific files, configurations, or logs. Network-based detections include inspection of east-west traffic, but there is no OOTB integration with third-party IDS or IPS. The platform provides limited identity-related detection derived mainly from endpoint telemetry and does not support detection of modern token theft techniques.

ESET PROTECT MDR supports automated containment actions such as isolating hosts, killing processes, and blocking executables, with policy-based approval. The service includes software patching through ESET Vulnerability and Patch Management. It can block ransomware before encryption and provides post-remediation validation. The platform includes built-in SOAR functionality, although integrations with external orchestration tools remain limited. The solution cannot enforce JIT privilege revocation or session termination via PAM or IdP integration and cannot automatically deprovision users or disable risky sessions via SCIM, SAML, or API calls.

Threat intelligence is a strong element of the service, supported by a dedicated global research team and telemetry-driven insight. MDR customers receive regular reporting on emerging threats, including the newer MDR Threat Report summarizing activity observed across deployments. The service includes automated and manual threat hunting, with enrichment from real-time intelligence feeds and support for common exchange standards such as STIX and TAXII.

ESET concentrates innovation in ESET PROTECT MDR on usability and automation. The ESET AI Advisor provides incident summaries and investigation support, while proprietary ransomware rollback and secure backup technology strengthens recovery capabilities. Vulnerability assessment and conditional patching help reduce exposure windows. ESET uses GenAI for generating compliance reports and recommendations for improving cyber resilience. ESET has announced new features to be introduced in 2026 designed to expand visibility in the ESET PROTECT Platform to investigate risks tied to AI usage and Agentic AI adoption, including protection against malicious links, scripts and content generated by LLMs. Roadmap priorities include expanded integrations, response actions extending into third-party systems, and future ITDR functionality.

ESET has obtained ISO 27001, SOC 2 Type II, and OPSWAT Platinum. It provides compliance reporting aligned with NIS2, DORA, and GDPR. The platform maps detections to the ATT&CK framework and supports data residency requirements for sovereignty-focused customers in the EU, the US, and Japan.

Customer support includes 24/7 SOC delivery with multilingual documentation and support services across a wide range of European and Asian languages. Customers benefit from dedicated analysts, risk advisory services, and customer success management. Customers can operate the service in a co-managed model, request cyber insurance coverage, and generate insurer-ready reports after incidents.

ESET PROTECT MDR is well-suited to small and mid-sized organizations seeking outsourced detection and response with fast containment and strong threat intelligence. It also fits MSPs and MSSPs through its partner-focused licensing model. The service is used across regulated sectors such as finance, government, retail, healthcare, and utilities,

especially where clear reporting, local language support, and ransomware protection are key priorities.

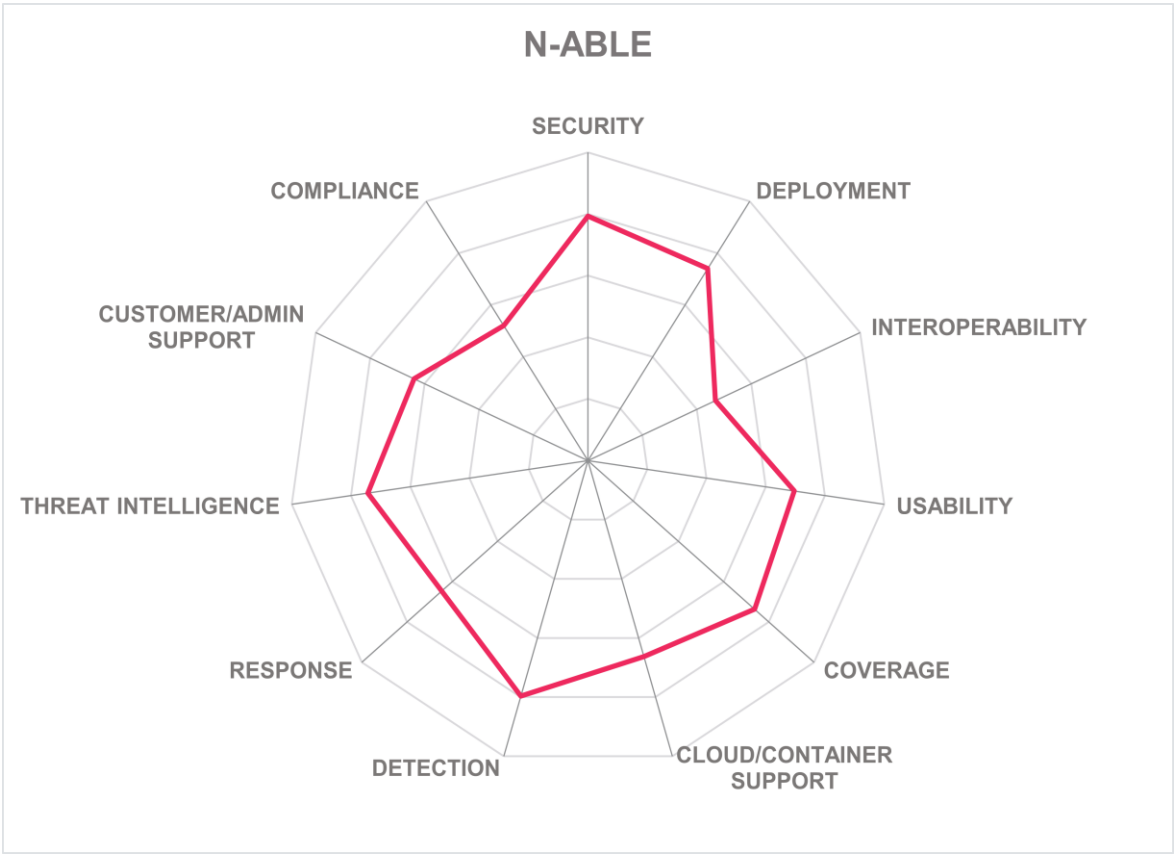
Strengths

- Integrated MDR within ESET PROTECT Console
- Fast automated response and containment
- AI-assisted investigation through ESET AI Advisor
- Mature threat intelligence and research capability
- Good customer visibility into incident timelines
- Built-in SOAR and automated remediation actions
- Vulnerability and patch management included
- Can discover and monitor shadow IT
- Multilingual support across many regions
- Ransomware prevention and rollback technology

Challenges

- Limited third-party EPDR, NDR, DLP, and SASE integrations
- No integrations with identity security solutions
- Does not include CSPM, but this is on the roadmap
- SaaS application monitoring limited to M365 and Google Workspace
- No broad support for industrial protocol analysis
- Container and serverless telemetry support limited
- Does not support the OCSF directly

N-able – Adlumin MDR



N-able is a publicly listed cybersecurity company founded in 2000 and headquartered in Burlington, Massachusetts, in the US. Its MDR offering, Adlumin MDR, joined the N-able portfolio through the acquisition of Adlumin in November 2024. Customers range from small businesses to enterprises, with most in NA, followed by EMEA and APAC. Pricing is based on the number of devices, with an optional IR retainer. N-able delivers Adlumin MDR as a cloud service and they claim it typically deploys within 90 minutes.

Adlumin MDR is a multitenant security operations service that combines SIEM, XDR, and MDR capabilities on a single platform. It ingests telemetry from endpoints, networks, cloud services, identity systems, and applications through APIs and agents. The service applies ML-based UEBA to identify threats across large volumes of events and provides automated response actions through integrated SOAR playbooks. Customers gain visibility into detections, investigations, and remediation steps. The service includes 24/7 monitoring, threat hunting, incident reporting, and compliance insights that help reduce exposure from stale accounts, misconfigurations, and risky access.

Adlumin MDR supports direct engagement with N-able SOC analysts who investigate incidents and communicate response actions with customers rather than providing alerts alone, combined with partner-focused multitenancy designed for MSP and MSSP operations. Its vendor-agnostic architecture supports a diverse range of customer technology stacks and enables consistent security operations without forcing standardization. Automated compliance insights and posture scoring add operational value beyond alert handling. Product improvements could include broader cloud service coverage and stronger support for Kubernetes monitoring. More integrations for identity security platforms and advanced response automation through privileged access workflows would also strengthen the offering.

Adlumin MDR covers endpoints, servers, identity systems, Edge environments, IoT environments, and remote workers, but not mobile devices. It supports Windows, Linux, and macOS, plus selected ICS environments, but not Android, iOS, or Chrome OS. Browser coverage excludes Apple Safari. ITDR is included, and the platform can analyze encrypted IP based protocols. It cannot discover or monitor shadow IT. The solution includes broad EPDR and XDR integrations, including ESET PROTECT, and limited NDR connectors for Darktrace DETECT and RESPOND, Palo Alto Networks Cortex XSIAM and XDR, and Cisco Secure Network Analytics. SIEM and SOAR are native, with no third-party SIEM or SOAR connectors. There are no dedicated connectors for DLP, SASE, identity security, vulnerability, or ASM platforms, although data ingestion via syslog is supported. N-able does not support the OCSF.

The service covers cloud services and SaaS applications, including detection of suspicious logins, unusual administrative activity, abnormal resource sharing, and exfiltration attempts. It includes CWP but not CSPM or multi-cloud vulnerability scanning. The platform analyzes telemetry from Amazon EKS, AWS Lambda, Azure Functions, Oracle Cloud, and GCP services, and correlates events from cloud DNS, gateways, and API gateways to detect malware command-and-control activity. The solution does not monitor and secure Kubernetes environments. The platform offers strong Microsoft 365 integrations OOTB and limited monitoring for Google Drive and Salesforce, but not Zoom, Box, GitHub, Jira, or Workday. CSPM integrations are limited to Prisma Cloud and Microsoft Defender for Cloud, with additional integrations supported through standard log ingestion.

Detection capabilities include identity-based threat coverage for account compromise, credential misuse, MFA bypass, token theft, and lateral movement. These detections are supported through integrations with identity platforms such as Microsoft Entra ID and Active Directory, with identity telemetry correlated with endpoint and network data to identify anomalous access patterns and suspicious authentication activity. The platform can also detect and report identity credential abuse and privilege escalation. The solution can detect and report risks associated with PUPs on monitored endpoints. Network detections include east-west traffic monitoring for insider threat and advanced persistent threat activity, and the investigation of unknown signals, but not on-demand full packet capture and inspection. The provider can fully manage UEBA, customers can manage it themselves, or both parties can operate it in a co-managed model. The solution can detect and report privilege escalation, abnormal access to sensitive data, unusual file uploads or downloads, and integrates out of

the box with third-party IDS and IPS. N-able reports an average detection time of one minute across the customer IT estate.

Responses include automated containment actions such as DNS redirects, rollback of configuration changes, prevention of unauthorized configuration changes, host isolation, and policy-approved automated containment. The service can block ransomware before encryption, detect and respond to phishing in real time, and address privilege escalation, insider threats, cloud misconfigurations, and living-off-the-land techniques. The built-in SOAR engine delivers response playbooks. Patch management and vulnerability services are available as an additional managed offering. The platform does not support automated JIT privilege revocation through PAM or IdP integration and cannot automatically deprovision users or disable risky sessions via SCIM, SAML, or API calls. The service does not provide on-site incident assistance, but post-remediation validation and remote forensic support are included.

