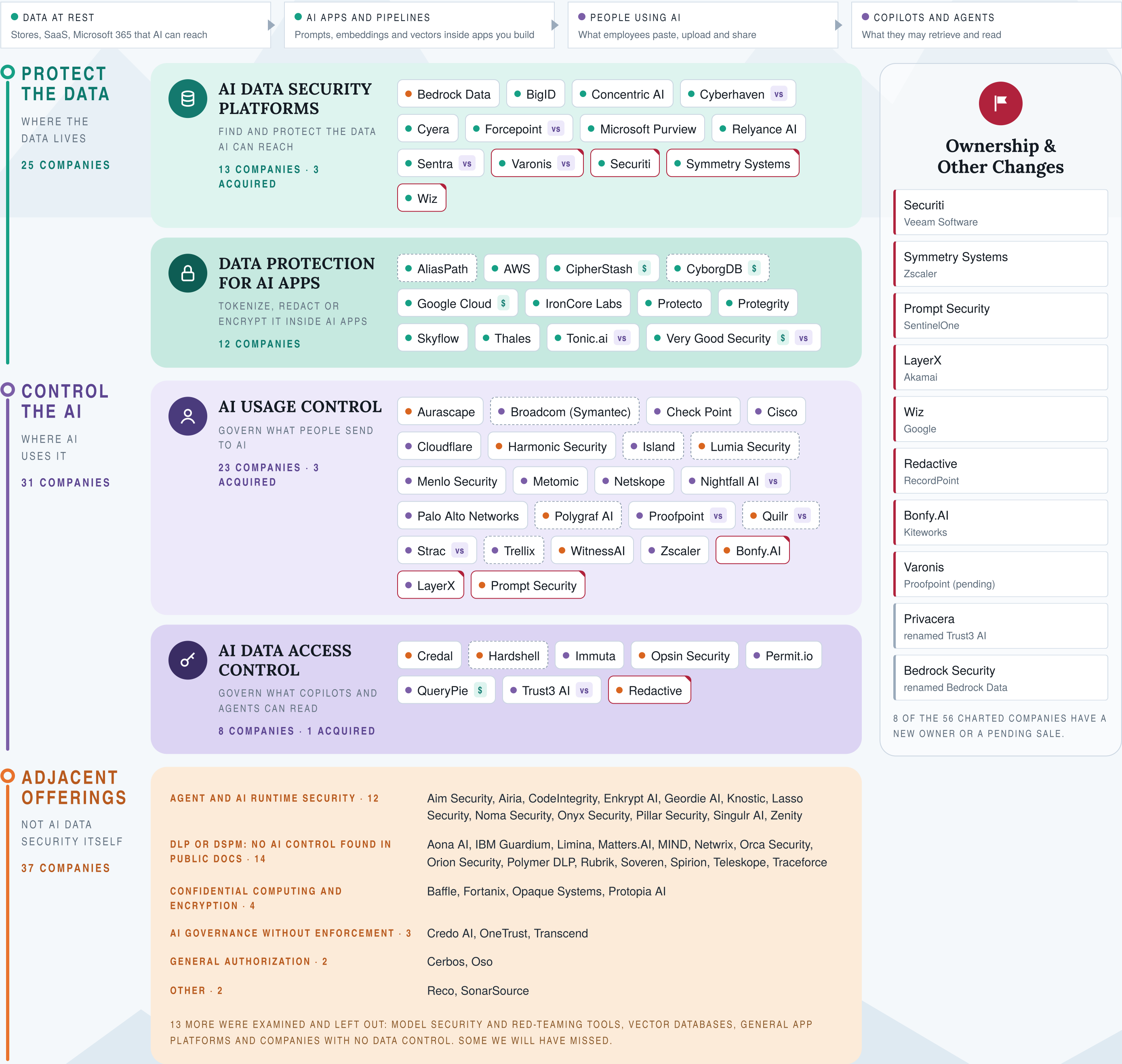


AI Data Security Market Map

New market, or new label?

106 EXAMINED → 56 CHARTED → 37 ADJACENT → 13 OUTSIDE | A PRODUCT WITH A DOCUMENTED CONTROL FOR DATA USED BY AI | OCTOBER 2026

38 OF 49 ACTIVE VENDORS PREDATE GENAI OR ARE BROAD PLATFORMS (10 AI-NATIVE, 1 UNKNOWN) | 22 OF 26 OLDER SPECIALISTS NOW LEAD WITH AI



AI Data Security Market Map

/ WHO IS BUYING AND WHO IS BUILDING · OCTOBER 2026

Who else is buying data security startups? (Hint: check your backup vendor.)

