RSAC 2026 Insight Report
Security Operations & MDR Landscape

How MDR Is Evolving In The AI SOC Era

Redefining AI Security Threats and Operational Standards

> Speed and judgment now define security resilience.

pago

The Global MDR Frontline
Owning the Decisions That Matter Most

This report begins with an analysis of the structural changes shaping the cybersecurity market observed at RSAC 2026. These changes, however, did not end with the conference itself.

In the weeks following RSAC, new developments and discussions surrounding Mythos AI rapidly gained momentum, once again changing market perceptions around AI driven security threats and defensive operations. With that context in mind, this report expands beyond the themes identified during RSAC to also examine the recent Mythos related developments and the market response that followed.

The goal is to provide a more comprehensive view of the current security environment. In particular, the report examines the gap between growing fears surrounding AI driven threats and the actual level of risk organizations face today. The analysis focuses on what organizations should realistically prepare for from a Security Operations perspective.

Table of Contents

MDR in the AI SOC Era

The Rise of AI SOC, the Evolution of MDR, and Where PAGO Stands

RSAC 2026 was far more than an event centered on AI as an industry trend. This year's conference highlighted a core industry transformation: cybersecurity is being shaped by operational models rather than standalone products. The center of gravity is moving toward operational security models built around Security Operations.

Held at San Francisco's Moscone Center from March 23 to 26, RSAC 2026 featured more than 700 speakers, 31 conference tracks, over 570 sessions, and more than 600 exhibitors. Across the event, discussions focused on how AI is accelerating both cyber risk and cyber defense at the same time. Three major themes stood out throughout the conference.

- First, MDR has evolved from a specialized service offered by a limited number of providers into a core market category;
- Second, as AI becomes embedded into security operations, the SOC itself is being redefined into what many now describe as the AI SOC or Agentic SOC;
- Third, despite rapid advances in AI and automation, the defining factor still comes down to who can make accurate decisions and respond with accountability when it matters most;

These trends underscore an industry-wide transition across the cybersecurity market. What is changing is not only the technology adoption, but the operational model itself.

Cyber defense frameworks are evolving toward a model built on Security Operations Platforms integrated with MDR. RSAC 2026 showed that this transition is already moving from concept to reality at a rapid pace.

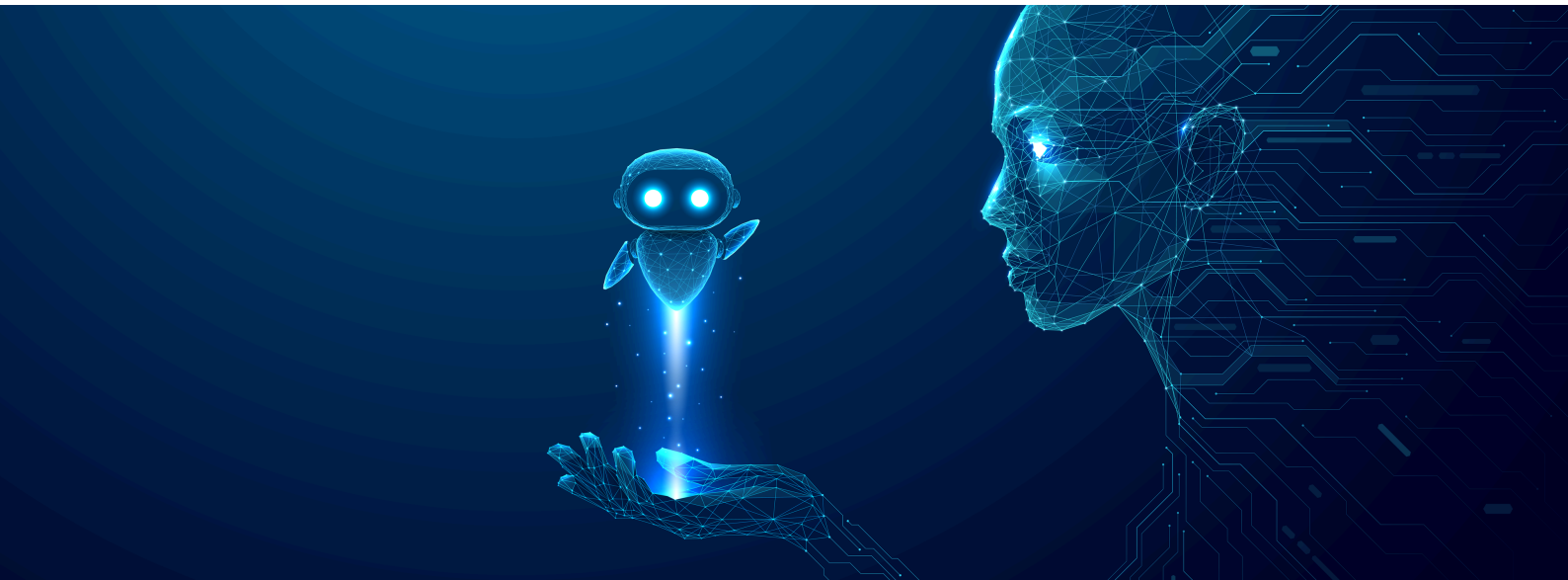
1. The Core Theme of RSAC 2026: AI Is Reshaping Security Operations