The MDR platform delivers threat intelligence as part of the service and supports proactive and manual threat hunting by a dedicated team. The service uses real-world attack data, internal incident data, telemetry from network, endpoint, and cloud environments, open-source data, and research sources to train and refine its ML-based detection analytics and provides reporting on emerging threats and security posture. Threat intelligence draws from customer deployments rather than technology partners. The platform supports several threat intelligence exchange standards but not OpenIOC or MISP.

Innovation centers on ML–driven behavioral analytics for detection, complemented by GenAI and LLM capabilities that enhance analyst usability and investigation workflows. The platform also applies ML to detect insider threats and anomalous access patterns and combines UBA with graph-based modeling of entities to identify suspicious relationships, multi-host logon chains, and unusual access paths. LLMs assist analysts with queries, code and configuration creation, and investigation summaries, but do not generate policies, compliance reports, simulations, or dynamically optimize response playbooks. A notable capability is the Lateral Movement Detection Framework, which applies ML baselines, process execution models, event correlation, and graph-based UEBA to detect attacker movement after compromise. Deception features include decoy hosts and systems, with optional BAS simulation and ransomware simulation tools, although activity recording and playback for forensic analysis is not supported.

N-able is ISO 27001 and SOC 2 Type II certified. The platform updates detections based on ATT&CK knowledge but does not generate ATT&CK mapped reports. It does not provide regulatory reporting for NIS2, DORA, or GDPR. Data residency is guaranteed for the EU, US, Canada, and Australia, and the service can operate within customer-controlled environments to meet sovereignty requirements.

N-able delivers customer support remotely. The solution can be used to outsource the SOC function, but co-management options are available. Communication channels include phone, email, dedicated IR collaboration calls, and service desk integrations. Support and documentation are available only in English. Each customer has a dedicated Customer Experience Manager. The platform provides insurer-ready incident reports and remote

forensic evidence gathering, but no ROI calculator or dedicated risk advisor services. Cyber insurance is not included, but a cyber warranty is available depending on the MDR package.

Adlumin MDR is well-suited for MSPs, MSSPs, and organizations from around 50 employees upwards, including enterprises. It supports a wide range of sectors, particularly regulated environments such as healthcare, manufacturing, and finance. The service appeals to customers seeking a transparent MDR platform with strong automation, rapid onboarding, and vendor-agnostic integration across diverse security stacks.

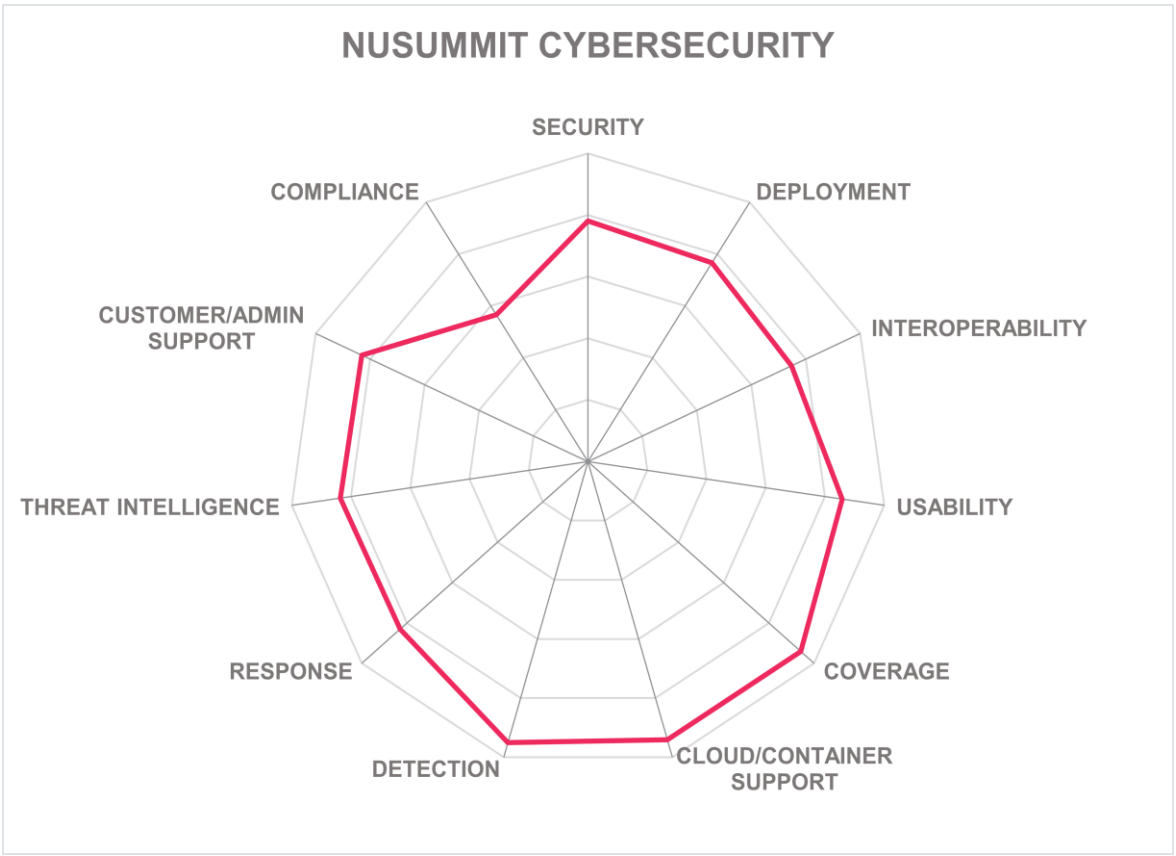
Strengths

- GenAI-powered query and reporting
- Vendor-agnostic integrations across diverse security stacks
- Built-in SIEM and SOAR capabilities
- Strong AI supported UEBA and lateral movement detection
- Includes Lateral Movement Detection Framework
- Ransomware prevention with pre-encryption blocking
- Analyzes telemetry from Amazon EKS, AWS Lambda, Azure Functions, Oracle Coud, and GCP services
- Includes deception functions
- Dedicated customer support engineer per customer

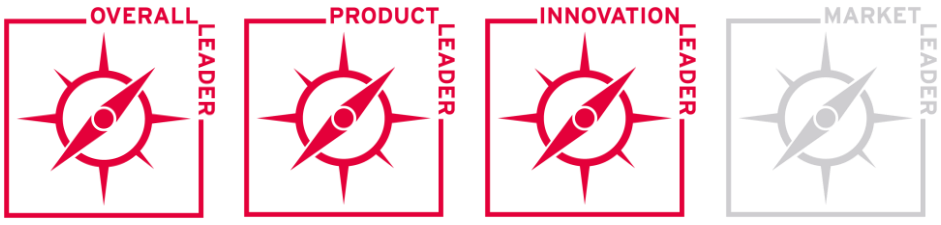
Challenges

- No support for Android or iOS monitoring
- Limited Kubernetes monitoring and container security depth
- No specific third-party SIEM or SOAR connectors
- No connectors for third-party DLP, SASE, or ASM solutions
- Limited cloud service coverage beyond core applications
- Identity layer responses are limited
- BAS and ransomware simulation is extra
- Does not support the OCSF

NuSummit Cybersecurity – CogniX MDR



Leadership



NuSummit Cybersecurity, a NuSummit group company, is a privately owned cybersecurity services provider founded in 2008 as Aujas Cybersecurity and now backed by Investcorp following a rebrand in 2025. The company is headquartered in Mumbai, India, with North American headquarters in Plano, Texas, in the US. NuSummit Cybersecurity delivers CogniX MDR through Cyber Defense Centers (CDCs) in India, with additional expansion planned in the US and the Middle East. NuSummit Cybersecurity prices the service mainly

on a consumption basis, with optional alert-based and per-node models depending on customer requirements.

CogniX MDR integrates security telemetry from across customer environments into a unified platform view. The service includes SIEM, EDR, XDR, threat hunting, and IR services. NuSummit Cybersecurity supports both managed and co-managed service models, with governance structures and SLAs aligned to customer priorities. The solution is suitable for IT, OT, and cloud monitoring.

NuSummit Cybersecurity has a deep engineering capability and has developed more than 120 threat hunting models, 400 custom parsers for integrating unsupported log sources, and 100 automation playbooks, which can be customized. NuSummit Cybersecurity could improve the user interface and navigation to make it easier for less experienced users, and its European market presence remains limited compared with other regions.

The service provides 24/7 monitoring and response across endpoints, servers, identity systems, mobile devices, Edge environments, remote workers, and IoT deployments, and can resolve every alert if required. It has ITDR capabilities, can discover and monitor Shadow IT, ingests logs from all major operating systems including macOS, Linux, Chrome OS, iOS, and Android, and covers most common browsers except Opera. The platform analyzes all major protocols such as DNS, HTTPS, SSH, and RDP, as well as IoT and OT/ICS protocols.

It integrates with a wide range of EPDR and XDR platforms, including Trellix Endpoint Security Complete; NDR solutions such as Fortinet FortiNDR; SOAR platforms including Palo Alto Networks Cortex XSOAR; SIEM platforms including Microsoft Sentinel and IBM QRadar; DLP and DSP tools including Zscaler Data Protection; identity platforms including Microsoft Entra ID; SASE solutions including Netskope Intelligent SSE; and exposure management platforms including Tenable One Cloud Security. The platform supports the OCSF.

CogniX MDR delivers continuous monitoring, detection, and response across cloud services, SaaS applications, and container environments. The solution includes CSPM, CWP, vulnerability scanning, and CTEM for multi-cloud deployments. It monitors suspicious logins, unusual administrative activity, resource sharing, and configuration changes, and correlates events from cloud DNS, gateways, and API traffic to identify exfiltration and command-and-control activity. The platform analyzes telemetry from Amazon EKS, AWS Lambda, Azure Functions, and GCP services, and monitors and secures Kubernetes environments. The platform integrates with a wide range of cloud services and CSPM platforms including Wiz CNAPP and supports monitoring of services such as Google Drive.

CogniX MDR can identify account compromise, credential misuse, token theft, and lateral movement across the environment. The service detects MFA attempts, privilege escalation, abnormal access to sensitive data, unusual file uploads or downloads, and risks related to PUPs. Network-based detections include east-west traffic inspection for insider threat and advanced persistent threat activity, on-demand full packet capture capabilities, and investigation of unknown or anomalous signals.

CogniX MDR correlates identity, device, and network telemetry to surface anomalous access patterns and provides managed UBA and attacker behavior analytics, with integration support for third-party IDS and IPS.

CogniX MDR offers automated response actions such as DNS redirects, configuration rollback, prevention of unauthorized configuration changes, session termination, and JIT privilege revocation through PAM and IdP integrations. The service supports policy-approved automated containment and can automatically deprovision users or disable risky sessions via SCIM, SAML, or API-based controls.

It can isolate affected hosts, block malicious indicators, and stop ransomware activity once encryption begins. CogniX MDR includes its own SOAR functionality with automated and semi-automated playbooks but does not provide software patching. The service provides post-remediation validation, SLA-backed response times, and optional on-site support.

Threat intelligence capabilities include automated and manual threat hunting, regular reporting on emerging threats, and enrichment from multiple external intelligence feeds. CogniX MDR provides CTEM services, with external ASM available as an optional add-on to extend external exposure visibility. The vendor draws intelligence from customer deployments, technology partners, and open-source data, while supporting standard threat intelligence exchange formats.

