

Beyond the SOC

A CISO's guide for evaluating
MDR services in the age of AI



Atos

Executive Summary: Rethinking MDR in today's threat landscape

Today, security leaders face a new reality. Cybersecurity is no longer measured by how many threats are detected, but by how effectively the organization continues operating when faced with a disruption.

The challenge is shifting from threat detection and visibility or risks to operational resilience.

For more than a decade now, organizations have invested heavily in security tools, telemetry and detection capabilities. Yet many still struggle with the same operational challenge of transforming visibility into timely decisions and coordinated action. As attack surfaces expand across cloud, identities, connected infrastructure and operational technology, complexity itself has become a security risk.

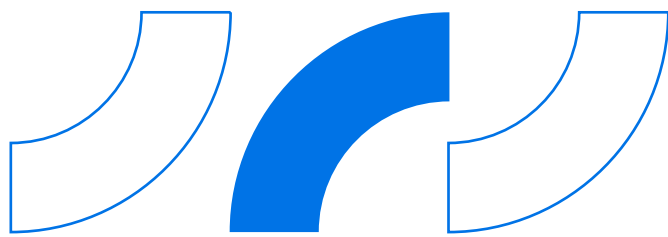
AI is accelerating the speed, scale and sophistication of cyber threats while simultaneously increasing expectations on security teams to respond faster than ever before.

The World Economic Forum's Global Cybersecurity Outlook 2026 identifies AI as the most significant driver of change in cybersecurity for 94% of surveyed organizations, also highlighting growing adoption of AI-enabled cyber defense capabilities. At the same time, CrowdStrike's 2026 Global Threat Report reports that the average cybercrime breakout times fell to 29 minutes, with the fastest observed breakout taking only 27 seconds.

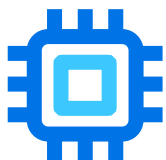
In this environment, Managed Detection and Response (MDR) is no longer simply a monitoring service. It has evolved into a critical operational capability that helps organizations prepare for emerging threats, respond decisively when incidents occur and continuously adapt as risks evolve. The most effective MDR providers deliver far more than alert management. They combine intelligence, automation, human expertise, governance and resilience-oriented operations to help organizations sustain business outcomes under pressure.

Buyers' mindsets have shifted from "Can this provider detect threats?" to "Can this provider help us operate securely, respond decisively and continuously improve resilience as risk changes?"

In this paper, our Atos Cybersecurity experts look to redefine MDR purchasing from a feature-and-alert comparison into a strategic assessment of which provider can best protect your enterprise with business continuity and resilience. It delves into traditional MDR evaluation criteria and why these are no longer sufficient, how a modern MDR service goes beyond alert monitoring, the security operations center (SOC) value that depends on operating capability, an outcome-led evaluation framework for CISOs and expectations from a mature MDR service provider to demonstrate measurable resilience over time.



Five cybersecurity shifts that are redefining MDR evaluation



1. AI is changing both offence and defense.

AI is being used by defenders to accelerate detection, triage and analysis, while attackers use it to increase speed, scale and precision. MDR buyers should not look at AI claims in isolation, but should consciously evaluate AI governance, human oversight and operational usefulness as well.



2. Adversaries are compressing response windows.

When breakout times are measured in minutes, manual handoffs and delayed escalation become business risks. MDR should be assessed by how quickly it can enrich, prioritize, investigate and support containment.



3. Trust is becoming an attack path.

Modern intrusions increasingly move through legitimate identities, cloud services, SaaS platforms and trusted systems. MDR must correlate signals beyond endpoint telemetry and understand the business context of every activity.



4. Security operations are becoming a resilience function.

Boards do not measure security by alert volumes. They are more concerned about whether disruption can be avoided, contained or recovered from. MDR should contribute to measurable resilience outcomes.



5. Sovereignty and regulatory proof matter more.

Data residency, auditability, reporting, local delivery expectations and regulated-sector assurance are now key drivers in the buying process, especially for large enterprises and public-sector organizations.

A modern MDR evaluation framework for CISOs

A strong MDR decision framework should help security leaders and their teams evaluate capability, operational fitness and long-term value before purchasing. The 8 dimensions highlighted below are deliberately customer-oriented: they focus on the outcomes an MDR buyer — the organization, its security leaders and teams — should expect, while leveraging the strengths of mature MDR providers.

