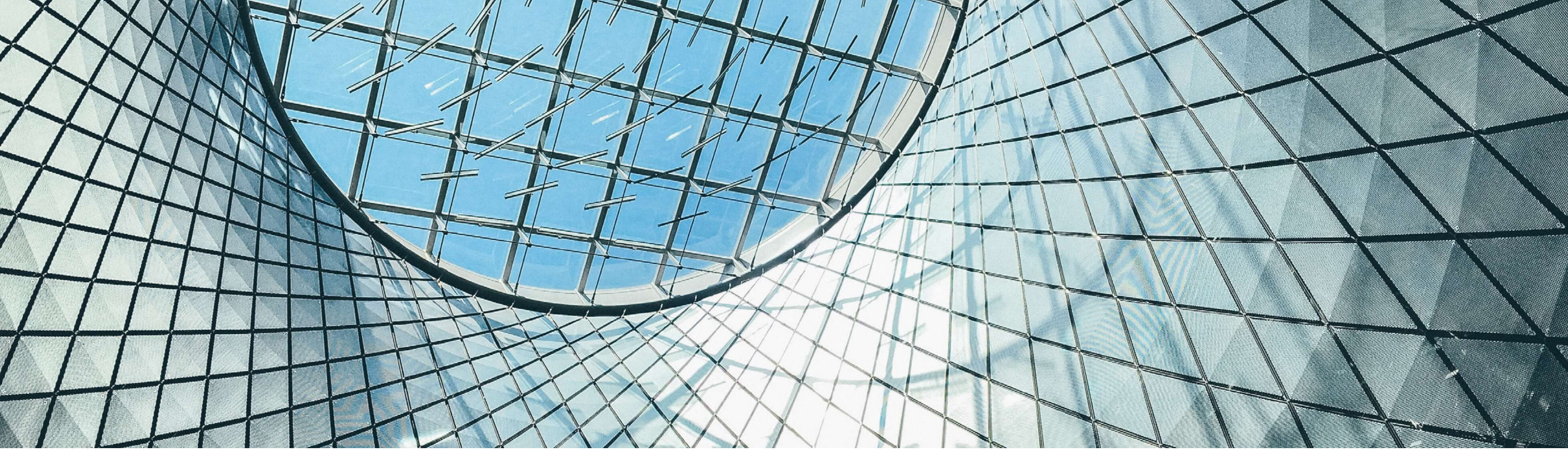


451 Research Market Insight Report Reprint

Securing the AI-driven enterprise: Cisco acquires security for AI with Robust Intelligence

August 27, 2024

by Scott Crawford

In the nearly two years since the introduction of ChatGPT, one of the first deals among major vendors for a security-for-AI startup has been announced. Cisco extends its bet on security with a greenfield opportunity that differentiates it as a first mover relative to competitors across the spectrum.

S&P Global
Market Intelligence

Introduction

Just short of two years since the introduction of ChatGPT, one of the first major vendor deals for a security-for-generative-AI target has been announced, with Cisco Systems Inc.'s agreement to acquire San Francisco-based Robust Intelligence for undisclosed terms. The deal is Cisco's first in security since the close of its multibillion-dollar acquisition of Splunk in March.

Snapshot

Acquirer	Cisco Systems Inc.
Target	Robust Intelligence
Subsector	Security for generative AI
Deal value	$350 million (451 Research estimate)
Date announced	August 26, 2024
Advisers	Perella Weinberg (Robust Intelligence)

THE TAKE

With Splunk, Cisco sought to bring on a major player in established markets in both observability and cybersecurity. With Robust Intelligence, Cisco signals its intent to take on the greenfield opportunity of security for AI with one of the first deals in the space among major vendors. Generative AI is a strategic priority for most of its major competitors, and for not a few of its major technology partners as well. With Robust Intelligence, Cisco sees its role as one of securing AI assets, leveraging its strengths in both infrastructure and security to address one of the highest current priorities among enterprise information security professionals reflected in our survey data.

Context

Deal details

While terms were not disclosed, we understand the transaction values Robust Intelligence at almost twice the post-money valuation it received in its late-2021 funding, according to S&P Capital IQ. (Subscribers to 451 Research's M&A KnowledgeBase can see our full estimate for price and revenue in the deal record.) Perella Weinberg advised Robust Intelligence in the sale.

