# Coralogix enhances observability platform with AI Centre to tackle risks of artificial intelligence



Coralogix, a Boston-based vendor, is advancing its observability platform by introducing new tools to aid organisations and Managed Security Service Providers (MSSPs) in managing the complexities associated with artificial intelligence (AI). The company recently launched its AI Center, featuring customizable evaluators designed to identify issues that traditional observability tools may overlook, particularly those related to the ethical and operational ramifications of AI usage.

Ariel Assaraf, co-founder and CEO of Coralogix, emphasised the challenges posed by AI in a conversation with MSSP Alert, stating, “AI introduces risks traditional observability tools can’t track. Unlike standard observability, which follows clear right-wrong signals, AI operates in a shifting gray area.” This newly unveiled AI Evaluation Engine continuously monitors AI models, identifies performance issues, and flags various concerns including hallucinations, data leaks, and security vulnerabilities in real time. Assaraf elaborated that the engine transcends typical infrastructure monitoring by addressing specific risks linked to AI.

The urgency for enhanced AI security measures is underscored by a report from global consultancy McKinsey & Co., revealing a surge in enterprise AI adoption. The report indicates that 78% of surveyed organisations utilised AI in at least one business function last year, a rise from 55% in 2023. As AI becomes more integrated into digital infrastructures, cybersecurity expert Exabeam warns of the increasing importance of tailored security measures to mitigate unauthorised access and manipulation of AI systems.

Coralogix’s full-stack observability platform facilitates real-time monitoring of data, application performance, security, and infrastructure. Assaraf critiqued the prevalent approach that treats AI merely as another piece of software that can be safeguarded with conventional security measures. “This approach ignores the reality that AI requires an entirely new infrastructure to handle its evolving risks,” he stated. He cited AI systems’ exposure to novel denial-of-service attacks that exploit token consumption, stressing that while traditional applications are typically monitored for such threats, these new, AI-specific attacks are often neglected.

The AI Center aims to counteract these threats for Coralogix’s more than 2,000 enterprise customers. Apart from the AI Evaluation Engine, the centre features security posture management dashboards to oversee the security and performance of AI agents, tools for tracking user interactions, and performance metrics optimisation. The enhancements are intended to improve real-time threat detection and response efficiency while supporting MSSPs in reducing storage costs significantly without compromising data observation capabilities.

Coralogix’s ongoing development also includes the service Snowbit, launched in 2022, which aggregates various security measures, including SIEM and managed detection and response, into a singular platform. Assaraf mentioned that partnerships, such as the one with Optiv, allow MSSPs to enhance their security services, providing comprehensive AI-specific observability that has previously been unattainable.

The establishment of Coralogix’s AI Centre is partly attributed to the firm’s acquisition of Aporia in December, a startup that specialised in AI observability. As part of their initiative, Coralogix plans to invest heavily in research focusing on the fundamental AI issues of transparency, security, governance, and control, with commitments amounting to tens of millions of dollars over the next two years.

Simultaneously, the landscape of artificial intelligence continues to evolve dramatically, with the rise of intelligent agents significantly impacting the technology's application in both commercial and personal contexts. Following the success of ChatGPT, which surged to 100 million monthly users within a mere two months after its release, industries are observing a shift towards intelligent agents capable of performing autonomous tasks rather than merely generating text.

These intelligent agents transcend traditional functionalities, enabling interactions with digital environments that lead to tangible outcomes. Platforms like DeepResearch and v0 by Vercel exemplify the transformative potential of this new approach which allows for seamless integration between AI and essential workflows, effectively reimagining professional roles across sectors.

As organisations increasingly rely on advanced AI tools, the full implications of these developments—ranging from efficiency enhancements to the ethical challenges posed by autonomous decision-making—remain an area of extensive focus and study. The ongoing evolution in AI indicates that while the pursuit for ever larger models has significant limitations, the integration of modular and collaborative systems heralds a new era in artificial intelligence and its accessibility to various user groups.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.channelinsider.com/news-and-trends/coralogix-ai-center/> - This URL supports the claim about Coralogix launching its AI Center to enhance AI observability and management, providing real-time insights into AI performance and security.
* <https://www.globenewswire.com/news-release/2025/03/19/3045302/0/en/Coralogix-Leverages-Aporia-Acquisition-to-Deliver-True-AI-Observability-Detecting-Hallucinations-Data-Leakage-Toxicity-and-More.html> - This URL corroborates the information about Coralogix's AI Center and its features, including AI evaluation engines and security posture management.
* <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/state-of-ai-in-2023> - This URL would typically support the claim about the rise in enterprise AI adoption, though the specific report mentioned in the article is not directly linked here.
* <https://www.exabeam.com/blog/ai-in-security/> - This URL supports the importance of tailored security measures for AI systems as highlighted by cybersecurity experts like Exabeam.
* <https://www.coralogix.com/platform/> - This URL provides information about Coralogix's full-stack observability platform, which includes real-time monitoring of data, application performance, security, and infrastructure.
* <https://www.openai.com/blog/chatgpt> - This URL supports the claim about the rapid growth and impact of AI tools like ChatGPT, which has significantly influenced the adoption of intelligent agents.