The CogniX MDR platform uses AI agents for Level 1 alert investigation and prioritization. The platform provides automated verdicts, contextual severity scoring, analyst chat-based interaction, and dynamic playbook optimization. NuSummit Cybersecurity also operates an automated threat hunting platform for proactive detection services. The solution allows activity recording and playback for forensic analysis and offers optional BAS and ransomware simulation tools.

NuSummit Cybersecurity is certified for ISO 27001 and holds SOC 2 Type II attestation. The CogniX MDR service aligns detections and reporting with the ATT&CK framework and generates compliance-relevant outputs for NIS2, DORA, and GDPR. NuSummit Cybersecurity offers guaranteed data and metadata residency for the EU, NA, and the Middle East.

NuSummit Cybersecurity provides support services and documentation in English and Arabic. NuSummit Cybersecurity provides role-based dashboards, ATT&CK heat maps, and regular governance meetings, with a named SOC lead assigned to each customer. A dedicated risk advisor and customer success manager are available as optional services. NuSummit Cybersecurity offers pre-sales trials and can deliver forensic support remotely or on site. Cyber insurance is not included, and the platform does not generate insurer-ready post-incident reports.

CogniX MDR is best suited to organizations seeking a strong services-based MDR partner with strong engineering depth and customization. The solution supports enterprises and large mid-market organizations, while also serving smaller customers through specific regional programs. NuSummit Cybersecurity has its strongest presence in NA, the Middle East, and India, with limited activity in Europe. It is of particular interest to customers in

finance, manufacturing, insurance, and healthcare that require tailored integrations and AI-supported SOC workflows.

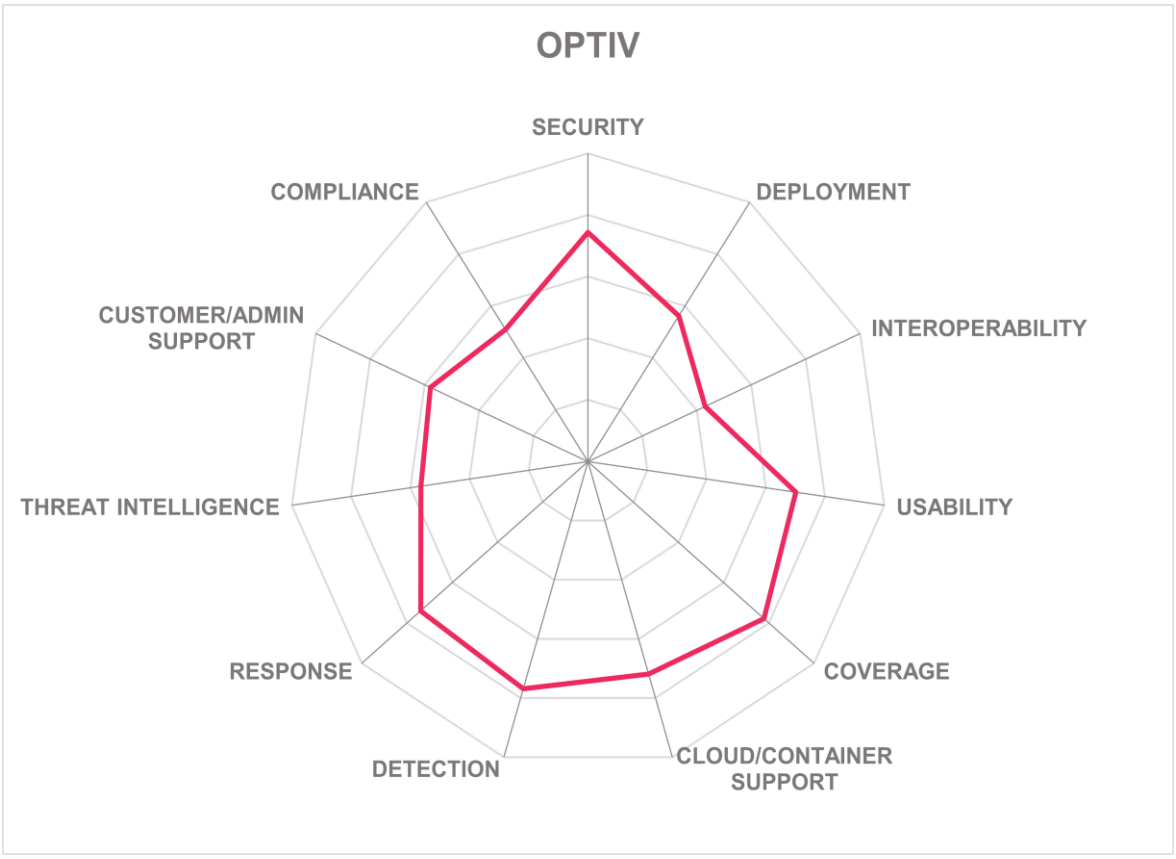
Strengths

- Services-driven MDR delivery with global CDC coverage
- Extensive custom parser development for unsupported log sources
- Large library of use cases and automation playbooks
- Agentic AI platform for faster alert triage and investigation
- Broad integration support across SIEM, SOAR, and identity tools
- Coverage across IT, OT, IoT, ICS, and cloud environments
- ATT&CK-aligned detections and reporting heat maps
- Transparent KPI dashboards tailored for multiple stakeholder roles
- Certified for ISO 27001 and holds SOC 2 Type II attestation

Challenges

- User interface could be challenging for new users
- Limited customer presence and focus in Europe
- No built-in software patching capability for remediation
- Dedicated risk advisor not included in standard service
- Support and documentation available only in English and Arabic

Optiv – Optiv MDR



Optiv is a private cybersecurity company founded in 2015 and headquartered in Denver, Colorado, in the US. Optiv has offices across the US and in Mississauga, Canada, with SOCs in Leawood, Kansas in the US and Bangalore in India. Optiv mainly targets mid-market organizations with its MDR service, followed by larger enterprises, with most customers in NA. Optiv bases core service licensing on the volume of data ingested per day. Optiv MDR is SaaS delivered. The service runs in the public cloud, with optional on-premises elements for log collection and integration, depending on customer requirements.

Optiv MDR combines Google SecOps with Optiv's own content, automation, and data engineering workflows. The platform ingests telemetry from endpoints, networks, identity systems, and cloud services through APIs and log collection. It provides round-the-clock monitoring, detection, and response with human oversight supported by Agentic AI

personas. The service includes Active Defense hours to bridge the gap between incident confirmation and full IR engagement.

Optiv's primary strength lies in its data engineering architecture, which uses dedicated ingestion pipelines to collect large volumes of heterogeneous security telemetry. This approach allows the platform to operationalize telemetry from diverse security tools and environments, improving detection quality and investigation speed. Optiv's specialized AI agents operate in defined roles such as threat hunter, detection engineer, and tiered analyst, each processing specific elements of an alert in parallel or sequence to preserve context and improve accuracy rather than relying on a single generalized model.

Optiv Essential Content provides a mapped detection library aligned to the ATT&CK framework. The user interface provides shared visibility through dashboards, case timelines, investigation views, and reporting that mirror the SOC experience. Areas for improvement include broader protocol coverage for IoT and industrial environments, addressing the absence of activity recording and playback, and adding stronger support for data sovereignty requirements outside the US.

Optiv MDR provides monitoring across endpoints, servers, identity systems, Edge environments, IoT devices, mobile devices, and remote workers. It supports all major operating systems and common browsers, and it includes ITDR capabilities for monitoring identity misuse and privilege abuse. The platform can resolve every alert when required by the customer through automated SOAR workflows. It can discover and continuously monitor shadow IT. It analyzes DNS, HTTPS, SSH, and RDP traffic, including encrypted sessions, but does not support industrial or SCADA protocols.

Integrations include selected EPDR solutions such as the CrowdStrike Falcon Platform, selected XDR platforms such as Palo Alto Networks Cortex XDR, SOAR platforms such as Google SecOps SOAR, a wide range of SIEM platforms including Microsoft Sentinel, limited DLP and DSP tools, selected identity platforms such as Microsoft Entra ID and Okta Workforce Identity, limited SASE support with Prisma SASE as the only native integration, and selected vulnerability and exposure platforms such as Tenable One Cloud Security. The platform supports the OCSF.

The service provides 24/7 monitoring across cloud services and SaaS applications and supports Kubernetes monitoring. It can detect suspicious logins, unusual administrative activity, and resource changes across major cloud services. However, it does not include native CWP, CSPM, or multi-cloud vulnerability scanning within the core MDR service, and it does not analyze serverless or container workload telemetry such as AWS Lambda or Azure Functions. Integrations include Microsoft 365, Box, GitHub, Jira, Google Workspace, and several CSPM platforms including Prisma Cloud, Microsoft Defender for Cloud, and Wiz.

Optiv MDR detects account compromise, credential misuse, token theft, privilege escalation, and anomalous access through correlated identity, endpoint, and network telemetry. According to Optiv, the average time taken to detect threats anywhere in the customer IT estate is one minute. Its analytics correlate identity, device, and network telemetry to identify anomalous access patterns across distributed environments. It can identify MFA bypass

attempts, abnormal access to sensitive data, unusual file uploads or downloads, and PUPs. Network detections support remediation actions and enrichment through threat intelligence, but exclude east-west traffic capture, on-demand full packet inspection, and investigation of unknown signals. The solution cannot perform baseline and periodic scans of endpoints for FIM and alerting. UBA is fully managed by Optiv and cannot be self- or co-managed by customers. Optiv MDR integrates with third-party IDS and IPS.

Optiv MDR provides automated response actions such as session termination, process disruption, and rollback of configuration changes. It supports policy-approved automated containment and can enforce JIT privilege revocation and session termination through identity and PAM integrations. It can also automatically deprovision users or disable risky sessions via SCIM, SAML, or API calls, depending on the available response actions of the IAM technology in use. The service does not include software patching. Ransomware can be blocked before encryption. Google SecOps orchestration and Optiv playbooks support response workflows. The solution can detect and respond to phishing attacks in real time. Optiv provides SLAs for time to respond, as well as update frequency and incident resolution.

Optiv MDR includes a dedicated threat hunting team that delivers automated and hypothesis-driven hunts, supported by real-time intelligence enrichment. Google Threat Intelligence is included as part of the base service. Threat intelligence draws on external feeds, open-source sources, and partner telemetry. Support for exchange standards is limited to MISP. The solution does not include CTEM. Customers receive reports on security posture, emerging threats, and hunting outcomes.

Optiv MDR‘s Agentic AI triage breaks investigations into specialized autonomous workflows with human oversight. These multi-step workflows use defined AI personas to automate alert ingestion, enrichment, correlation, triage, and early analysis while preserving context for human analysts. LLMs facilitate alert summarization, query creation, code and configuration development, and dynamic playbook optimization. The platform applies ML to detect abnormal activities, insider threats, and other cyber threats, and to improve usability. The platform includes UBA, but not attacker behavior analytics. Optiv continues to improve automation for detection engineering. Customers benefit from direct access to multiple layers of telemetry and investigation context. The platform offers BAS support as an optional extra. The service does not include deception capabilities or forensic playback features.

