S&P Global
Market Intelligence

Coverage Initiation: Airrived aims to democratize AI agent development

Analysts - Mark Ehr

Publication date: Friday, January 9 2026

Introduction

Airrived is a Dublin, California-based security vendor founded in 2024 by serial entrepreneur Anurag Gurtu and backed by lead investor Cannage Capital. The company is expected to emerge from stealth in January 2026. Airrived offers a platform that enables organizations to create their own AI-native applications and agents without coding. The offering includes an app store that contains ready-to-use agentic applications composed of prebuilt agents and integrations with third-party systems. The company also offers a set of building-block agents that can be used stand-alone or combined with other agents to create complete custom applications, including a set of AI tools designed to create custom agents that satisfy use cases beyond cybersecurity. The Airrived platform can be hosted on-premises, run in a virtual private cloud or hosted on a public PaaS platform (AWS, Azure, Google Cloud Platform and Oracle Cloud Infrastructure are supported).

The Take

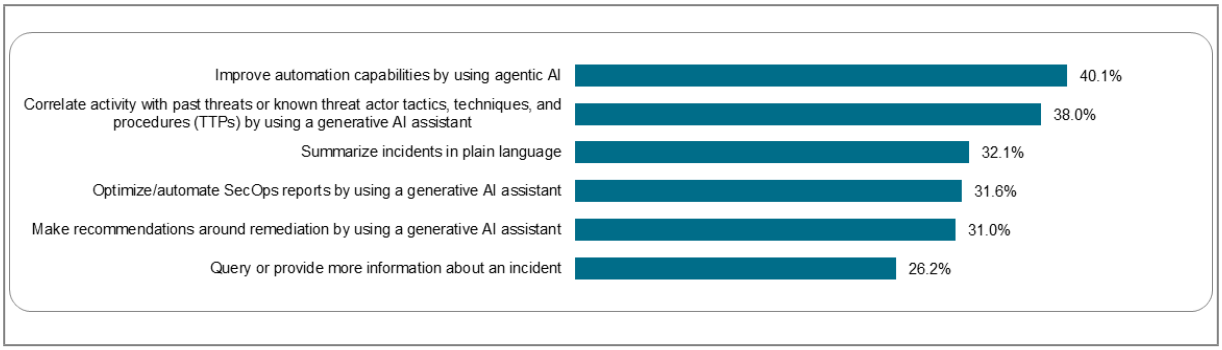
Organizations are turning to GenAI and agentic AI to increase the efficiency of their security operations (SecOps) teams. This is not just an efficiency play: GenAI is widely used by organizations for defensive purposes, as well as by adversaries seeking to increase the sophistication, scale and severity of attacks. This was illustrated when attackers manipulated Anthropic Claude into performing as an autonomous cyber-espionage agent that executed activities ranging from reconnaissance to exploit development, delivery and data analysis. Organizations realize that they must deploy AI to effectively defend against AI-driven attackers. While many security vendors claim to leverage agentic AI, even the largest ones have only a handful of agents capable of performing real work — and those are generally limited to low-risk cases like generating compliance reports, prioritizing vulnerabilities, script analysis and detecting phishing email messages. Some organizations have begun creating their own agents, which can be an expensive undertaking — AI talent is hard to find, and it is not trivial to set up an AI development environment at enterprise scale.

Context

AI (generative AI, in particular) has taken the world by storm, and information security is no exception. 451 Research data bears this out, with respondents to our Voice of the Enterprise: Information Security, SecOps 2025 selecting GenAI assistants as the primary additional technology they have combined with their security information and event management platforms. In the same report, integration of SecOps tooling with GenAI-based tooling was ranked as important by 87% of respondents (49% of whom ranked it "very important"). Agentic AI represents a substantial paradigm shift that allows large language models to evolve beyond passive inference engines into active reasoning controllers capable of executing multi-step workflows, leveraging external APIs to manipulate external systems and transforming LLMs from stateless text generators into state-aware systems capable of orchestrating actions.

A good way to think about the difference between GenAI chatbots and agentic AI is this: An SOC analyst, involved in an ongoing incident investigation, asks a chatbot, "What is the reputation of IP 1.2.3.4?" and receives an answer based on what the LLM knows. In the agentic paradigm, the SOC analyst sets a goal like, "Monitor for suspicious logins, and if verified, lock the account and notify their manager." The agent uses APIs to monitor login activity, determines if there is a potential issue (like checking the reputation of the IP being used), connects to the identity provider API to perform the action and sends an email — all autonomously. And if the organization chooses, it can inject a human into the workflow to analyze the agent's logic and approve or block the action.

Figure 1: GenAI technologies in use by SecOps organizations



Source: 451 Research's Voice of the Enterprise: Information Security, SecOps 2025.
Q. In which of the following ways, if any, does your organization use generative AI technology for SecOps? Please select all that apply.
Base: All respondents, abbreviated fielding (n=187).

Customers

Airrived has been closely involved with several customers that have been using their platform throughout the stealth period, including a large insurance carrier that uses the platform for security operations, threat hunting and firewall rule management; a major US-based fast-casual restaurant chain that uses the platform for threat intelligence operationalization; and an African mobile phone operator and a large US-based fintech firm that use the platform for identity management and access governance. Customers typically start with a single agent and then grow their deployment "virally" from there. The company projects significant growth in 2026.

Competition

Airrived's technology is new and differentiated, so the competitive landscape is limited to organizations that decide to build out their own agentic development team versus using Airrived's platform. Glean Technologies is the only competitor that we have identified that provides a similar offering, which it terms as a "work AI" platform that combines an enterprise graph, agentic reasoning engine and "universal knowledge service" that can combine internal company data with real-time internet data in support of rapid agent development and deployment.

SWOT Analysis

Strengths	Weaknesses
Airrived takes a novel approach to creating and deploying custom GenAI applications using a no-code platform and "building block" agents that can be combined into a full application. Applications can be built to run autonomously or with a human in the loop. Airrived has shown early traction, generating over $1 million in ARR over five months. The company reports a burn rate of one-third of spending; it is well-positioned to scale without additional capital in the near term.	Given that the company's approach is new and many organizations are unaware of Airrived, its biggest weakness may be "build versus buy" — organizations may already be well down the road of developing their own AI agents. That said, if the company is successful in demonstrating rapid ROI and faster time to market for custom agents, this may not be an issue given the current "land rush" to deploy AI-based solutions.
Opportunities	**Threats**
Airrived can capitalize on the explosion of interest in GenAI applications that solve real-world security and other business problems. The competitive landscape is nearly zero, with only one similar vendor, and if the company can build a significant partner channel, it could grow rapidly. If it continues gaining traction, there are also opportunities to be acquired by a larger vendor.	Larger AI-native organizations may choose to copy Airrived's technological concepts and launch their own competitive offerings, and Glean will likely emerge as a key competitor.

Source: 451 Research.