

Survey

Security Is the Gate on Enterprise AI

Greycroft

Contents

01	Executive Summary	3
02	What Is Holding Back AI Deployment	4
03	AI Threats and Which AI Tools Work	7
04	Which Categories Are Open to New Vendors	11
05	Who Captures AI Security Spend	16
06	How Startups Win and Lose Deals	20
07	Who We Surveyed	22

Executive Summary

The Hugging Face breach made the risk real. In July, an autonomous AI agent system breached Hugging Face through its data pipeline, weeks after frontier labs warned their models could attack weakly defended systems. We asked CISOs what now stands between them and shipping AI.

Security is now a condition for deploying AI. Most leaders have seen AI projects stall or die over security. They are funding the fix with new money, and that budget often sits outside the security organization.

Foundation models alone will not close the gap. Buyers need a control plane around the model: enforcement before a prompt, a record of what was approved, and agent permissions across providers. No model vendor can provide that on behalf of its competitors.

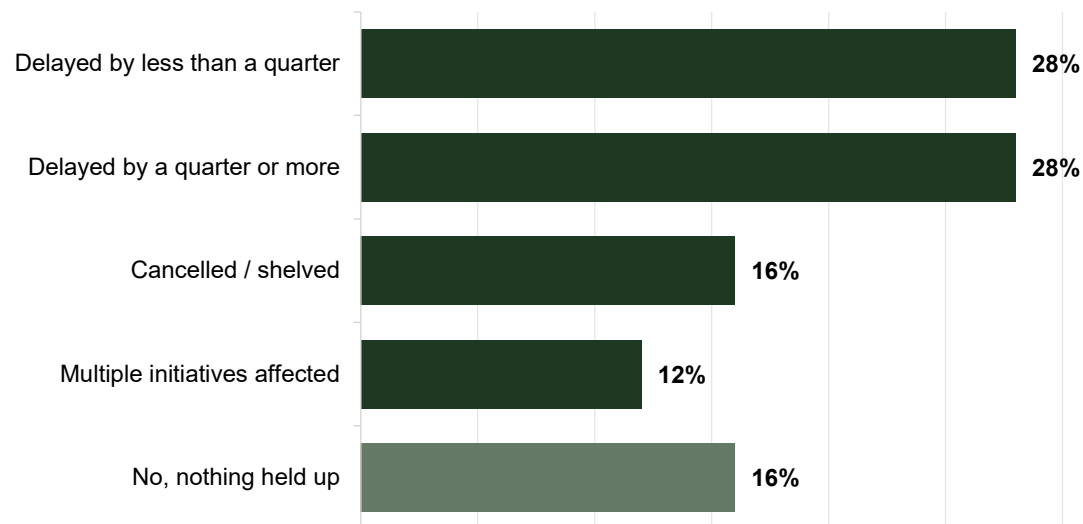
Incumbents win on distribution, but the door is open. Few buyers wait for an existing vendor to catch up. They buy startups that are materially better, deploy without moving customer data, and fill a gap rather than overlap current spend.

The opportunity is to build the reason an AI project ships. We see openings in offensive security, agent containment on the endpoint, AI governance, non-human identity and the AI-native SOC.

What Is Holding Back AI Deployment

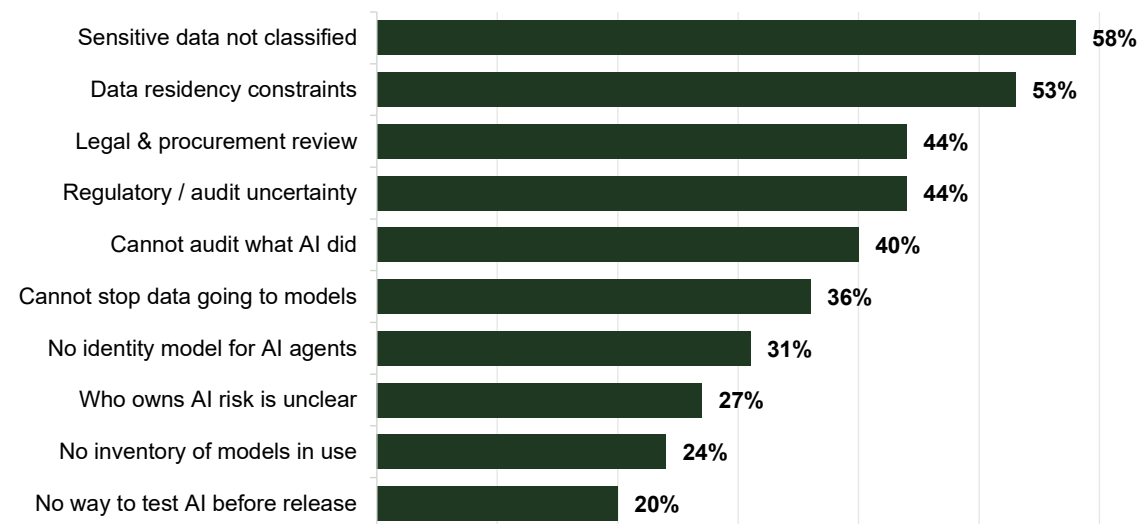
Security Is Gating AI Deployment

AI Initiative Delayed, Blocked or Cancelled (N = 50)