Optiv MDR aligns detections and reporting with the ATT&CK framework and generates ATT&CK-mapped incident reports. The service has SOC 2 Type I and Type II attestation. It does not provide regulatory reporting for NIS2, DORA, or GDPR. The platform guarantees data residency only for the US, and the platform cannot operate fully within customer-controlled environments for sovereignty needs.

Optiv MDR provides SOC coverage with co-management options, supported by a dedicated customer success manager. Optiv provides support and documentation only in English. Optiv provides on-site support only in NA. Optiv offers an ROI calculator and pre-sales trial access for qualified prospects. Optiv offers dedicated risk advisory services only as an add-on. The service does not provide insurer-ready reporting or forensic evidence gathering.

Optiv MDR is suitable for organizations from around 50 employees upward, including large enterprises, seeking a transparent MDR service with deep integration into existing security investments. It is of particular interest to North American organizations in regulated sectors that require tailored detection engineering, identity-focused threat coverage, and strong operational support.

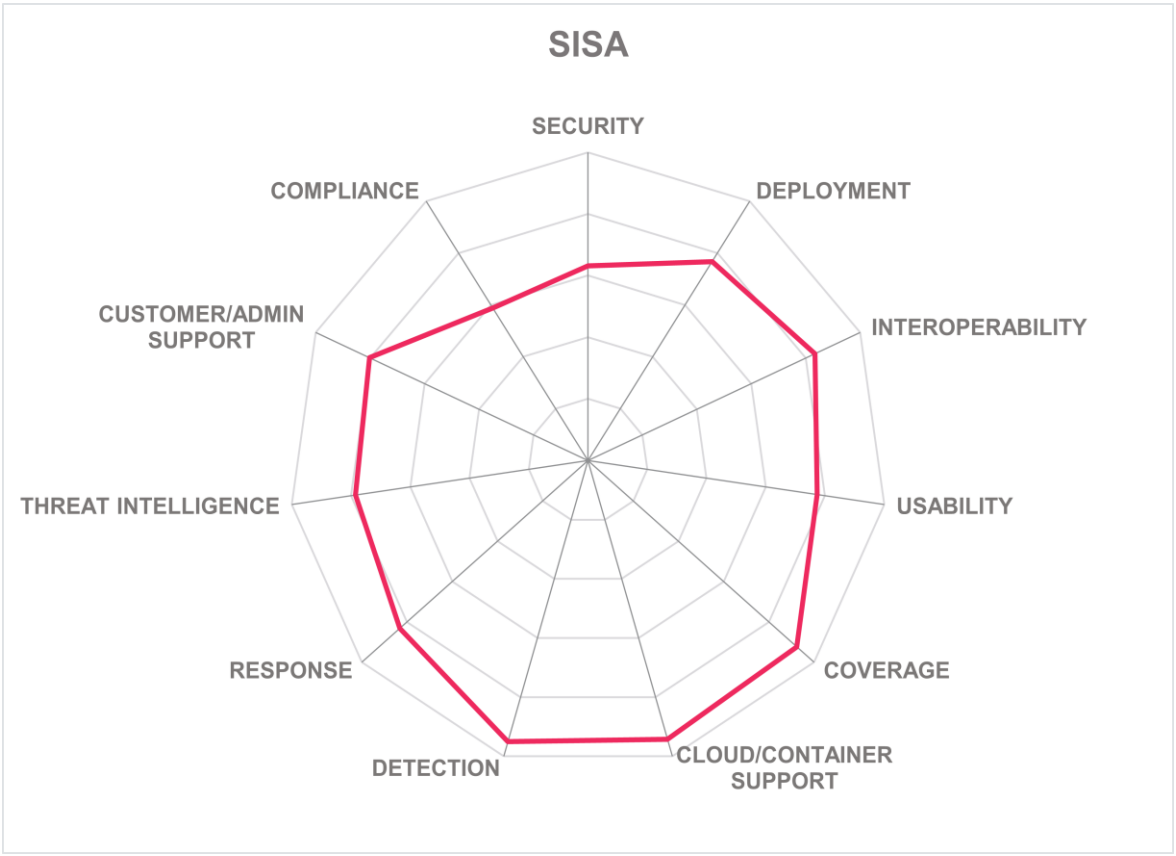
Strengths

- Advanced data engineering for telemetry normalization and enrichment
- Multi-persona Agentic AI triage with human-in-the-loop oversight
- Full client transparency into underlying MDR platform
- Deep integration with Google SecOps capabilities
- Broad monitoring across endpoints, identity, and cloud services
- Automated containment and response actions through SOAR playbooks
- Dedicated threat hunting and intelligence reporting included
- Can detect and respond to phishing attacks in real time
- Service has SOC 2 Type I and Type II attestation

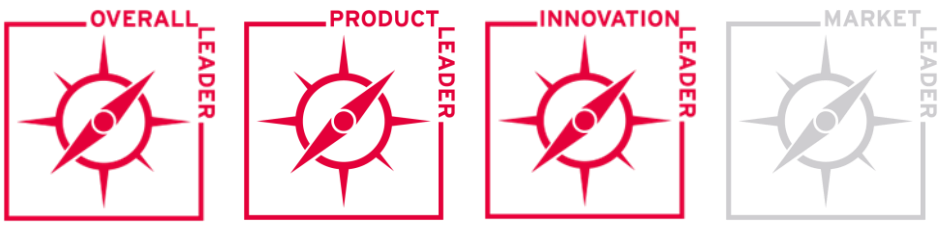
Challenges

- Cannot analyze OT/ICS protocols
- No native CSPM, CWP, or vulnerability scanning capabilities
- Data residency guaranteed only for the US
- No functionality for software patching
- Lacks CTEM
- No baseline and periodic scans of endpoints for FIM and alerting
- No forensic activity recording and playback capabilities
- Does not support regulatory reporting for NIS2, DORA, or GDPR
- Support and documentation available only in English

SISA – SISA ProACT Agentic SOC



Leadership



SISA is a private cybersecurity company founded in 2006 and headquartered in Bangalore, India. The company is forensics-driven and caters strongly to regulated sectors, with a long track record in the payment ecosystem. Most customers are in APAC, followed by EMEA and NA, with the majority of those in the US. SISA offers ProACT Agentic SOC as an MDR service that can be deployed as a cloud-based service, as a cloud-based service with on-

premises elements, or as a fully on-premises deployment. SISA prices the platform by asset covered when customers host it and by data volume per terabyte when SISA hosts it.

SISA ProACT Agentic SOC combines an extended threat detection platform with SIEM, FIM, UEBA, threat hunting, BAS, threat exposure management, IR tooling, SOAR, and a forensics investigation platform. SISA delivers the service as a single all-inclusive offering rather than multiple MDR tiers. Customers can adopt SISA SIEM and UEBA as part of the stack or integrate existing SIEM tooling and forward alerts into SISA for investigation, automation, and response. SISA provides deep and dark web monitoring, brand monitoring, and ASM through partners. SISA supports phased adoption to avoid forcing a rip-and-replace project.

SISA's forensics-led operating model is a key feature, which turns investigation learnings into new detection use cases and threat hunting hypotheses. The portal design also stands out, with an alerts view, a customizable executive dashboard, detailed incident views with chronology and recommendations, an IR workspace, and a governance portal that produces automated weekly, monthly, quarterly, and board-level reports. LLM-enhanced investigations generate draft incident and threat hunting reports that the SOC reviews internally before delivering them to customers, which keeps a human in the loop while reducing analyst workload. Potential product improvement areas include adding automated software patching capabilities and adding GenAI support for creating queries, code, and configurations where appropriate.

Coverage is broad across endpoints, servers, email, identity systems, Edge computing, IoT, mobile devices, and remote and contract workers, with ITDR included. The solution supports major operating systems and common browsers, and it analyzes encrypted and unencrypted IP protocols including DNS, HTTPS, RDP, SSH, IPsec, and VoIP, as well as IoT, ICS, and SCADA protocols such as Modbus, MQTT, and DNP3. The SOAR layer can resolve alerts automatically where integrated security tools expose the necessary APIs and response actions, and playbooks can be customized. Integrations span third-party EPDR solutions such as Microsoft Defender for Endpoint and SentinelOne Singularity Platform, NDR such as Fortinet FortiNDR, SIEM such as Microsoft Sentinel, DLP and DSP such as Microsoft Purview DLP, identity security platforms such as Microsoft Entra ID, SASE platforms such as Netskope Intelligent SSE, and vulnerability and exposure platforms such as Tenable One Cloud Security. The solution supports the OCSF and includes discovery and monitoring of shadow IT.

SISA ProACT Agentic SOC provides 24/7 monitoring and response across cloud services and SaaS applications, with connectors to cloud services and OOTB integration for Microsoft 365 including Teams. It monitors services such as Microsoft Defender for Cloud Apps, Google Workplace, and Google Drive, and integrates with third-party CSPM platforms such as Microsoft Defender for Cloud, Wiz CNAPP and CSPM, and Palo Alto Networks Prisma Cloud. The service supports Kubernetes and analyzes telemetry from container and serverless services such as Amazon EKS, AWS Lambda, Azure Functions, and GCP services, and it correlates events from cloud DNS, gateways, and API gateways. The service includes CSPM and CWP but does not include vulnerability scanning for customer multi-cloud environments.

Detection spans identity, endpoint, network, and cloud telemetry correlation, including detections for account compromise, credential misuse, lateral movement, MFA bypass, and token theft. Analytics correlate identity, device, and network activity to identify anomalous access patterns and insider threats. Network detections include east-west traffic capture for insider threat and advanced threat detection, on-demand full packet capture and inspection, and investigation of unknown or suspicious signals. FIM supports baseline and periodic scans with alerting for unauthorized file changes. UEBA can be fully managed by SISA or co-managed with customers. SISA states an average time to detect of three minutes. The platform integrates with IDS and IPS and detects privilege escalation, abnormal access to sensitive data, unusual file transfers, and PUPs.

Response includes automated actions such as session termination, JIT privilege revocation through PAM or IdP integration, SCIM and SAML-based user deprovisioning, DNS redirects, rollback of configuration changes, and on-demand packet capture initiation. Risky sessions can be disabled through API-driven controls. Containment can be fully automated if enabled by policy, with approval workflows governing sensitive actions. The service can block ransomware before encryption, respond to phishing in real time, and address privilege escalation, and cloud misconfigurations. Built-in SOAR and incident response tooling support playbooks, investigation workflows, and post remediation validation to confirm threats have been neutralized. Software patching is not included.

Threat intelligence capabilities include a dedicated threat hunting team, regular reporting on posture, emerging threats, and hunting outcomes, and both automated proactive and manual threat hunting. The service uses threat intelligence feeds and open-source sources to train ML models, and for enrichment and correlation. Intelligence also comes from customer deployments, technology partners, and SISA’s forensics engagements, where patterns and techniques get translated into use cases. The service supports the main cyber threat intelligence exchange standards. The service includes CTEM with prioritized remediation recommendations.

Innovation centers on the move toward an autonomous SOC operating model, with Agentic AI and GenAI supporting investigations, alert summarization, structured incident drafting, and recommendation creation, plus workflow automation such as shift handover summaries and continuous health checks across critical assets. The platform applies ML within its UEBA to baseline user and asset activity, detect anomalous access patterns, insider threats, credential misuse, and lateral movement. The platform correlates identity, endpoint, and network telemetry to strengthen behavioral risk scoring. The platform also includes activity recording and playback for forensic analysis, BAS, and ransomware attack simulation. Potential product improvement areas include adding dedicated attacker behavior analytics and adding AI support to generate and optimize response playbooks dynamically.

