CYBERSECURITY **DIVE**

DIVE BRIEF

Agentic AI surges in financial sector even as many firms fail to manage security risks

One-fifth of firms aren't even sure if they've been hacked through their AI tools, according to a new report.

Published June 12, 2026

Eric Geller
Senior Reporter

Getty Images

Dive Brief:

- Financial services organizations are widely using AI agents for common business operations, but many of them aren't sure whether their AI tools have opened the door for hackers, according to a new report.
- Sixty-two percent of financial services firms have deployed AI agents, and 93% of those firms have given them some level of

- autonomy, the Cloud Security Alliance (CSA) said in its Tuesday report.
- The report's authors said the main conclusion from their survey, which consisted of interviews with 340 global IT and security professionals between Jan. 15 and March 1, is that "financial institutions have deployed AI faster than they have secured it."

Dive Insight:

For now, the CSA found, financial firms are mostly using AI agents for functions such as customer service (63% of survey participants cited this function), cybersecurity (47%) and fraud detection (41%). But in the future, the vast majority (85%) of organizations expect AI agents to directly facilitate payments, according to the report, even as roughly two-thirds say that function will require new technologies for authorizing legitimate activity.

"Existing payment instruments and authentication models were designed around a human being present to confirm details of the transaction," the report's authors wrote. "They were not designed for a delegated software agent that can negotiate, select, and execute purchases on a consumer's behalf."

The industry's expectations — and concerns — about agentic capabilities come as security incidents tied to AI tools become more common occurrences. One-fifth of survey respondents said their organization had experienced such an incident. And perhaps more alarmingly, 21% of respondents said they didn't even know if hackers had breached their networks through misconfigured AI tools.

When the CSA asked IT and security professionals about their biggest AI-related concerns, 61% cited data leakage, underscoring how much access AI tools have to companies' most important and sensitive records.

The report identifies seven key trends for the financial services sector, including how AI is accelerating third-party risks, the looming potential for agentic finance and global regulatory disparities and the need for new AI-centric security controls.

“The results of this year’s survey show an industry speeding toward autonomous AI-driven operations while also recognizing that visibility, identity governance, and real-time security controls must mature just as quickly,” Troy Leach, the CSA’s chief strategy officer and a lead author of the report, said in a statement.