AI was unquestionably the dominant theme throughout RSAC 2026. More important than the volume of AI related announcements, however, was the way AI was being positioned within security operations.

Ahead of the conference, RSAC had already identified AI security, cloud attacks, and emerging threats as major themes for 2026. Across keynote sessions and the exhibition floor, AI emerged as a core operational model shaping how security teams investigate, prioritize, and respond to threats. Much of the discussion focused on accelerating the early stages of security operations, including triage, classification, and investigation workflows. Rather than centering on the idea of fully replacing analysts, vendors concentrated on how AI could reduce the operational burden on SOC teams and improve response speed.

Many of the AI SOC platform providers highlighted the use of agentic AI to automate or compress Level 1 triage work, allowing analysts to focus more on higher value decision making and response coordination. At the same time, accountability for operational judgment and final response actions remained tied to human operators. This distinction became one of the defining themes of the conference. Although terms such as “autonomous security” appeared frequently across the event, the direction of the market reflected a more practical operating model built around analyst augmentation and operational acceleration.

AI is already embedded into most of the front end of security operations, especially in areas involving data correlation, event prioritization, and investigative workflows. The interpretation of incidents, escalation decisions, and response ownership, however, continue to depend on experienced analysts and operational teams. These market pressures redefine the baseline requirements for MDR. The value of MDR comes from operational judgment, response coordination, and accountability during critical moments, rather than automation itself.



2. MDR and the Shift Toward Operational Execution

A few years ago, MDR was still viewed as a specialized operating model used by a limited segment of the cybersecurity market. RSAC 2026 showed how quickly that perception has changed. Today, almost every major vendor, platform provider, and security service company is positioning itself around MDR in some form.

As MDR adoption expands across the market, the discussion is shifting toward operational depth and execution quality. The gap between mature MDR services and offerings that remain closer to Managed EDR is becoming much more visible.

Managed EDR focuses on endpoint detection, alert monitoring, and response recommendations. MDR expands on this foundation, combining threat analysis, prioritization, investigation, and response execution across EDR, NDR, XDR, network, identity, and email environments.

The operational difference becomes most visible after detection. What matters is how threats are interpreted, how decisions are made, and how far the response process extends into actual containment and operational action. This movement also changes how organizations evaluate providers. Customers are placing greater focus on operational accountability, response ownership, and integration capabilities across complex environments.