15 of the 17 AI runtime, red-teaming and agent security startups sold since 2023 went to network, endpoint and data security vendors. Data security targets split differently. Backup, cloud, content and data platforms took 8 of 20, more than any single security segment: Veeam bought Securiti, Rubrik bought Laminar, Databricks bought Antimatter and Google bought Wiz. The largest deal still went to a security vendor: Proofpoint's pending \$6.3B offer for Varonis.

8 of 20

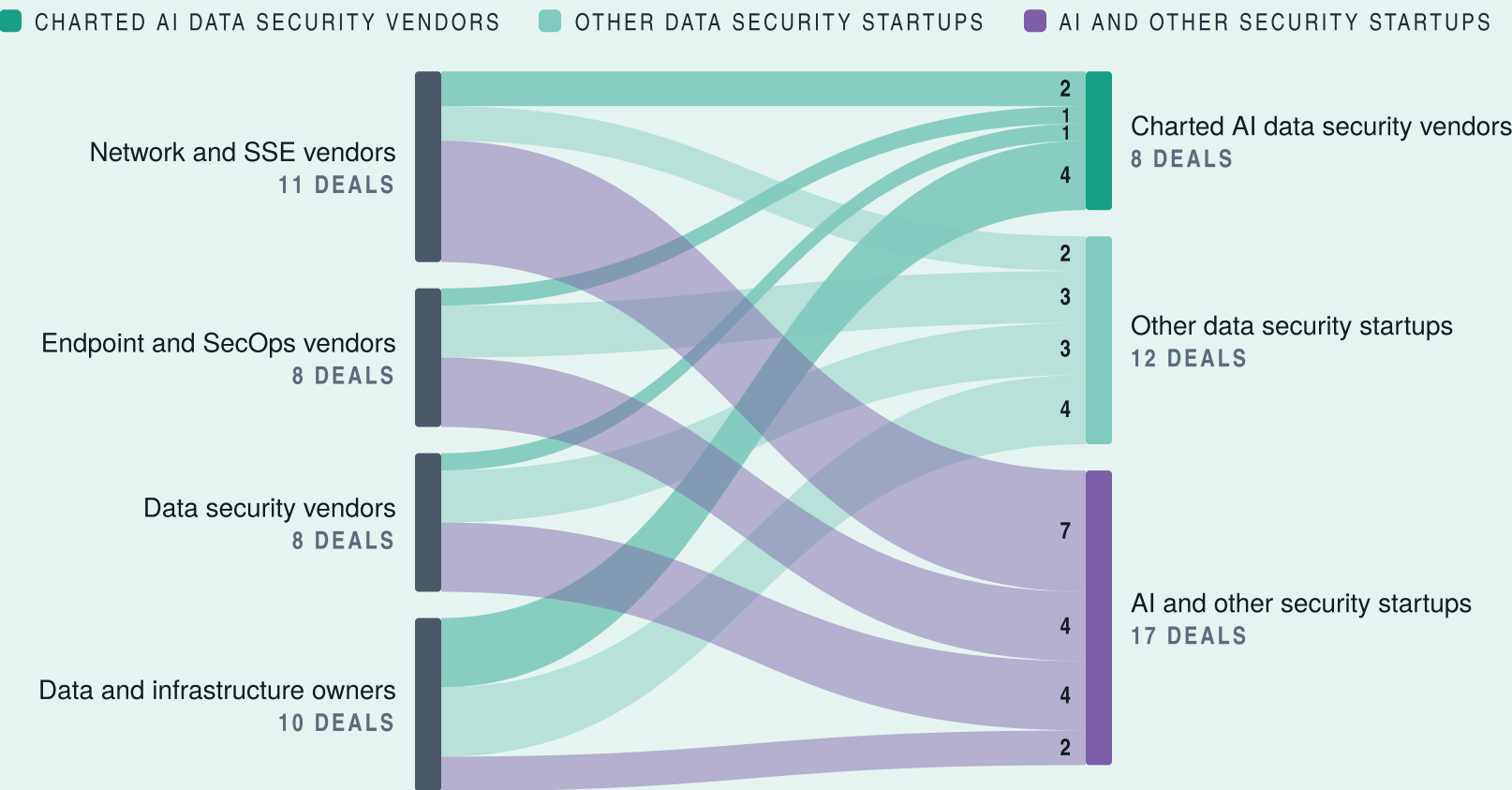
DATA SECURITY TARGETS BOUGHT BY DATA OWNERS