SISA has ISO 27001 certification and SOC 2 Type I and Type II attestation. SISA is a PCI Qualified Security Assessor. The platform aligns detections and response mapping to the ATT&CK framework, and it generates reports that map threats to tactics and techniques. It also supports regulatory compliance reporting for NIS2, DORA, and GDPR. SISA offers guaranteed data and metadata residency for the EU, the US, and the UAE, and it can operate inside customer-controlled environments to meet sovereignty requirements.

Support includes round-the-clock SOC services, a portal that supports collaboration and reporting, and governance reporting that supports continuous improvement and risk management. SISA assigns a dedicated analyst to each customer and includes a customer success manager as standard. SISA offers risk advisor services as an optional extra. On-site support is available in EMEA and APAC, with support and documentation in English only. The service includes cyber insurance options and can generate insurer-ready post-incident reports, supported by remote and on-site forensics, if necessary.

SISA ProACT Agentic SOC is of interest to regulated organizations that need data localization and audit readiness particularly in the finance and payments sectors, followed by government, retail, healthcare, oil and gas, utilities, and travel and hospitality. The deployment model suits organizations that must keep data in country or operate in customer-controlled environments, as well as those that prefer a provider-hosted SaaS model. It also suits organizations that want to keep existing SIEM investments while adding MDR automation, investigation depth, and governance reporting.

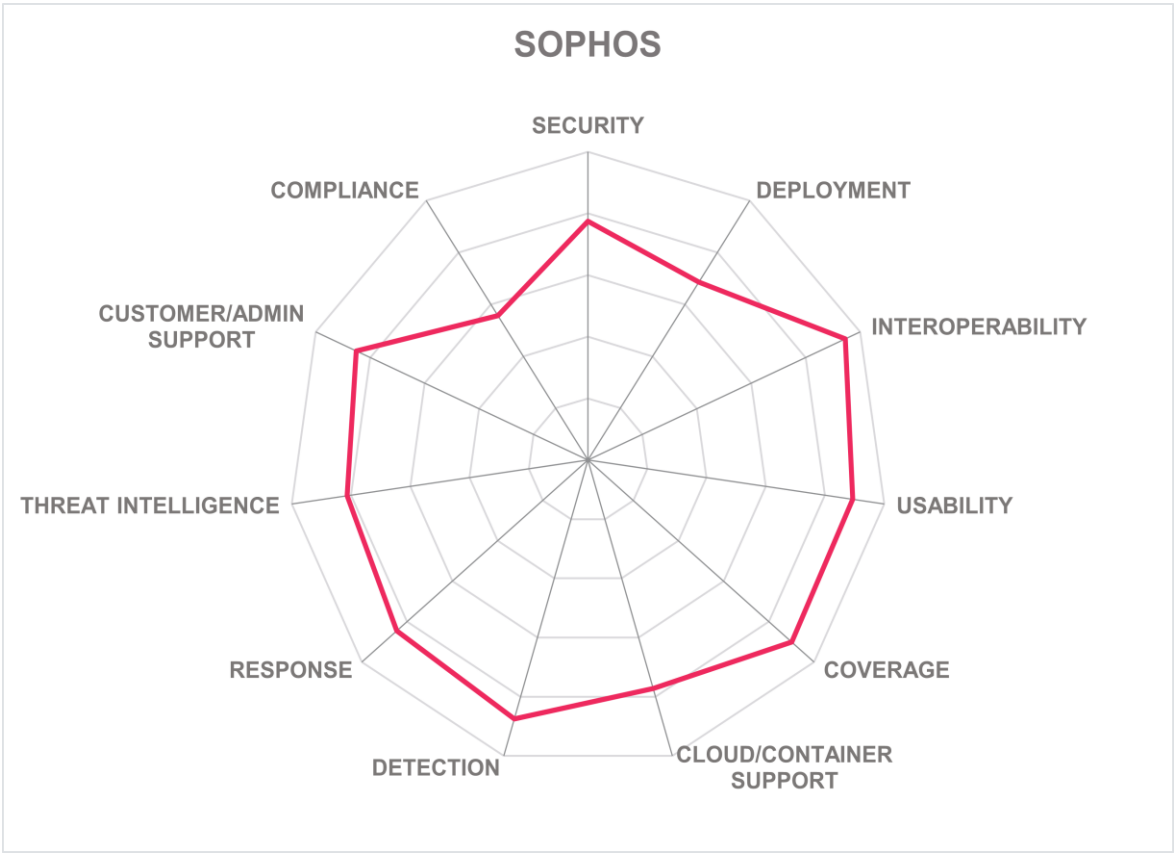
Strengths

- Agentic AI-assisted investigations
- Human-in-the-loop quality control
- Broad integration ecosystem support
- Analyzes IoT, ICS, and SCADA protocols
- FIM supports baseline and periodic scans
- Flexible deployment with data residency options
- Built-in governance and compliance reporting
- Established payment sector domain expertise
- Automated proactive and reactive threat hunting
- Service includes a dedicated analyst and customer success manager

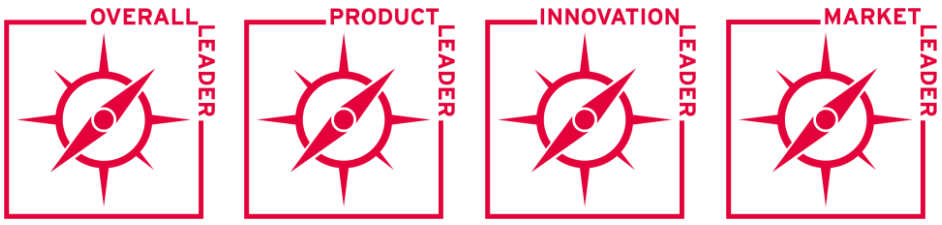
Challenges

- No built-in software patching
- Limited GenAI content generation capabilities
- English only support and documentation
- Attacker behavior analytics not supported
- ASM only available from partners
- Higher than average reported detection times

Sophos – Sophos MDR



Leadership



Sophos is a private cybersecurity company founded in 1985 and headquartered in Abingdon in the UK. Customers range from small businesses to large enterprises, with most in the medium market. They are primarily located in NA and EMEA, followed by APAC and LATAM. Sophos licenses MDR by users and servers and delivers it as a SaaS offering through the Sophos Central platform. Deployment requires an XDR agent on endpoints and servers, with optional on-premises components for log collection and NDR. Sophos sells the service directly and through MSSPs and channel partners. The Secureworks acquisition in February 2025 expanded SOC scale, SIEM depth, and identity coverage.

Sophos delivers MDR through two service tiers: Sophos MDR Essentials and Sophos MDR Complete. Both tiers provide round-the-clock monitoring, detection, threat hunting, investigation, containment, and reporting. Essentials supports environments that rely on third-party endpoint tools such as Microsoft Defender, while Complete requires the Sophos XDR agent and includes full IR coverage. The platform can ingest telemetry from Sophos products and third-party tools and normalizes and correlates that telemetry in a unified console. GenAI capabilities support alert summarization, query creation, investigation workflows, and analyst productivity. Sophos Managed Risk is an optional add-on to both service tiers that extends MDR into vulnerability and exposure management through integration with Tenable.

Sophos MDR leverages Sophos X-Ops, which combines threat intelligence, SOC operations, malware analysis, and AI research. Sophos X-Ops doubled in size with the addition of the Counter Threat Unit research team from its acquisition of Secureworks. Dashboards are highly customizable and suited to analysts and executives. The platform includes Microsoft and Google connectors as standard, enabling telemetry ingestion and response actions across a range of Microsoft and Google Services, allowing organizations to extend MDR coverage across identity, email, and cloud environments using existing security investments. Identity detections for Business Email Compromise (BEC) and account takeover add value for Microsoft customers. Areas for improvement include limited Kubernetes monitoring and no native attack path mapping. Some advisory services remain optional extras.

Sophos MDR provides continuous monitoring and response across endpoints, servers, email systems, identity platforms, Edge environments, IoT-connected assets, mobile devices, and remote users. It supports Windows, Linux, macOS, Android, iOS, and Chrome OS, as well as all common browsers. The service includes ITDR and can analyze encrypted IP-based protocols such as DNS, HTTPS, RDP, SSH, IPsec, and VoIP. It can also analyze selected IoT, ICS, and SCADA protocols. The solution can discover and monitor shadow IT.

The service can also ingest telemetry from third-party security tools, including EPDR and XDR platforms such as Microsoft Defender for Endpoint and the CrowdStrike Falcon Platform, NDR solutions such as Darktrace and ExtraHop, and SIEM platforms including Microsoft Sentinel and Splunk via API and syslog ingestion. It includes integrations with Microsoft Entra ID and Okta Workforce Identity, selected DLP tools such as Microsoft Purview, and a wide range SASE platforms, including Palo Alto Networks Prisma SASE, Fortinet FortiSASE, and Netskope Intelligent SSE. Sophos XDR and Sophos Central have SOAR features, and third-party SOAR platforms can be integrated via API. Sophos supports the OCSF.

Sophos MDR delivers monitoring and response across cloud services and SaaS applications. It includes CWP, CSPM, and vulnerability scanning capabilities. The service analyzes telemetry from containerized and serverless environments including Amazon EKS, AWS Lambda, Microsoft Azure, and GCP services. It correlates events from cloud DNS, gateways, and APIs to identify exfiltration attempts and command-and-control activity. The MDR solution cannot detect any specific threats to Kubernetes environments and cannot handle logging and monitoring across multiple Kubernetes clusters, but Sophos provides

container workload protection and Kubernetes-related security capabilities through its server and cloud-native security offerings. Sophos MDR integrates with Microsoft 365, Microsoft Defender for Cloud Apps, Google Workspace, and other SaaS platforms via API-based connectors. It also integrates with Microsoft Defender for Cloud and selected third-party CSPM tools, with telemetry consolidated into Sophos XDR for cross-domain detection and response.

Sophos MDR detects threats across endpoint, identity, network, and cloud telemetry. It identifies credential abuse, lateral movement, MFA bypass, and token theft. Network detections include east-west traffic analysis and packet capture. The platform correlates identity, device, and network data to identify anomalous access. The platform supports FIM. The service detects privilege escalation, insider activity, data access anomalies, and phishing. The platform supports integration with third-party IDS and IPS. ML models and analyst-led investigation support detection.

Sophos MDR supports automated and human-led response actions. The service isolates endpoints, blocks malicious activity, and terminates active user sessions across endpoint, network, and cloud control planes. The platform supports JIT privilege revocation and user deprovisioning through deep integrations with identity providers such as Microsoft Entra ID, Active Directory, and Okta. This enables session termination, token invalidation, account disablement, group membership changes, and automated deprovisioning via SCIM, SAML, or API calls. The platform enables fully automated containment when policy allows it. The platform can block ransomware before encryption, includes IR playbooks, and supports software patching. The platform includes its own SOAR capability, and post-remediation validation confirms threat removal.