#	Dimension	A buyer's outlook	Why this matters	How mature MDR providers demonstrate it
1	Visibility without blind spots	Can the provider understand my risks and consolidate relevant signals across IT, cloud, endpoint, identity, network and OT/IoT environments?	Disconnected telemetry slows investigation. Unified visibility helps teams understand attack paths rather than isolated alerts.	• Telemetry aligned with business risks • Full-stack visibility across IT, cloud, endpoints, identity, network and OT/IoT • Vendor-agnostic integration across existing security investments
2	Intelligence that improves decisions	How does threat intelligence become detection logic, hunting hypotheses and actionable response guidance?	Threat intelligence has limited value if it remains a report. It should continuously improve detections, prioritization and response playbooks.	• Focus on global threat intelligence. • Focus on strong proactive detection engineering • Often has a dedicated Threat Research Center
3	Human expertise at scale	What expertise is available beyond first-line monitoring when an incident becomes complex?	AI can accelerate investigations, but experienced analysts, threat hunters and responders are critical when context and judgement matter.	• A global security operations center (SOC) network with regional capacity, threat hunting support and DFIR integration
4	Response maturity	What happens after a high-risk threat is identified?	The value of MDR is measured in reduced exposure and faster containment, not simply in alerts processed.	• Solution highlights include continuous monitoring, investigation, remote containment, guided remediation and automation to minimize impact
5	Technology and operating flexibility	Can the service work with the organization's current ecosystem and maturity level?	MDR should reduce operational friction. It should not begin with forced technology replacement where existing investments can be optimized.	• Innovative delivery models, including end-to-end service, Managed Microsoft XDR, flexible technology-agnostic MDR, full outcome-based service and co-management
6	Governance and accountability	How are ownership, escalation, reporting and decision rights defined?	When incidents escalate, ambiguity creates delay. Effective MDR partnerships clarify accountability before a crisis occurs.	• Operational accountability for transparent outcomes • Portal-based visibility and SLA-driven accountability
7	Resilience contribution	How does the MDR engagement improve readiness, response and continuous improvement over time?	Modern MDR should help organizations become harder to disrupt — not only faster to notify Modern MDR is proactive by design.	• Reduced dwell time • Combined MDR and Vulnerability operation • Strong Detection engineering
8	AI governance and operational trust	How is AI governed, validated and supervised across the MDR service?	AI can improve detection, investigation and response efficiency, but it can also introduce operational, regulatory and trust-related risks if deployed without sufficient oversight.	• A combination of AI-assisted workflows with human analyst oversight, clear governance processes, explainability controls and continuous validation mechanisms • Trustworthy operational outcomes
9	Tailored to client risk exposure and context	Human and AI analyst aligned to deliver outcomes tailored to client risks and attack surface	When alerts are processed or when new detections are engineered, they need to adapt to each client unique context	• Agentic AI tuned to client realities • Strong client context applied to alert management and detection engineering

Why modern SOC architecture is critical to MDR success

A security operations center (SOC) is often discussed as a place or a team. In a modern MDR engagement, it should be evaluated as an operating capability, with its value derived from how it combines telemetry, workflows, people, intelligence, automation and governance to reduce the time between signal and action.

For large enterprises, especially those operating across regions, sectors or regulated environments, SOC architecture matters because cyber incidents do not respect organizational silos. A cloud identity signal, an endpoint event, a network anomaly and an OT concern may be part of the same attack sequence. The MDR provider's SOC model must be able to connect those signals, apply context and support coordinated response.

The business value of a mature SOC model

A mature SOC model gives the enterprise three things at once:

- Monitoring continuity
- Specialist expertise
- A repeatable governance model for response

That combination is difficult to build internally at a global scale, especially as threats accelerate and security talent remains constrained.

When evaluating an MDR provider, here are some of the key capabilities that buyers need to consider:

SOC capabilities	Why it matters to the enterprise	Questions to ask a provider
Global and local coverage	Supports continuity while respecting regional operating and regulatory requirements	• How do global and local SOC teams collaborate during an incident?
Specialist escalation paths	Ensures complex threats can move beyond first-line triage into threat hunting, DFIR or crisis response	• What expertise is available when an incident exceeds routine monitoring?
Security data integration	A holistic detection design matching client risks. Helps reduce blind spots by connecting signals across domains and existing tools	• Which telemetry sources can be integrated without forcing a rip-and-replace approach? • If AI is used, how and where is my data processed
AI security and governance	AI should accelerates MDR while analysts retain accountability for consequential response actions.	• Which actions are fully automated, analyst-approved or customer-approved? Where AI is applied, are the right guardrails in place?
Executive and operational reporting	Provides CISOs with evidence for risk, compliance and board-level conversations	• Can reporting be tailored for SOC teams, executives and compliance stakeholders?

Six questions to ask an MDR provider

Here are 6 questions designed to reveal a provider's maturity, not just salient features of the service.