N = 37 DEALS ANNOUNCED 2023 TO OCTOBER 2026, INCLUDING 2 PENDING · 20 DATA SECURITY TARGETS + 17 AI AND OTHER SECURITY TARGETS



Who bought what

ACQUIRER TYPE TO TARGET TYPE · N = 37 DEALS, COMPLETE

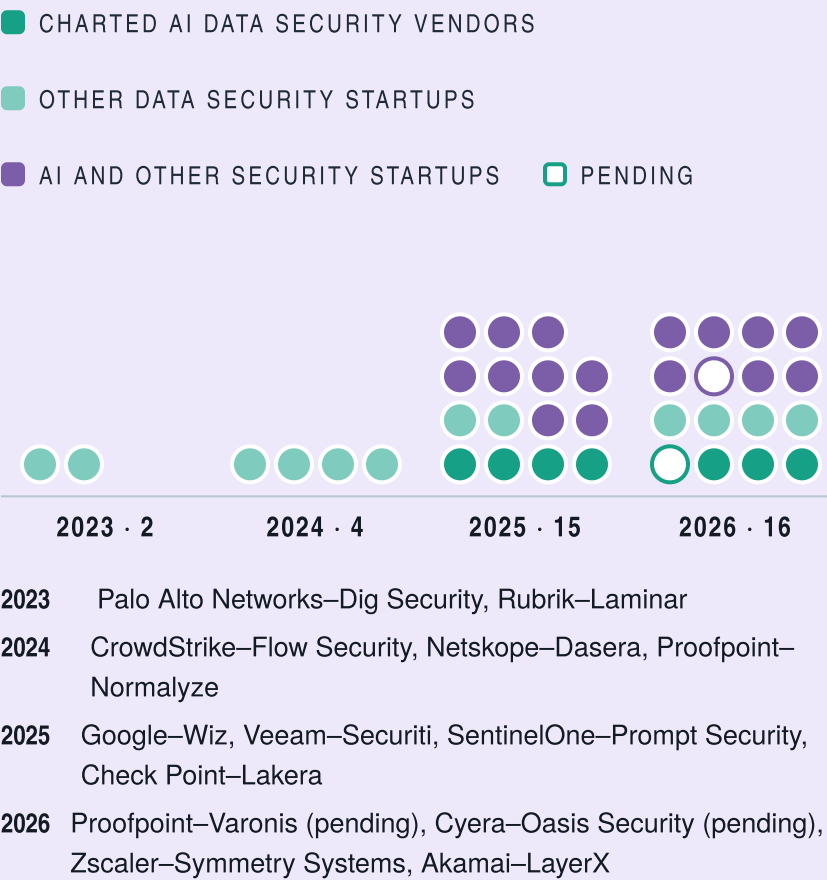


Data owners made 10 deals, and 8 of them were data security companies.



The pace picked up

DEALS BY YEAR ANNOUNCED · N = 37, COMPLETE



31 of the 37 deals were announced in 2025 and 2026.