Sophos MDR uses threat intelligence from Sophos X-Ops and global customer telemetry. Intelligence supports detection, prioritization, and threat hunting. The service includes automated and manual threat hunts. Reporting covers emerging threats and posture trends. Real-time threat intelligence feeds enrich detections. Intelligence sources include proprietary data, partners, and open-source feeds. The Sophos threat intelligence and analysis platform, Intelix, integrates with Microsoft Copilot to support analyst workflows. ASM, CTEM, and exposure prioritization are available as optional services rather than core features.

The company’s PRIME initiative introduces GenAI-driven quality assurance as part of a human-led QA process that evaluates the clarity and completeness of analyst case documentation and customer-facing reporting, as well as case recording, investigation depth, mobilization of resources, and efficiency across every analyst-handled case. Agentic AI supports triage, investigation, and threat hunting across Sophos and Microsoft telemetry. The solution includes user and attacker behavior analytics to identify anomalous activity and adversary techniques. ML and automation reduce alert noise and improve usability. Sophos has reduced the system resource footprint of its endpoint agents across customer deployments through performance optimizations. ML-driven analytics dynamically trigger and prioritize response playbooks based on threat context. The platform does not include deception or BAS tools.

Sophos has obtained ISO 27001, PCI DSS, SOC 2 Type II, and Germany's C5 certifications. The service aligns detections and reporting with the ATT&CK framework. Regulatory compliance reports are available for NIS2, DORA, and GDPR. The platform supports data residency in the EU, US, UAE, Canada, Australia, India, and Japan. However, the service cannot operate fully within customer-controlled environments for strict sovereignty requirements.

Sophos MDR provides on-site assistance available when required. Sophos provides services and documentation in multiple languages. Customers can outsource the SOC function or operate in a co-managed model. Reporting supports risk assessment and continuous improvement. Customers can access shared dashboards and collaboration tools. The service includes an ROI calculator. Sophos provides cyber insurance support through insurer-ready reports and a breach protection warranty of up to $1M. Sophos offers dedicated customer success management as a premium option.

Sophos MDR supports organizations of all sizes across many sectors. The service is well-suited to small and medium-sized organizations lacking internal security teams. It also supports larger enterprises seeking augmentation. Use cases include endpoint protection, identity-driven attacks, ransomware, phishing, and cloud security monitoring. Coverage is strong for manufacturing, government, retail, and healthcare. MSPs and MSSPs can also use the service to extend managed security offerings.

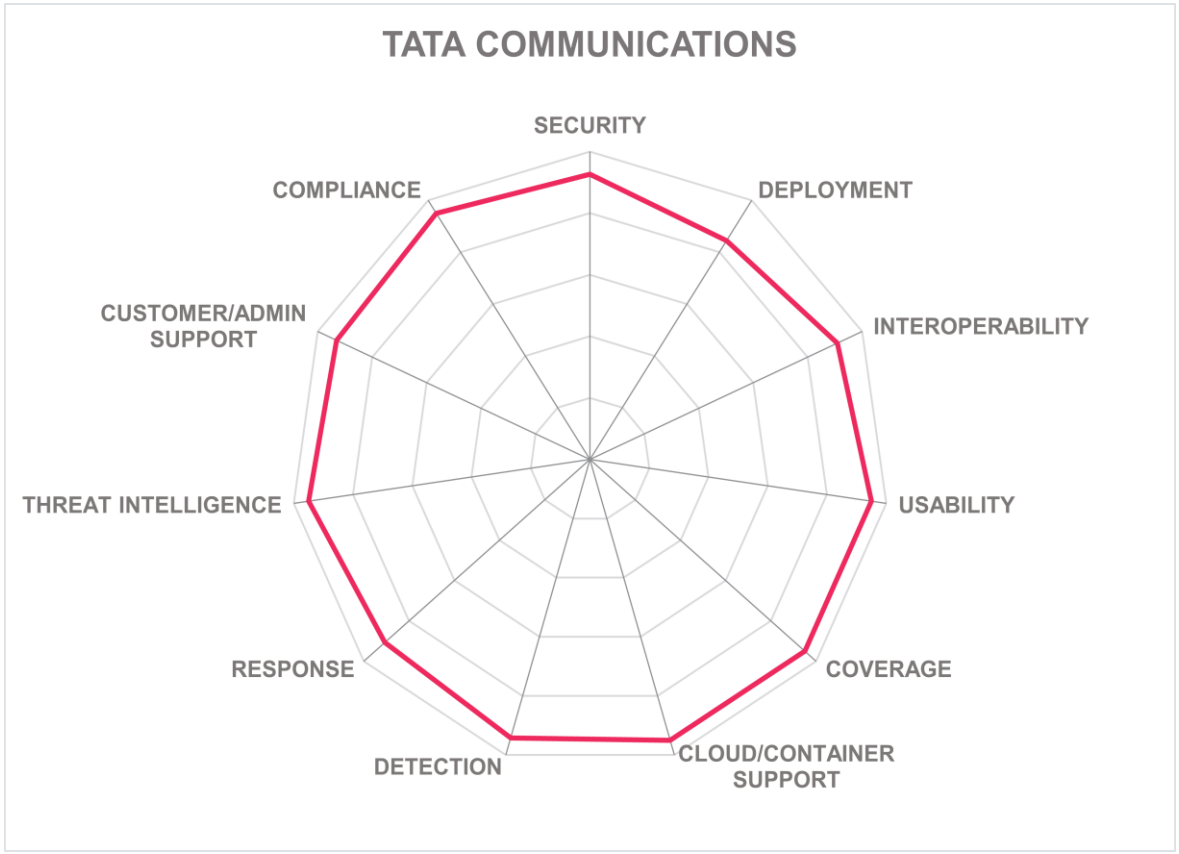
Strengths

- Large scale global MDR operations and customer base
- Strong Microsoft integration across identity and productivity services
- Two MDR tiers supporting Sophos and third-party tools
- Integrated SOAR with automated and authorized response actions
- Sophos Intelix threat intelligence and human-led threat hunting
- GenAI facilitates alert summarization, query creation, and investigation workflows
- Agentic AI supports triage, investigation, and threat hunting
- Compliance reports for NIS2, DORA, and GDPR
- Breach protection warranty with insurer-ready reporting
- Broad coverage across endpoint, network, cloud, and identity
- Supports data residency in the EU, US, UAE, Canada, Australia, India, and Japan

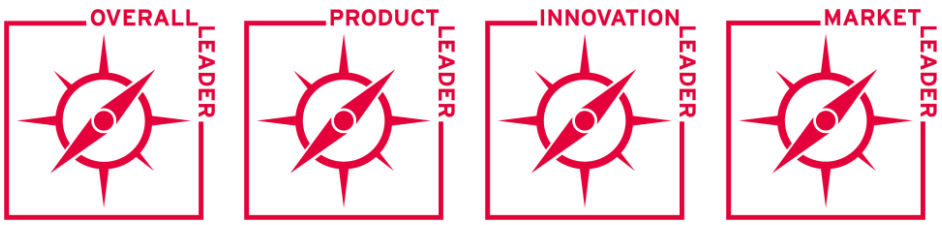
Challenges

- Limited Kubernetes-specific capabilities
- ASM and CTEM capabilities offered only as add-ons
- No native attack path mapping functionality
- Cannot operate fully within customer-controlled environments for strict sovereignty requirements

Tata Communications – Tata Communications MDR



Leadership



Tata Communications is a global public communications and digital services provider founded in 2002 and headquartered in Mumbai, India. The company operates in more than 190 countries and offers network services, cloud services, and cybersecurity covering IT, IoT, and OT environments, including Tata Communications MDR. Customers range from medium sized organizations to large enterprises, with most customers in the enterprise segment. The customer base is strongest in APAC, followed by EMEA and the US. The solution is SaaS delivered with cloud-based analytics and an on-premises data collection component. Licensing options are tiered Standard and Enterprise models with pricing based

on data ingestion, devices, or environments. Tata Communications supports SOC operations through global locations, with satellite SOCs across multiple geographies.

Tata Communications MDR combines SIEM, native SOAR, EDR, NDR, UEBA, threat hunting, and cyber threat intelligence into a single managed service. The Enterprise tier includes capabilities such as ASM, IR retainer services, and advanced threat hunting. Core capabilities include 24/7 monitoring, investigation, containment, remediation, and reporting. The service supports fully managed and co-managed operating models. Recent additions include dynamic response workflows, expanded OT SOC capabilities, and response integration with the Edge Distribution Platform, which is designed to bring detection and response closer to the network edge, using the company's global infrastructure.

A key strength of the solution is the carrier scale visibility of Tata Communications, derived from handling a significant portion of global internet traffic, which feeds early Indicators of Compromise (IoCs) into detection workflows. The Tata Communications eXperience (TCX) portal provides clear executive and operational dashboards, security posture views, and ATT&CK mapping with extensive customization options. LLM-supported agentic analysis helps analysts with triage and investigation while retaining human validation. The open architecture supports integration without replacing existing tools. Areas for improvement include the lack of built-in BAS capabilities and the absence of a dedicated risk advisor in the Standard Tier.

The service provides monitoring, analysis, and response across endpoints, servers, email systems, identity platforms, Edge environments, IoT, OT, mobile devices, and remote and contract workers. It supports all major operating systems and browsers, includes ITDR capabilities, and can discover and monitor shadow IT across the environment. Network analysis covers common encrypted protocols such as DNS, HTTPS, RDP, SSH, and VoIP, as well as a wide range of IoT, ICS, and SCADA protocols. The platform integrates with a broad ecosystem of third-party EPDR, NDR, SIEM, SOAR, identity, SASE, DLP, vulnerability, and ASM solutions, including Microsoft Sentinel, Palo Alto Networks Cortex XSOAR, CrowdStrike Falcon Platform, Check Point Horizon NDR, Microsoft Entra ID, Netskope Intelligent SSE, Zscaler Data Protection, and Tenable One Cloud Security. It supports the OCSF.

Tata Communications MDR includes CSPM, CWP, and vulnerability scanning across multi-cloud environments. The service monitors administrative activity, identity misuse, configuration changes, resource sharing, and data movement. It analyzes telemetry from Kubernetes clusters, container platforms, and workload telemetry from container and serverless functions such as Amazon EKS, AWS Lambda, Azure Functions, and GCP services, and correlates cloud DNS and API gateway activity for command-and-control or exfiltration attempts. The solution integrates with major cloud providers and third-party CSPM platforms, including Wiz CNAPP, and includes extensive Microsoft 365 integrations OOTB, including Microsoft Teams, as well as coverage for Microsoft Defender for Cloud Apps, Google Drive, and Google Workspace.

Detection capabilities cover identity compromise, credential misuse, MFA bypass, lateral movement, insider threats, and abnormal data access. Network analytics include east-west

traffic analysis, packet capture, and investigation of unknown signals. Detection models combine behavioral, pattern-based, and ML-driven analytics. Tata Communications reports an average detection time of approximately one minute. The service supports UBA under fully managed, self-managed, or co-managed modes and integrates with third-party IDS and IPS.

The service supports automated and analyst-driven response actions including session termination, JIT privilege revocation, DNS redirection, configuration rollback, and on-demand packet capture across endpoints and network segments. Through integration with identity providers and PAM platforms, it can invalidate tokens, disable accounts, remove group memberships, and automatically deprovision users via SCIM, SAML, or API calls. It supports software patching with policy-based control, including scanning and automated deployment, and can block ransomware before encryption. The platform enables fully automated containment when policy allows it. The platform includes native SOAR with dynamic workflows and playbooks and supports integrations with external SOAR platforms. SLAs cover detection and response times and platform availability, while SLOs apply to customer specific integrations and custom requests.