1. How do you support sovereign security operations and data residency requirements?



2. How do you extend MDR coverage across operational technology and critical infrastructure environments?



3. What specialist expertise can you deploy when an incident exceeds normal monitoring activities?



4. How do you improve resilience outcomes rather than simply reduce alert volumes or process alerts timely ?



5. How do you help organizations optimize existing security investments rather than replace them?



6. How is AI governed, validated and supervised within security operations?

Evaluation dimension	Suggested weight	Provider A	Provider B	Provider C
Visibility across attack surface	15%			
Threat intelligence and detection engineering	15%			
Technology flexibility and integration model	15%			
Response and DFIR integration	15%			
SOC maturity and specialist expertise	10%			
Governance, reporting and accountability	10%			
Resilience contribution and continuous improvement	10%			
AI governance and operational trust	10%			

Common MDR evaluation pitfalls to avoid

During the evaluation phase, buyers shouldn't just be looking for what they need but should also pay close attention to any signs that the MDR engagement may become a monitoring contract rather than a resilience partnership. Here are a few signs to watch out for:

Tool-first conversation

The provider leads with platform features but cannot clearly explain operational outcomes, governance or response ownership.

Limited telemetry scope

Coverage is concentrated in only one domain, making it difficult to detect attacks that move across identity, cloud, endpoint and network layers.

Unclear response authority

The provider detects and escalates, but containment responsibilities and decision rights are ambiguous.

Forced replacement model

The service assumes a technology migration before value can be delivered, even where existing tools are fit for purpose.

Reporting without board relevance

Reports focus on alert volume rather than business risk, resilience improvement, response effectiveness or compliance evidence..

AI without governance

AI is described as a differentiator, but there is little clarity on oversight, quality assurance, explainability or approved response boundaries. Details of AI processing are not available; what data is processed? Where? (many LLMs operate global or regionally, not at country level)

Gaps in Detection Engineering Relevant and adaptive detection is a key success factor for MDR at Frontier AI time. Detection engineering is not included as a key proactive component of the MDR service.

AI without governance

AI is described as a differentiator, but there is little clarity on oversight, quality assurance, explainability or approved response boundaries. Details of AI processing are not available; what data is processed? Where? (many LLMs operate global or regionally, not at country level)

Gaps in Detection Engineering Relevant and adaptive detection is a key success factor for MDR at Frontier AI time. Detection engineering is not included as a key proactive component of the MDR service.

MDR disconnected from vulnerability management

Lack of convergence between MDR and vulnerability management. When these operations remain siloed, organizations cannot correlate active threats with known vulnerabilities, weakening risk-based prioritization and delaying remediation of the exposures most likely to be exploited.

Remember, the right MDR provider will extend beyond monitoring to strengthen a buyer's resilience – integrating with the new environment, taking clear ownership of response and demonstrating measurable improvements in business risk and preparedness.

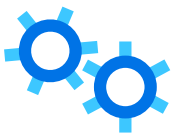
Next steps: Resilience over detection

The future of MDR is not about processing more alerts or monitoring more data sources. It is about helping organizations operate confidently in an environment where threats move faster, attack surfaces continue to expand and cyber incidents increasingly have direct business consequences.

The most effective MDR relationships do not simply detect attacks. They help organizations prepare through better visibility and intelligence, respond through coordinated security operations and adapt through continuous improvement and governance. As organizations evaluate providers, the most important question is not which vendor has the most tools or the largest analyst team to monitor more.

The more strategic question is, “Who can help our organization operate more securely, respond more confidently and become more resilient?”

Organizations that apply the framework, scorecard and guidance as outlined in this guide will be better positioned to reduce risk, maintain trust and sustain operations under real-world pressure. The next steps will be to test shortlisted providers against real operating scenarios, define outcomes that matter most and demand evidence that the service can deliver under pressure.



Intrigued to know more?
Connect with Atos's cybersecurity experts and MDR specialists to learn how you can deploy a winning MDR framework for sustainable security in a dynamic threat landscape.



Find out how global leaders are embracing the Atos MDR framework for sustainable success and cyber resilience.

About Atos

Atos Group is a global leader in digital transformation with c. 72,000 employees and annual revenue of c. € 10 billion, operating in 68 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing. Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us

atos.net

atos.net/career

Let's start a discussion together



Atos is a registered trademark of Atos SE. May 2025. © Copyright 2025, Atos SE. Confidential Information owned by Atos group, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval of Atos.

000000 - INITIALS DESIGNER + INITIALS BP

The Atos logo, featuring the word 'Atos' in a bold, blue, sans-serif font. The 'o' is stylized with a circular cutout in the center.