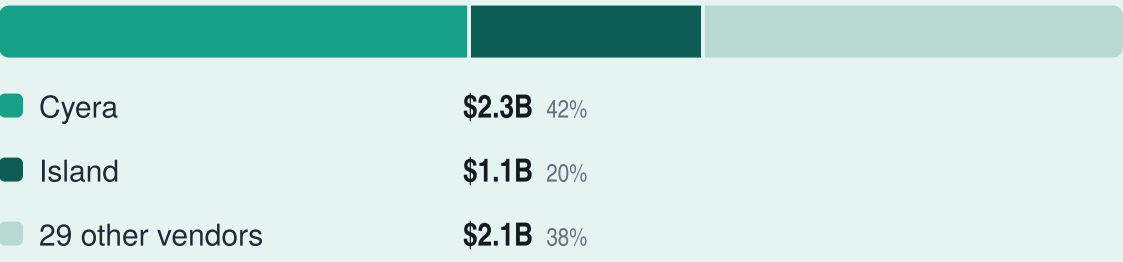


Two companies hold most of the money

DISCLOSED COMPANY-WIDE VENTURE FUNDING, ACTIVE CHARTED VENDORS · N = 31 OF 49 · 18 ARE PUBLIC OR DISCLOSE NONE

62%

OF \$5.5B RAISED WENT TO CYERA AND ISLAND



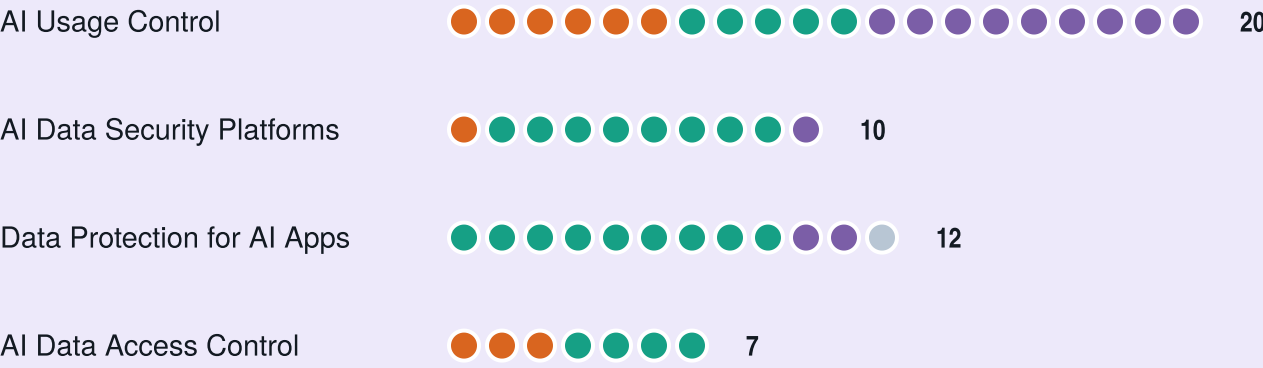
Whole-company funding, not AI-specific. Totals as stated by each company or summed from announced rounds; Island's total varies by source (\$1.1B to \$1.2B).



Who builds each category

ONE DOT PER VENDOR · N = 49 ACTIVE, COMPLETE · 7 ACQUIRED NOT SHOWN

AI-NATIVE, FOUNDED 2022 OR LATER · 10 FOUNDED EARLIER · 26
BROAD SECURITY OR CLOUD PLATFORM · 12 UNKNOWN · 1



AI-native startups sit mostly in usage control. Data protection for AI apps has none: tokenization and encryption vendors and the hyperscalers built it.

AI Data Security Market Map

/ WHAT THE MARKET SAYS ABOUT ITSELF · OCTOBER 2026

44 names for one market. Which one goes in your RFP?

Vendors protecting data used by AI have not agreed on what to call it. The same control is sold as a data security platform, AI DLP, AI usage control, AI security posture, a secure browser and agent security. A buyer comparing them meets 44 different labels; we grouped them into 9 families, and this map adds its own four category names. Gartner's Market Overview for AI Usage Control (August 2026) is the closest thing to a shared name; Harmonic Security is the one vendor we found citing it.