Tata Communications MDR includes automated and manual threat hunting, CTEM, and external ASM. The platform draws threat intelligence from more than 65 sources, customer environments, and the company's own network visibility and DDoS infrastructure. The platform applies threat intelligence in real time for enrichment and correlation and supports multiple exchange standards. Regular reports cover security posture, emerging threats, and hunting outcomes, supported by a dedicated threat hunting team and automated retro threat hunting capabilities.

Innovation centers on agent-assisted analysis, GenAI and Agentic AI-supported investigations, and dynamic response optimization. The platform applies ML–driven behavioral and network analytics across UEBA, attacker behavior detection, identity threat detection, and DDoS detection and mitigation. Behavioral models establish baselines for user logins, privilege use, data access, file transfers, and administrative actions, then identify anomalies such as lateral movement, token misuse, command-and-control patterns, or insider activity. Attacker behavior analytics map activity chains to ATT&CK techniques to expose coordinated campaigns. GenAI assists analysts with summarization, query creation, content development, and policy generation. Tata Communications has introduced agent-assisted triage, automated content management, and dynamic ATT&CK-aligned detection content since the previous assessment. The platform includes deception technologies and ransomware simulation, but BAS is an add-on.

Tata Communications has achieved ISO 27001/27017/27018 and SOC 2 Type II certifications. It also supports regulatory reporting for NIS2, DORA, and GDPR. The service has SOC 2 Type I and Type II attestations. The platform supports data residency in the EU, US, and UAE and can operate within customer-controlled environments to meet sovereignty requirements.

Tata Communications provides support with on-site assistance across APAC, EMEA, NA, and LATAM. The service supports full SOC outsourcing or co-managed operations.

Customers receive a dedicated analyst and a customer success manager as standard. Reporting supports insurer-ready documentation, although cyber insurance is not included. The platform provides dashboards, collaboration tools, and regular risk assessments. Tata Communications provides documentation in multiple languages and supports pre-sales PoC deployments.

Tata Communications MDR is suitable for organizations of all sizes, with particularly medium to large enterprises in regulated sectors such as financial services, manufacturing, automotive, healthcare, and government. It is also relevant for MSPs and MSSPs seeking a white label MDR platform. The service supports IT and OT environments, complex regulatory requirements, regional data residency needs, and organizations seeking strong integration with existing security stacks and network-centric threat visibility.

Strengths

- Carrier scale network visibility and early IoC detection
- Extensive connector base across security and IT systems
- AI agent-assisted triage with human validation
- Good OT and industrial protocol coverage
- Wide coverage, including IoT, mobile devices, and remote workers
- Native SOAR with dynamic response workflows
- Granular data residency and sovereignty support
- Includes software patching
- Highly customizable executive and SOC dashboards
- Includes deception technologies and ransomware simulation

Challenges

- No built-in BAS but it is available as an add-on
- Dedicated risk advisor only at the Executive Tier
- Limited cyber insurance options within the service
- ASM not present in Standard tier

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 several reasons but nevertheless offer a significant contribution to the market space.

Accenture

Accenture is a global professional services company founded in 1989 and headquartered in Dublin, Ireland. The company provides a broad portfolio of technology and security services, including MDR delivered through its managed security operations and cyber defense offerings. Its MDR service integrates Accenture's proprietary threat intelligence, automation capabilities, and global network of Cyber Fusion Centers. Over the past year, Accenture has continued to expand its security operations capacity and refine its MDR portfolio to support organizations across multiple regions and industries.

Why worth watching: Accenture MDR is suited to organizations seeking a partner with global reach, industry-specific expertise, and the ability to integrate MDR outcomes into broader security and business initiatives. It appeals to enterprises looking to supplement internal SOC teams with continuous monitoring, tailored threat insights, and collaborative incident response support, and may also appeal to European organizations that value regional presence, experience with EU regulatory frameworks, and the ability to deliver services through locally operated Cyber Fusion Centers.

AgileBlue

AgileBlue is a privately held cybersecurity company founded in 2019 and headquartered in Cleveland, Ohio, in the US. The company provides cloud-delivered MDR and SOC-as-a-Service capabilities aimed at simplifying threat detection and security operations for resource-constrained teams. AgileBlue's platform combines analytics, behavioral monitoring, and automated response workflows to support customers across regulated industries. In recent years, AgileBlue has expanded its service footprint and enhanced platform automation to improve detection accuracy and operational efficiency.

Why worth watching: AgileBlue MDR is suited to organizations seeking a cost-effective service that supports continuous monitoring while helping teams gain better visibility into threats without heavy operational overhead. It appeals to small and mid-market enterprises looking to strengthen day-to-day security operations with a partner that emphasizes ease of deployment and ongoing support.

Binary Defense

Binary Defense was founded in 2014 and is headquartered in Stow, Ohio, in the US. The company delivers MDR services powered by its AI-supported proprietary detection platform

and analyst-driven threat hunting capabilities. The solution is aimed at helping organizations improve detection speed and incident containment through monitoring of endpoints, networks, cloud environments, and identities. Binary Defense is progressing toward an Open XDR approach to integrate with existing security tools and continues to enhance its platform through analytics improvements and expanded integrations.

Why worth watching: Binary Defense MDR is suited to organizations looking for a service that combines behavioral analytics with human-led investigation to identify high-priority threats. It is a good fit for businesses wanting collaborative incident response guidance and a partner that adapts detection coverage to unique operational requirements.

Blackpoint Cyber

Blackpoint Cyber is a private cybersecurity company founded in 2014 and headquartered in Denver, Colorado, in the US. The company provides MDR services based on its security operations platform, which brings together detection, response, threat intelligence, and partner-focused workflow capabilities. Blackpoint Cyber is known for its extensive engagement with the MSP community and has continued strengthening its offerings through platform enhancements and deeper integrations supporting managed service ecosystems.

Why worth watching: Blackpoint Cyber MDR is suited to organizations working with MSPs or those needing a service that rapidly investigates and contains active threats. It appeals to businesses seeking a partner with established operational processes, clear communication, and strong alignment with IT service providers.

Expel

Expel is a private security operations provider, founded in 2016 and headquartered in Herndon, Virginia, in the US. Expel MDR is delivered through the Expel Workbench, a cloud-native, multi-tenant platform that supports monitoring and analysis across customer environments. The company's service model emphasizes transparency, guided remediation, and the ability to integrate with a wide range of security tools. Expel continues expanding its detection coverage, including support for cloud and Kubernetes environments.

Why worth watching: Expel MDR is suitable for most companies, particularly medium-sized businesses and mid-market enterprises, looking to maximize returns on existing investments. It is well-suited to organizations seeking full MDR coverage with clear operational guidance and a focus on accelerating response outcomes.

Fortinet

Fortinet is a public cybersecurity company founded in 2000 and headquartered in Sunnyvale, California, in the US. Fortinet Managed Detection and Response is a cloud-based service built on FortiEDR and FortiXDR and supported by Fortinet's global network of SOCs. The service integrates telemetry from Fortinet's security portfolio as well as third-

party products to enhance detection quality. Over the past year, Fortinet has continued expanding AI-assisted analytics and response automation within its MDR service.

Why worth watching: Fortinet MDR supports all but the smallest businesses and is suited to medium and mid-market enterprises that have internal SOCs and need continuous threat monitoring, alert management, automated containment, and assistance with incident remediation. The service can supplement existing internal SOCs or act as an outsourced team for organizations with limited resources. Its broad partner ecosystem, strong presence across EMEA, and integration with widely deployed Fortinet security infrastructure also make it relevant to European organizations seeking MDR that can extend existing Fortinet deployments.

Fortra

Fortra, formerly HelpSystems, is a private cybersecurity company founded in 1982 and headquartered in Eden Prairie, Minnesota, in the US. The company has expanded significantly through acquisitions over the past several years and now provides a broad security portfolio covering email security, data protection, threat intelligence, and security operations. Fortra MDR leverages the company's consolidated technologies and security operations expertise to provide monitoring, detection, and guided response support.

Why worth watching: Fortra MDR is suited to organizations looking for a service built on integrated security technologies that reduce operational complexity. It appeals to customers that want MDR connected to data protection, email threat defense, and threat intelligence capabilities within a single ecosystem.

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 delivered as a managed service built on IBM's MDR platform and supported by IBM global SOCs. The service provides monitoring and detection across customer environments, regardless of technology location, with options for customization and integration with third-party security products. IBM continues to evolve its MDR offerings with AI-assisted investigation and automation enhancements.

Why worth watching: IBM Security MDR is suited to large, mid-market, and medium enterprises across all verticals seeking a customizable service with broad technology support. It appeals to organizations that value integration flexibility and want to increase the return on existing security investments while improving response readiness. European organizations may also value IBM's long-standing presence in the region, local delivery capabilities, and experience supporting regulatory requirements and complex multi-country environments.

Kudelski Security

Kudelski Security was launched in 2012 as the cybersecurity division of the Kudelski Group and is headquartered in Cheseaux-sur-Lausanne, Switzerland, with a US headquarters in Phoenix, Arizona. The company delivers a mix of managed security services and advisory work, with MDR anchored in its Cyber Fusion Center operations. Its MDR services are powered by FusionDetect, which acts as the security analytics and response layer used by Kudelski Security analysts. The offer targets mid-market and enterprise organizations that want provider-run monitoring, threat hunting, and guided response.

Why worth watching: Kudelski Security combines FusionDetect automation with a high-touch operating model that keeps analysts close to investigations and remediation steps. It is worth tracking for organizations that want MDR that can plug into existing detection tooling while adding structured threat hunting and response workflows through the Cyber Fusion Center, including European organizations that value regional presence and familiarity with European regulatory expectations.

LevelBlue

LevelBlue was launched in 2024 and was formed through the combination of AT&T Cybersecurity and WillJam Ventures, with is headquarters in Dallas, Texas, in the US. The company delivers threat detection, vulnerability management, and security operations services through its Unified Security Management platform, which continues to advance with updated analytics and integration features. LevelBlue has expanded significantly through acquisition, including Cybereason in 2025, adding its XDR technology, incident response expertise, and global research team to the MDR portfolio. The company also acquired Trustwave, Identity Sentinel, and PhishGuard, bringing additional threat intelligence, identity-focused detection, and phishing simulation capabilities into its service stack.

Why worth watching: LevelBlue MDR is suited to organizations looking for comprehensive monitoring and response across endpoint, network, cloud, and identity layers supported through a unified operational model. It appeals to small and mid-market enterprises seeking an MDR partner that simplifies security operations while incorporating extended threat intelligence and enrichment gained through recent acquisitions.

Obrela

Obrela is a private cybersecurity services company founded in 2009 with roots in Athens, Greece and headquarters in London, UK. It maintains a major operational and delivery center in Athens and has a presence in the Middle East. Obrela acquired Encode at the end of 2021 and expanded its MDR delivery and engineering capabilities. Obrela MDR is delivered using its Swordfish platform, including the SOCStreams module for incident workflow and automation.