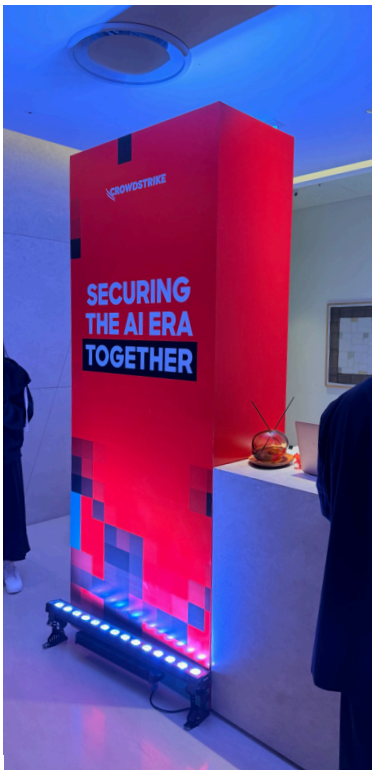
Organizations want to understand:

- Who makes decisions during an active incident?
- Who takes responsibility for investigative findings?
- How deeply the provider participates in response and containment;
- Whether multiple security technologies can be operationally integrated into a unified workflow;

RSAC 2026 showed that MDR competitiveness is now shaped by operational maturity, decision making structures, and the ability to execute effectively during real incidents.

> **As MDR becomes a standard offering across the industry, a sharper distinction is emerging between mature MDR services and Managed EDR level offerings.**

3. RSAC 2026 Vendor Strategies: Market Positioning



CrowdStrike: Expanding the Agentic SOC Platform Strategy

At RSAC 2026, CrowdStrike centered its messaging around **"Securing the AI Era Together"** while placing strong emphasis on what it described as **"the future of the agentic SOC."**

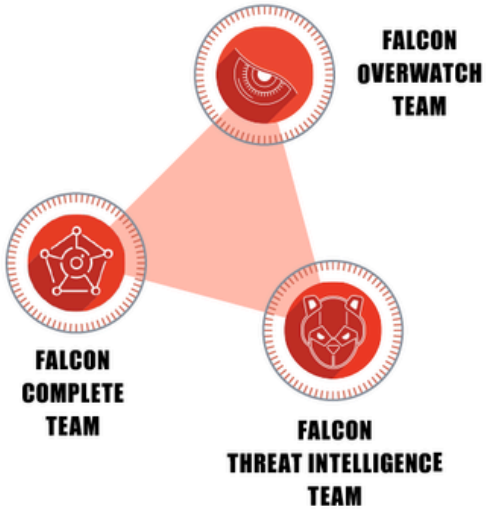
CEO George Kurtz focused heavily on AI security and governance during his keynote, while the Falcon Spring '26 release highlighted AI, unified data, and platform driven security operations.

A major theme throughout CrowdStrike's positioning was the idea of the endpoint becoming the central layer for AI security operations. This reflects a broader effort to evolve beyond traditional endpoint protection and position the Falcon platform as the operational foundation for AI era security.

The company also reinforced its platform strategy by integrating MDR, AI capabilities, operational automation, and flexible consumption models into a single operating structure.