44

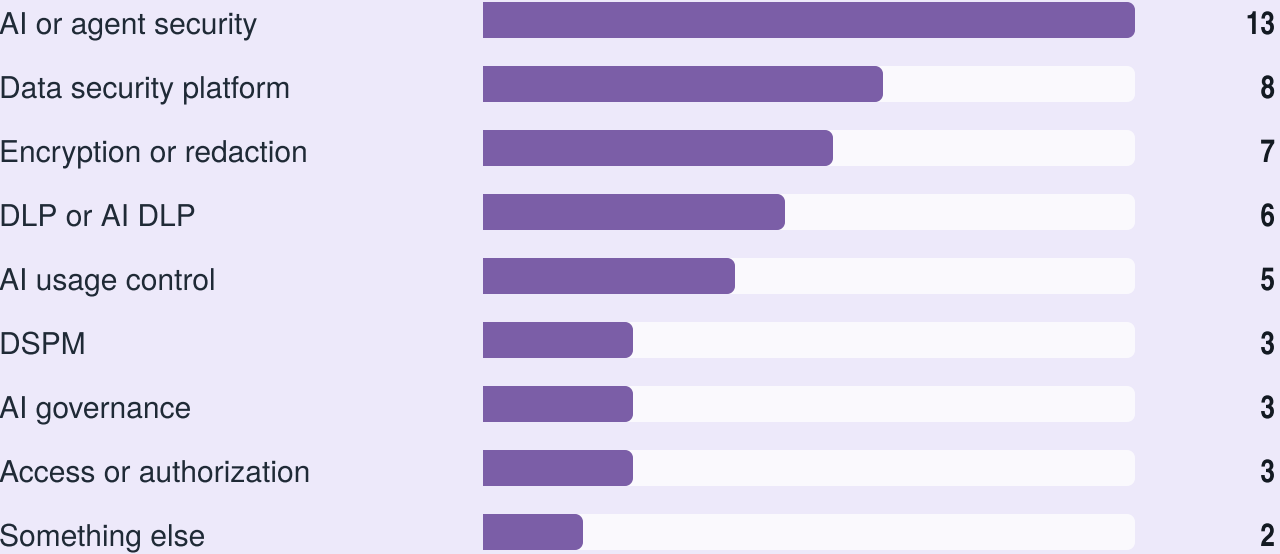
DIFFERENT CATEGORY LABELS

N = 50 CHARTED VENDORS · 6 NOT CAPTURED (5 ACQUIRED, 1 SITE BLOCKED) · EACH VENDOR'S OWN LABEL, READ FROM ITS HOMEPAGE AND PRODUCT PAGE



What vendors call the category

LABELS GROUPED BY FAMILY · N = 50 · 6 NOT CAPTURED

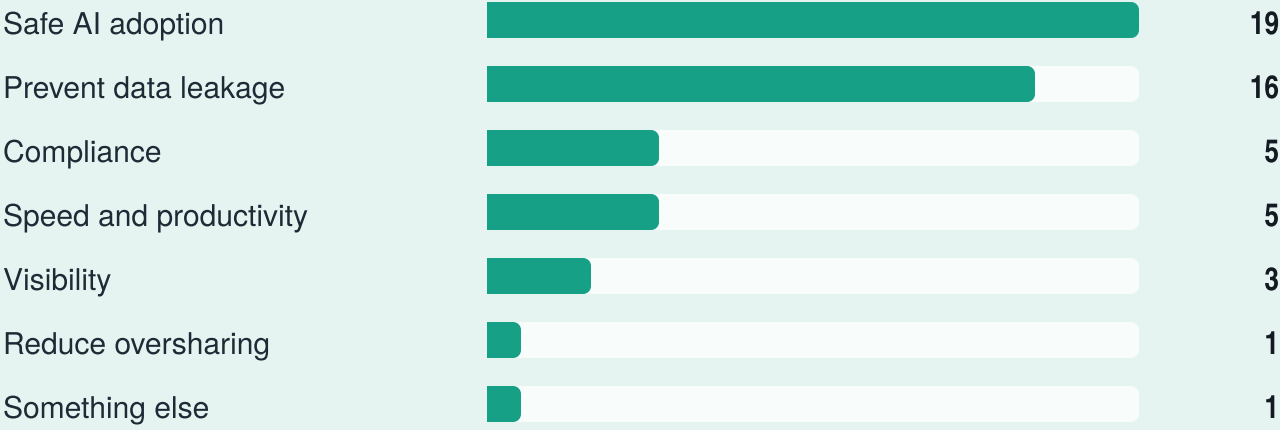


The largest family, about a quarter of vendors, calls it AI or agent security rather than data security.