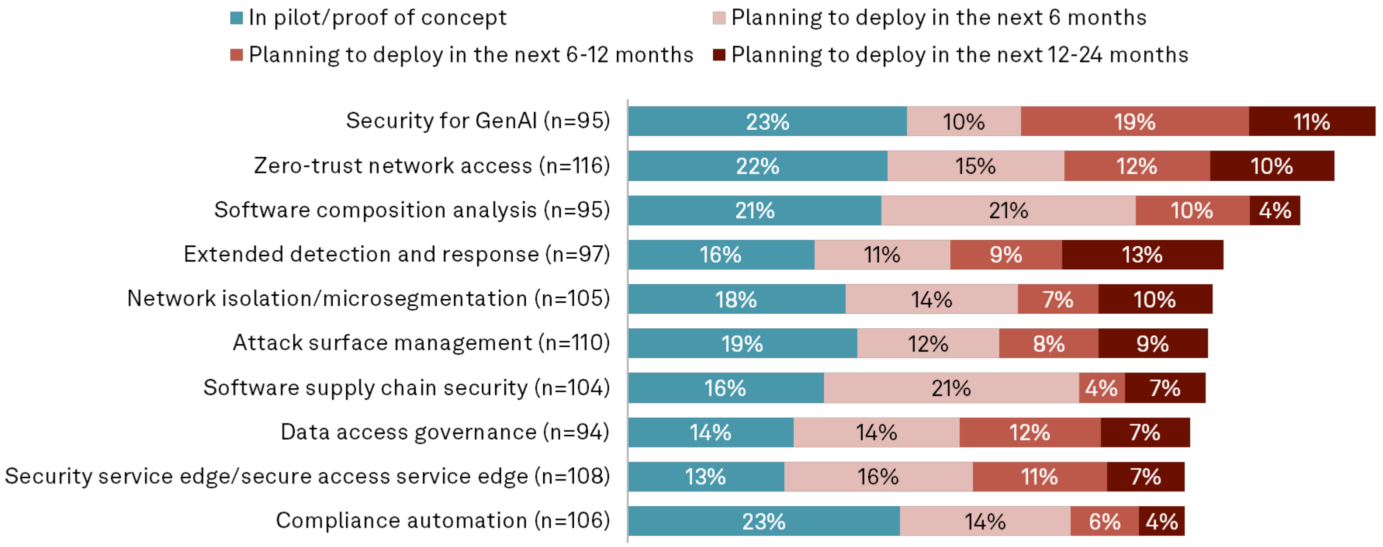
The deal comes after just five months after the close of Cisco's pickup of Splunk, and is one of the first acquisitions of a security-for-generative-AI pure play among major vendors. Most deals in this corner of the security space have so far been largely limited to consolidation deals among emerging pure plays. Protect AI alone has made three acquisitions in a little over a year to add to its security-for-AI portfolio: huntr (August 2023), Laiyer AI (January 2024) and SydeLabs (August 2024).

Deal rationale

Machine learning has long played a role in technology investment, but its impact remains dramatic as an extended investment rally fueled not least by AI's potential continues nearly two years after the emergence of generative AI. Much of this investment has been in the development of more capable models and the foundations of AI and its critical processing and infrastructure demands.

Security, however, is far from an afterthought to all this enthusiasm, at least among practitioners. In 451 Research's Voice of the Enterprise: Information Security, Technology Roadmap 2024 survey, security for generative AI was the most-often cited technology in pilot/proof of concept or plan to deploy in the next 6-24 months.

Top 10 infosec technologies in pilot/proof of concept or plan to deploy in the next 6-24 months



Q. What is your organization's status of implementation for the following information security technologies?

Base: All respondents.

Source: 451 Research's Voice of the Enterprise: Information Security Technology Roadmap 2024.

Robust Intelligence is a security-for-AI pure play that taps into this priority, giving Cisco first-mover advantage among strategic vendors in taking on this opportunity directly. Additionally, the number of providers having a good repository of prompt insertion data to test model robustness is limited, which could help give Cisco an edge beyond security alone.

Target profile

Robust Intelligence was founded in 2019 by CEO Yaron Singer, former professor of computer science and applied mathematics, and machine-learning researcher Kojin Oshiba; the pair first collaborated at Harvard. Launched in 2021, the Robust Intelligence platform emphasizes functionality for AI validation and protection. Its AI Validation capability offers automated model and data pipeline checks that incorporate stress testing features, a process that Robust Intelligence refers to as "algorithmic red teaming." Outcomes of evaluation provides recommendations for protection of models in production, which the company offers through its AI Protection functionality centered on its AI Firewall offering that provides guardrails against issues identified through AI Validation.

Robust Intelligence has raised roughly $53 million in four rounds of funding, most recently in a $30 million series B round led by Tiger Global in 2021 with participation from existing investors Sequoia Capital, Harpoon and Engineering Capital.

Acquirer profile

Cisco Systems has long been not only an avid cybersecurity acquirer but a record-setter for its security acquisitions, with two among the largest ever at the time. While Duo Security scored big in 2018 with its $2.3 billion price tag, Splunk was an order of magnitude greater. Prior to Splunk, Cisco had made 33 security deals for a total value of $9.21 billion according to 451 Research's M&A KnowledgeBase. Although not exclusively a cybersecurity player (it has a substantial stake in observability and other fields), Splunk was three times larger than Cisco's prior security deal values combined.

Robust Intelligence extends this priority in a new direction for the cybersecurity market. The deal supports Cisco's AI strategy across its portfolio, including a $1 billion global investment fund announced in June to "expand and develop secure, reliable and trustworthy AI solutions," according to a company press release.

Competition

Startups tackling the generative AI security, risk and governance opportunity emerged nearly as soon as generative AI itself became widely known. In addition to Robust Intelligence, examples include Aporia, the Arthur Shield functionality of Arthur AI, Bosch Global Software Technologies' AIShield, Calypso AI, HiddenLayer (the winner of the 2023 RSA Conference Innovation Sandbox competition), Mithril Security, Protect AI and TrojAI. Vendors emphasizing protection for data used in generative AI range from the offerings of major strategic vendors to startups such as Protopia AI. AI governance and observability players emphasizing cyber risk include Credo AI, Fairly, ModelOp, Monitaur, Saidot and WhyLabs.

Cisco's major competitors — in security as well as more broadly — are also often among AI's largest investors. In their security portfolios, however, generative AI most often appears as "AI for security" in the form of copilots and generative AI-enhanced automation. With Robust Intelligence, Cisco has departed from these competitors and staked out a claim to the other side of the intersection of security and AI that aligns with its role in infrastructure. At the moment, a "security for AI" play is differentiating among strategies. Given the sheer number of potential acquisition targets in this active space, however, it is not likely to remain so for long.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.