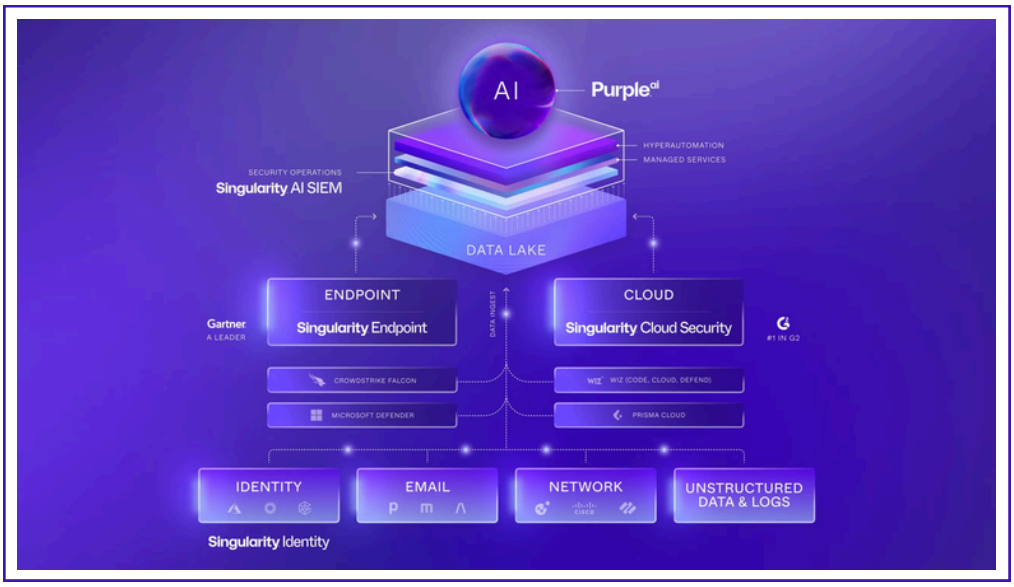
Rather than positioning MDR as a standalone service, CrowdStrike presented it as part of the platform experience itself.

This direction points to an industry redefinition as security operations move toward integrated platforms designed to unify data, workflows, and response execution.



SentinelOne: Purple AI and the Evolution of 'Explainable Automation'

SentinelOne used RSAC 2026 to further expand its AI driven operational strategy centered around Purple AI. According to the company's announcements, Purple AI Auto Investigation has now reached general availability, enabling analysts to perform automated investigations through a unified interface. The platform collects evidence across environments, correlates threat data, and builds attack timelines while integrating response actions through Hyperautomation workflows.



A key element of SentinelOne's messaging was its continued emphasis on "analyst in the loop governance." The company framed AI as a way to accelerate investigations and operational workflows while maintaining human oversight for judgment and operational control.

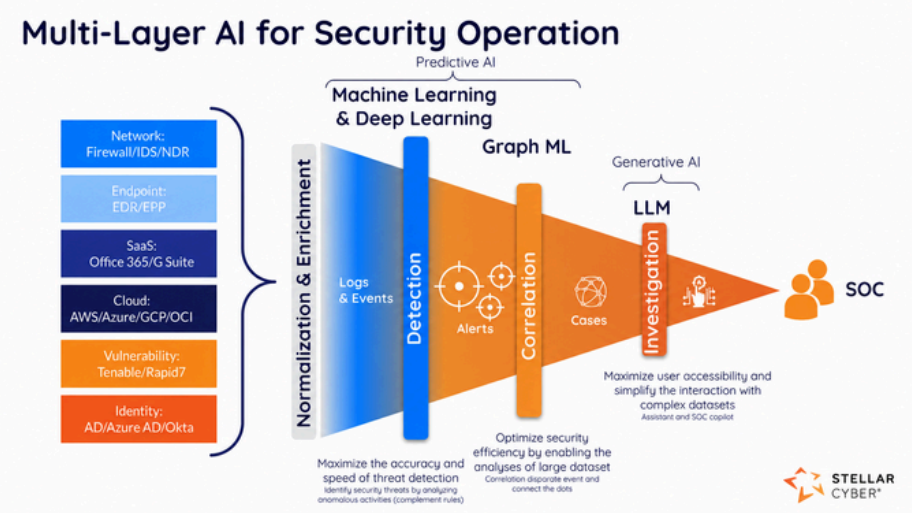
This approach reflects a broader industry direction in which explainability, governance, and operational visibility are becoming more important alongside automation itself.

SentinelOne's strategy also signals continued expansion beyond endpoint security toward a more integrated operational platform combining investigation, analysis, and response functions.

Stellar Cyber: Open XDR and the Expansion of Human Augmented SOC Operations

Stellar Cyber emphasized the concept of the **"Human Augmented Autonomous SOC"** throughout RSAC 2026. Across its messaging, the company positioned GenAI and human expertise as complementary elements within modern security operations.