The outcome they lead with

PROMISE ON THE ENTRY PAGE · N = 50 · 6 NOT CAPTURED

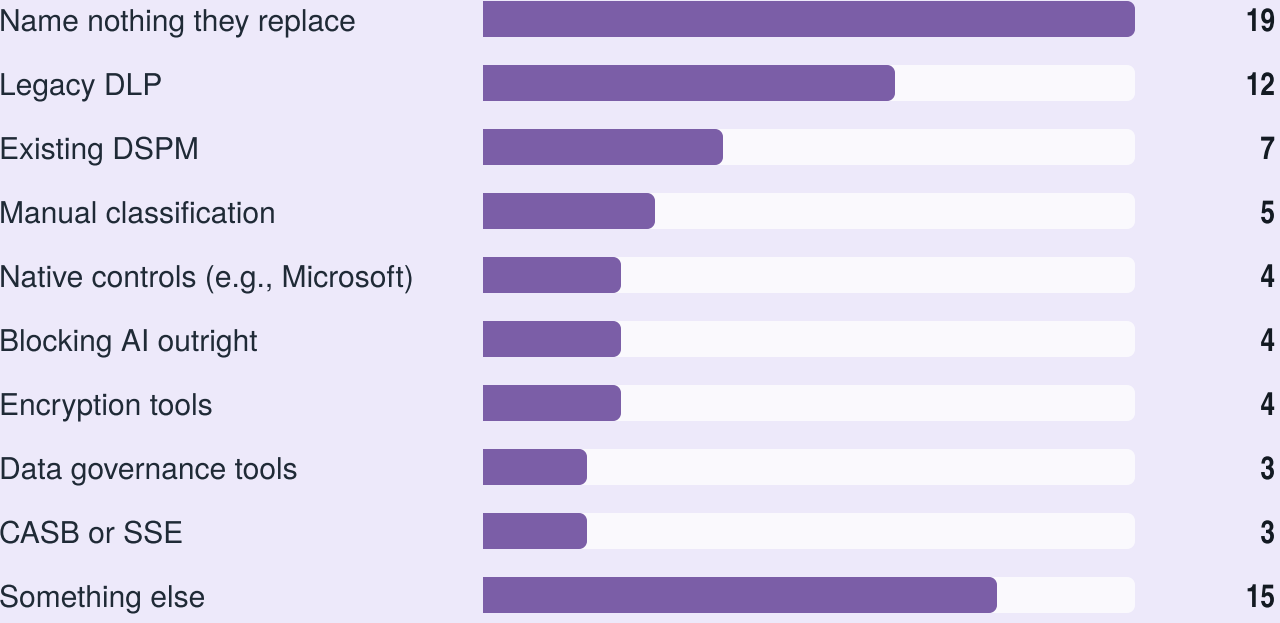


Lead messages split between enabling AI (19) and stopping leaks (16).



What they promise to replace

N = 50 · 6 NOT CAPTURED · A VENDOR CAN NAME SEVERAL

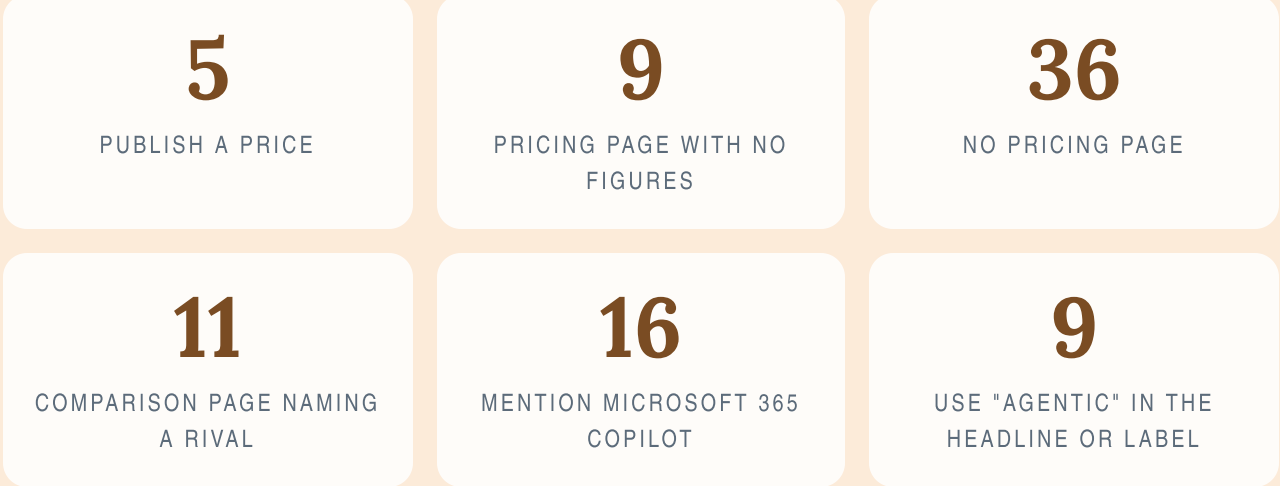


Legacy DLP is the most named target. More vendors name nothing at all.



Only 10% publish a real price

AN ACTUAL FIGURE, NOT A PRICING PAGE · N = 50 · 6 NOT CAPTURED



The vendors that publish a price: QueryPie, CipherStash, CyborgDB, Google Cloud and Very Good Security.

The author's read: what it means for go-to-market

Usage control is crowded with suites. 9 of the 20 active vendors are broad security platforms buyers already own. Independents win on depth the suites skip: data lineage, endpoint coverage, agent and MCP traffic.

Data protection for AI apps sells to engineering. No vendor founded since 2022 is in it yet. Developer documentation, transparent pricing and integrations matter more than CISO messaging.

Buyers: write the RFP around controls, not category names. Ask which data each product protects, where it enforces and what it blocks. The labels will not tell you.

Name the problem buyers search for. With 44 labels in play, a category name buyers already recognize is an advantage most vendors are leaving unused.