Why worth watching: Obrela is adding Agentic AI into Swordfish for MDR triage and response automation, with published updates in February 2026. The combination of a service-led MDR model and a provider-built operations platform makes it worth watching for organizations that want to outsource SOC operations or augment smaller internal teams. Its

European base and operational presence within the region may also appeal to European organizations that prefer MDR providers with regional delivery capabilities and familiarity with European regulatory requirements.

Ontinue

Ontinue is a private MDR services company established in 2023, with dual headquarters in Redwood City, California, in the US, and Zurich, Switzerland. Ontinue originated from the former MXDR division of Open Systems and has operated as a standalone business under the Ontinue brand since the separation. ION MXDR is designed for organizations standardized on the Microsoft security stack and uses Microsoft Teams as the primary user interface, which reduces the need for an additional MDR console. It offers add-on services for vulnerability mitigation and IoT security.

Why worth watching: Ontinue is pushing automation in Microsoft-focused SecOps, including Agentic AI-based investigations introduced in June 2025 to reduce investigation time and resolve most incidents without customer involvement. The Teams-based operating model supports fast collaboration and quick engagement with senior analysts, which suits organizations that want to outsource SOC operations or supplement smaller internal teams while staying inside the Microsoft tooling they already use. The headquarters in Zurich and established presence in Europe may also appeal to organizations that prefer MDR providers with European operational capabilities and proximity to local customers.

Palo Alto Networks

Palo Alto Networks is a public cybersecurity company founded in 2005 and headquartered in Santa Clara, California, in the US. Its MDR offering is delivered through Palo Alto Networks security operations platform, which brings together analytics, automation, threat intelligence, and telemetry from the company’s endpoint, network, and cloud products. The service is supported by global SOC teams and integrates AI-driven detection to accelerate analyst workflows. Recent enhancements have expanded detection depth across identity, cloud workloads, and application-level activity.

Why worth watching: Palo Alto Networks MDR is suited to organizations looking for a service that aligns closely with a consolidated security operations platform. It appeals to enterprises seeking consistent monitoring and response across multiple security domains while benefiting from integrated threat intelligence and automated response actions. The global SOC model and strong presence in the European enterprise market also make the service relevant to European customers that want MDR closely aligned with widely deployed Palo Alto Networks security technologies and regional regulatory and operational requirements.

PricewaterhouseCoopers (PwC)

PwC, founded in 1998 through the merger of Price Waterhouse and Coopers & Lybrand, is headquartered in London, UK, with SOCs across multiple global regions. PwC's Managed Cyber Defense and MDR services provide 24/7 monitoring, threat hunting, and incident response supported by its analysts and detection engineering teams. These services are delivered through standardized playbooks, analytics pipelines, and service portals integrated with leading XDR and SIEM platforms. PwC continues to expand automation within its MDR workflows and strengthen alignment with its broader incident response and threat intelligence services.

Why worth watching: PwC MDR is suited to mid-market and enterprise organizations looking for a service that enhances internal SOC capabilities with continuous monitoring and guided investigation support. It appeals to businesses seeking a partner with established operational processes, threat intelligence resources, and the ability to help mature security operations over time. Its European headquarters, regional SOC presence, and experience supporting regulatory frameworks such as GDPR and NIS2 also make it relevant to organizations operating in highly regulated European markets.

Proficio

Proficio is a private cybersecurity services company founded in 2010 and headquartered in Carlsbad, California, in the US. It provides MDR, managed security services, and SOC services, delivering 24/7 monitoring from its SOC operations in San Diego, Barcelona, and Singapore. Proficio's flagship ProSOC MDR service is delivered as a fully hosted platform or as a co-managed model that works with customer-owned SIEM deployments. In 2025, Proficio also expanded its managed XDR offering through a partnership that brings additional XDR telemetry and response options into its service.

Why worth watching: Proficio featured among the Overall, Product, and Innovation leaders in the previous edition of this report. It continues to invest in automation and analyst-assist capabilities, including an AI Assistant module designed to speed investigation and improve response workflow for ProSOC MDR teams. For organizations that want to outsource day-to-day detection and response while retaining visibility and control, its combination of SOCaaS delivery and co-managed options provides a way to balance services with internal capacity.

Rapid7

Rapid7 was founded in 2000 and is headquartered in Boston, Massachusetts in the US. It is a public company that provides MDR through its Managed Threat Complete (MTC) service, delivered under a SaaS model as a cloud service and a managed service. MTC is sold as fixed cost packages across Essential, Advanced, and Ultimate tiers, priced for a defined asset count and contract term. In 2024, Rapid7 acquired Noetic Cyber to expand cyber asset ASM in its platform.

Why worth watching: MTC brings together SOC services with SIEM, SOAR, vulnerability management, and incident response, and it can also manage selected third-party security

tools already deployed by customers. Rapid7 has continued to invest in SOC automation through Agentic AI workflows and related operational features that aim to reduce analyst workload and speed investigations.

Red Canary

Red Canary, a Zscaler company, is an MDR provider founded in 2014 and based in Denver, Colorado, in the US. In August 2025, Red Canary was acquired by Zscaler and now operates as a separate business unit while its technology is progressively integrated into the broader Zscaler platform. The MDR service continues to deliver endpoint, network, identity, and cloud coverage supported by Red Canary's detection engineering, threat hunting, and analyst-led investigation. The acquisition is aimed at aligning Red Canary's capabilities with Zscaler's push toward a unified, AI-driven security operations experience.

Why worth watching: Red Canary MDR is suited to organizations of all sizes, particularly those running Linux-based production systems or seeking tight alignment between detection, response, and secure access workflows. It appeals to companies looking for an MDR partner that maintains its established operational model while benefiting from deeper integration with Zscaler's security platform.

ReliaQuest

Founded in 2007 and headquartered in Tampa, Florida, in the US, ReliaQuest is a privately held cybersecurity technology company delivering managed detection and response services for mid-sized and large organizations. Its MDR offering is built on the GreyMatter platform, an ML-driven security operations platform based on an open XDR approach. ReliaQuest operates multiple global SOCs across NA, Europe, and India, providing continuous monitoring and response coverage. GreyMatter supports deployment as a fully cloud-based service or in configurations that include on-premises components, enabling organizations to integrate existing security tools while retaining control over their environments.

Why worth watching: ReliaQuest featured among the Overall, Product, Innovation, and Market leaders in the previous edition of this report. It is notable for its open XDR-driven MDR service that allows customers to retain and operationalize their existing security investments while benefiting from automation, threat intelligence, and analyst-led response. The GreyMatter platform supports rapid onboarding, broad third-party integrations, and consistent visibility across endpoints, networks, cloud services, and operational environments. The solution is aimed at supporting analyst efficiency, automation, and shared access to tools and data. This aligns well with organizations looking to supplement internal security teams without relinquishing operational transparency.

SecurityHQ

SecurityHQ is a privately held global managed security services provider founded in 2003, with headquarters in London, UK. SecurityHQ MDR is a cloud-based service established in 2008 and built on the company's Response Platform, which unifies threat monitoring, analytics, and incident handling workflows. The company operates multiple SOCs internationally and maintains a strong regional presence across EMEA and other regions.

Why worth watching: SecurityHQ MDR supports organizations of all sizes but is well-suited to medium and mid-market enterprises looking for a customizable service with continual security recommendations. Its strong presence across Europe and wider EMEA, combined with SOC coverage in the region, makes it attractive to European organizations that require local expertise, regional support, and alignment with European regulatory expectations. It appeals to organizations that value the combination of regional presence, analyst expertise, and adaptable service models.

SentinelOne

SentinelOne is a cybersecurity company founded in 2013 and headquartered in Mountain View, California, in the US. The company offers advanced endpoint protection and response capabilities through its Singularity platform, which integrates EPP, EDR, and XDR. SentinelOne's Singularity MDR service combines platform telemetry with human expertise to deliver monitoring, investigation, and guided remediation. Recent updates extend detection and response across cloud, identity, email, and network signals.

Why worth watching: SentinelOne's Singularity MDR suits organizations seeking a rapid response service that blends AI-assisted analytics with human investigation. It appeals to businesses needing transparent operations, optional forensic services, and broad threat coverage beyond endpoint activity. The service is also relevant for European organizations through SentinelOne's strong presence in the EMEA market, regional SOC coverage, and support for data residency and regulatory requirements common in European environments.

ThreatLocker

ThreatLocker is a private cybersecurity company founded in 2017 and headquartered in Orlando, Florida, in the US. The company focuses on endpoint-centric security controls delivered through its Zero Trust Platform, combining application allowlisting, privilege management, and endpoint detection capabilities. Its MDR service, Cyber Hero MDR, builds on this controls-first approach and is delivered as a SaaS offering supported by a global SOC. ThreatLocker primarily serves mid-market organizations, with growing adoption through MSP and MSSP channels and an expanding international presence.

Why worth watching: ThreatLocker Cyber Hero MDR takes a controls-first approach, using deny-by-default enforcement at the endpoint to prevent malicious activity before detection and response workflows are triggered. This makes it particularly relevant for organizations seeking tightly integrated endpoint protection and MDR, especially those looking to reduce reliance on alert-driven response models and strengthen operational control over endpoint behavior.

Uptycs

Uptycs was founded in 2016 and is headquartered in Waltham, Massachusetts, in the US. It is a privately held cybersecurity company that provides a unified security analytics platform covering endpoints, containers, Kubernetes, cloud services, and developer environments. Its MDR service is delivered as an extension of the Uptycs CNAPP and is supported by a follow-the-sun SOC with analysts based in the US, India, and Australia. Uptycs serves primarily large organizations in NA and EMEA, with delivery through channel partners only.

Why worth watching: Uptycs MDR is structured around graduated service levels that allow organizations to move from assisted onboarding to full monitoring and response as operational needs change. Its tight integration with the Uptycs platform makes it particularly relevant for organizations that want MDR coverage tightly aligned with endpoint, workload, and Kubernetes security without introducing additional tooling layers.

WatchGuard

WatchGuard Technologies was founded in 1996 and is headquartered in Seattle, Washington, in the US. The company is best known for security products sold through channel partners, but it has expanded its managed services portfolio in recent years. WatchGuard offers MDR services in tiers that include WatchGuard Core MDR, WatchGuard Core MDR for Microsoft, and WatchGuard Total MDR. In January 2025, WatchGuard acquired ActZero to strengthen its 24/7 MDR capabilities and SOC operations.

Why worth watching: WatchGuard MDR merits attention from organizations that want round-the-clock monitoring, threat hunting, investigation, and containment delivered as a managed service, without building their own SOC. The portfolio also includes options aligned to Microsoft environments and a “Total MDR” tier that extends coverage across the WatchGuard security technology stack, which may appeal to teams seeking to supplement internal security operations with a single managed offering.

Related Research

Leadership Compass: Managed Detection and Response (MDR) 2024

Leadership Compass: Identity Threat Detection and Response (ITDR)

Leadership Compass: Network Detection and Response (NDR)

Leadership Compass: eXtended Detection and Response (XDR)

Leadership Compass: Attack Surface Management

Leadership Compass: Endpoint Protection Detection and Response (EPDR)

Buyer's Compass: Managed Detection and Response (MDR)

Analyst's View: Managed Detection and Response (MDR)

Copyright

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole Analysts 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 technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

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