The platform combines Open XDR, AI driven SIEM, NDR/OT, ITDR, and UEBA into a unified operational structure designed to reduce alert fatigue, automate triage processes, and generate higher fidelity investigative cases.



Stellar Cyber also placed significant focus on MSSP and MDR friendly operational models, reinforcing the importance of platform flexibility across diverse customer environments.

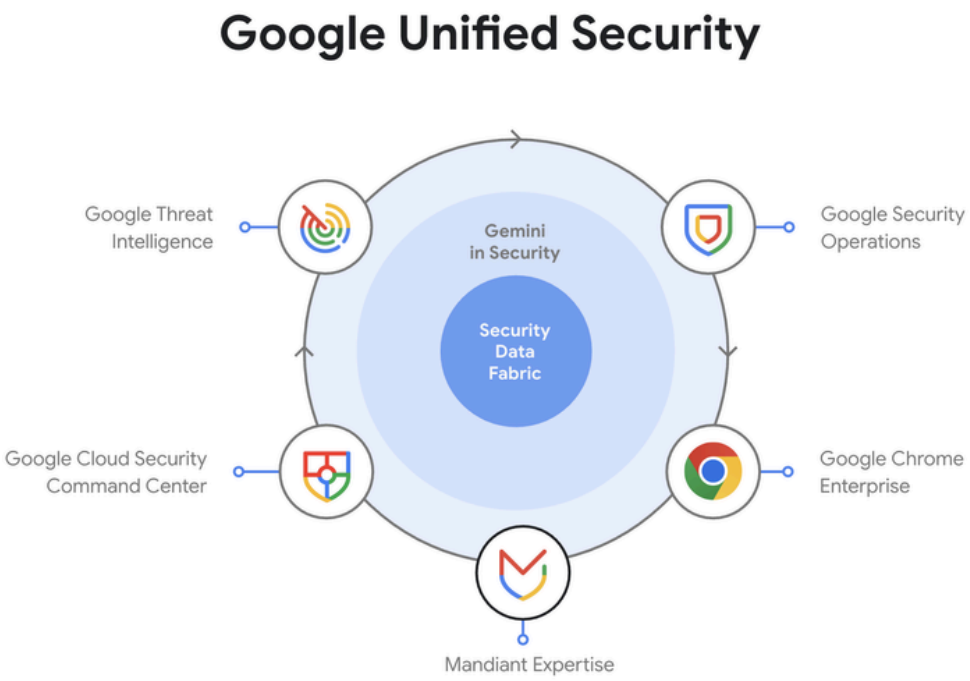
Its overall direction reflects a growing industry preference for open operational architectures capable of integrating multiple technologies and data sources into a unified operational workflow.

The company also reinforced a fundamental operational reality visible across the market: as automation expands, the role of experienced analysts in validating context, interpreting risk, and driving operational decisions gains importance.

Google Security: Connecting SecOps and Threat Intelligence

Google Security presented one of the strongest operational narratives at RSAC 2026 by combining AI powered defense, cloud security, frontline threat intelligence, and agentic SOC concepts into a unified vision for modern security operations.

Across presentations and product discussions, Google connected Mandiant research, Gemini based reasoning, frontline threat intelligence, Wiz integration, and SecOps workflows into a integrated operational model.



One of the most important aspects of Google's positioning was how Security Operations and Threat Intelligence were presented as interconnected operational functions rather than separate capabilities.

This reflects a systemic realignment within modern SOC environments, elevating the need to decode threat context and translate intelligence into immediate operational decisions.

As cloud and hybrid environments continue to grow more complex, the integration of SecOps and Threat Intelligence is evolving into a core operational requirement for modern security teams.

Other Notable Vendors: Different Approaches to Operational Strategy

RSAC 2026 showcased diverse specialized vendors challenging the status quo established by dominant platform providers. While technical strategies differed, their collective focus pointed to a clear industry transition toward execution-centered security frameworks.

Expel described its approach as a "human powered, AI accelerated approach to security operations," emphasizing operational speed and analyst support through AI driven workflows. This reflects how providers are using AI to improve investigation efficiency while keeping human expertise central to operations.

eSentire focused on its Atlas based Security Operations Platform while continuing to emphasize expert validation as a core part of its MDR approach. This reflects how MDR providers are positioning themselves around operational platforms and delivery structures alongside service expertise itself.

Rapid7 expanded its messaging around "Preemptive Security Operations" and "Preemptive MDR," placing greater emphasis on exposure management and proactive operational readiness. This reflects how MDR providers are extending their role beyond post detection response into continuous risk reduction and preparation.

Securonix introduced the phrase "Breach Ready. Board Ready. AI Powered." as part of its RSAC 2026 positioning, highlighting operational readiness and AI enabled security workflows. This reflects how traditional SIEM vendors are evolving toward operationally focused platforms centered around visibility, coordination, and execution.

Although each vendor approached the market in a different way, the overall direction remained consistent throughout RSAC 2026. **Greater emphasis is now being placed on how security operations are structured, integrated, and operationalized across real customer environments.**

Three Structural Shifts Highlighted at RSAC 2026

This year's RSAC reflected three structural transitions taking shape across the cybersecurity industry:

- Security operations are moving toward open architectures designed to integrate diverse technologies and operational workflows.
- AI is being applied primarily to accelerate analysis, investigation, and response processes, helping security teams operate with greater speed and efficiency.
- MDR is gradually changing into an operational model built around platforms, workflows, and execution structures rather than a standalone security service.

4. Mythos AI and the Debate Around AI Security Threats

RSAC 2026 outlined a comprehensive path for the future of security operations. Following the event, discussions surrounding Mythos AI introduced a new variable into how the market understands AI-driven threats and defensive operations.

While RSAC focused on structural changes across the cybersecurity industry, Mythos quickly became an example of how AI related threats are interpreted, amplified, and discussed across the market. The technology is currently spreading through the industry as a next generation form of "Offensive AI," with some viewing it as a development capable of reshaping the security paradigm. At this stage, however, much of the conversation continues to be shaped by uncertainty and interpretation rather than verified operational evidence.

Based on currently available information, Mythos remains a preview system operating within a controlled environment rather than a publicly released commercial model. There have also been no confirmed reports of real world attacks or intrusions directly tied to the platform so far. Even so, the perception that AI driven offensive capabilities are becoming operational reality has continued to spread throughout the market.

This dynamic highlights an important characteristic of today's AI security environment. In many cases, "perceived risk" expands faster than technically verified risk itself. As limited previews, internal materials, and fragmented technical details surrounding Mythos began circulating, narratives around autonomous vulnerability discovery and AI generated exploit development quickly gained momentum. Rumors of hypothetical attack scenarios travel faster than validated facts, amplifying the general sense of uncertainty across the industry.

Questions surrounding whether "AI driven attacks" had already entered operational use appeared repeatedly throughout the market conversation, even in situations where publicly verified evidence remained limited.

PROJECT GLASSWING

Against this backdrop, discussions surrounding Project Glasswing emerged, a collaborative initiative focused on identifying and mitigating vulnerabilities within advanced AI systems. Glasswing can be interpreted as part of a broader industry response framework designed to address the uncertainty and trust concerns amplified by discussions surrounding Mythos AI.

The initiative also illustrates another challenge emerging within AI security. Even defensive frameworks intended to improve safety and transparency can contribute to additional uncertainty when operational details remain highly controlled or selectively disclosed.

Viewed together, Mythos and Glasswing represent more than isolated industry developments. They mirror a systemic cycle in which threat perception, market reaction, and defensive response shape the AI security discussion alongside the technology itself. At a deeper level, the issue extends beyond the emergence of new attack techniques. What is accelerating most rapidly is the speed of both attack and defense operations.

Across recent AI security discussions, one message has appeared repeatedly: AI is not fundamentally reinventing attacker TTPs as much as it is dramatically accelerating execution speed. **The operational window available for detection, investigation, and response is shrinking fast. This pressure reduces security operations to a simple "time and judgment".**

At the same time, defensive AI models are creating similar acceleration on the defensive side. AI driven investigation workflows, event correlation, and automated triage are helping security teams process incidents more quickly and reduce operational burden across SOC environments. As a result, the security environment is evolving into a structure where AI driven attack capabilities and AI driven defense operations advance simultaneously, while human analysts remain responsible for operational judgment and response execution.

This direction underscores the main "Agentic SOC" themes visible throughout RSAC 2026. AI is handling early stage analysis and investigative workflows, while human operators continue to oversee interpretation, escalation, and response decisions. In many ways, the discussion surrounding Mythos reinforces this operational direction rather than changing it. Several key points emerge from this market dynamic:

- AI driven attack capabilities are progressing fast, although a meaningful gap still exists between current market perception and real world operational deployment;
- The defining factor in modern security operations is tied to the speed of attack and response cycles rather than entirely new attack methods;
- Automation is not enough. As operational environments grow faster and more complex, the importance of experienced analysts, operational workflows, and coordinated response structures continues to grow alongside AI adoption.

In this context, Mythos serves as a signal for where security operations are heading and how operational expectations across the cybersecurity industry continue to evolve.

5. The Rise of AI SOC Platforms: A New Operational Layer Emerges

Another major trend highlighted at RSAC 2026 was the growing presence of emerging players centered around AI driven SOC platforms. Across the exhibition floor, a wide range of companies focused on AI agents, SOC automation, autonomous workflows, and AI driven response operations drew all the attention. Related sessions also explored themes such as AI agents, AI autonomy, and reasoning based security operations.

These developments suggest that the security operations market is entering a new phase beyond the traditional structure of products, platforms, and services. In many ways, a new operational layer is beginning to take shape around AI driven SOC operations. Broadly, this movement can be divided into 2 directions:

- **The first is the rise of the "AI SOC Platform," where agentic AI is used to automate or compress Level 1 SOC workflows such as triage, event organization, and initial investigations.**

- **The second is the emergence of "AI MDR," which extends beyond the platform itself into operational delivery models that include onboarding, service workflows, pricing structures, and response operations.**

Both approaches share a common objective: accelerating the earliest stages of security operations through AI driven automation and operational efficiency.

At the same time, these developments do not necessarily point toward fully autonomous security operations. In practice, the opposite dynamic is becoming more visible. As AI driven platforms continue to mature, the role of experienced operational teams becomes even more important in interpreting automated outputs, validating context, and translating analysis into real response actions. Across complex environments and multi stage attack scenarios, final operational judgment and execution continue to remain tied to human decision making.

This reflects a universal industry direction in which security operations are now being shaped through the combination of platforms and operational expertise rather than tools alone. In this context, AI SOC platforms are likely to function less as replacements for existing security operations and more as foundational layers enabling more advanced and scalable operational models.

The Growing Importance of Operationally Driven MDR

RSAC 2026 also reinforced another important message. Even as AI, automation, and platform technologies continue to advance rapidly, the foundation of security operations still revolves around judgment, coordination, and accountability.

Across real customer environments, the central challenge continues to revolve around what happens after detection: how incidents are interpreted, how decisions are made, and how response actions are executed.

This reflects an established operational reality within cyber defense. Security operations focus on organizational structure and decision-making models over isolated technology deployment. Driven by this dynamic, MDR scales into an extended operational framework. Greater emphasis is being placed on the ability to integrate diverse security technologies, manage complex environments, and coordinate operations across multiple layers of infrastructure.

The role of MDR is also growing beyond post detection response into areas such as exposure visibility, operational readiness, and proactive risk management. This reflects the industry's growing focus on operational resilience and continuous preparation alongside incident response itself.

Ultimately, RSAC 2026 reinforced a consistent message across the market. **Security competitiveness is now determined by how effectively organizations can connect technologies, interpret operational context, and translate decisions into coordinated response actions.**

6. MDR Competitiveness Through the Lens of RSAC 2026

One of the most important theme emerging at RSAC 2026 was the growing clarity around how MDR providers are being evaluated across the market. The discussion is centered on how security operations are managed, how decisions are made, and how operational responsibility is carried through real incidents.

Several common characteristics has emerged as key indicators of MDR competitiveness:

Multi Layered Operational Integration

Modern MDR is built around multi layered operational structures that extend beyond EDR into areas such as NDR, XDR, ASM, DRP, and vulnerability management. The focus targets operational models designed to connect varied tools and interpret attacks as part of an end-to-end operational flow rather than isolated events. This direction aligns with the platform strategies and operational models emphasized throughout RSAC 2026.

Operational Scope Beyond Detection

MDR is also expanding further into operational decision making and response execution. Organizations look to providers for detection, analysis, containment, operational coordination, and response actions during active incidents. This requirement highlights a fundamental change in customer expectations, transforming MDR into an element of the operational decision-making process.

AI Integrated with Operational Control

RSAC 2026 also reinforced a consistent theme surrounding AI adoption within security operations. AI is playing an important role in accelerating investigation and analysis workflows, particularly during early stage triage and event processing. At the same time, operational control, escalation decisions, and response accountability continue to be tied to human operators.

As a result, the way organizations integrate AI into operational workflows while maintaining governance and decision making structures is becoming an important point of differentiation.

Expanding Beyond Traditional IT Environments

Security operations are also expanding across diverse environments, including manufacturing, energy, infrastructure, and OT operations. MDR providers are therefore being evaluated not only on technical coverage, but also on their ability to operate across environments with different operational risks and infrastructure requirements. This movement signals a deeper commitment to operational adaptability across complex customer environments.

Flexibility Across Global Environments and Technology Stacks

As customer environments continue to diversify, flexibility is becoming another critical operational requirement. MDR providers are expected to integrate and operate across multiple security technologies, platforms, and infrastructure environments rather than relying on closed vendor ecosystems.
This flexibility is becoming more important for organizations operating across global environments and hybrid technology stacks.

Together, these developments map out the overarching theme of RSAC 2026. MDR is gradually expanding into an operational model centered around integration, execution, operational judgment, and coordinated response capabilities.

7. Conclusion: Returning to the Core of Security Operations

RSAC 2026 demonstrated how quickly AI and platform driven technologies are reshaping the cybersecurity industry. At the same time, the event reinforced another reality that remained consistent across vendor messaging and operational discussions throughout the conference: the foundation of security operations still depends on judgment, coordination, and accountability.

AI driven solutions and automated workflows continue to expand across the market, yet organizations are placing increasing importance on who can understand situations quickly, make accurate operational decisions, and take responsibility during critical moments.

This transitions mirror the natural maturation of the MDR itself. MDR is moving beyond a detection focused service model toward a structure that supports and operates core security operations within customer environments. As technologies and platforms continue to advance, the ability to operationalize those technologies across complex environments is very important. The value of security operations is now far more dependent on how effectively organizations can connect technologies, interpret operational context, and execute coordinated response actions.

RSAC 2026 established a new industry standard, framing the future of MDR around operational depth, decision-making structures, and execution capabilities over simple feature competition.That direction is gradually converging around a single operational reality.

In the AI SOC era, competitive advantage will depend on an organization's ability to operationalize technology, coordinate response, and make decisions under pressure.

www.pagonetworks.com

www.pagonetworks.com