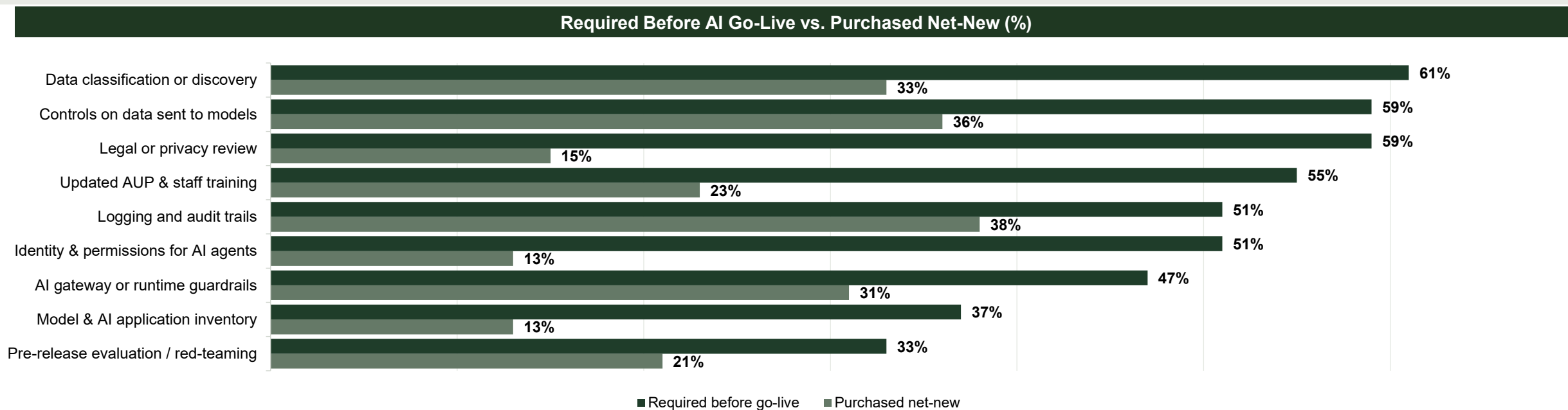
- **Security concerns now stall or kill most enterprise AI projects**
- 84% have had an AI initiative delayed, blocked or cancelled over security, governance or data-protection concerns; 44% were delayed a quarter or more, or cancelled

What Is Slowing AI Deployment (N = 45, up to 3)



- **Data and compliance gaps, not agent security, are what hold AI deployments back**
- Unclassified sensitive data (58%) and data residency (53%) lead, ahead of legal review and regulatory uncertainty (44% each); agent identity, model inventory and pre-release testing rank lowest

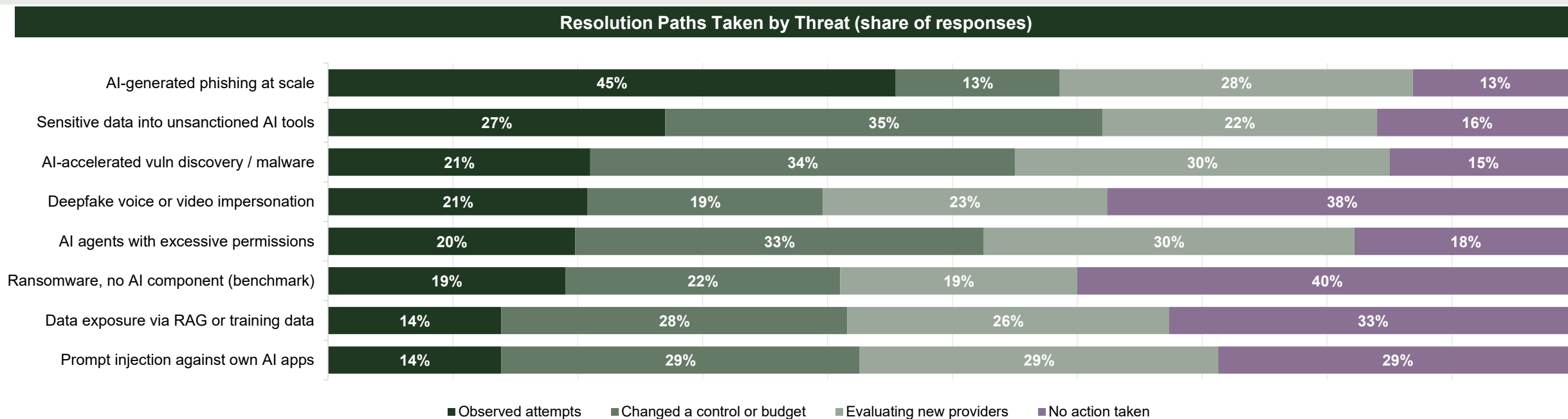
Requirement Does Not Necessarily Drive Purchase



- **Enterprises buy new tools for AI audit and data controls, but cover agent identity with the IAM they already own**
- The wider the gap between the bars, the more likely existing tooling covers the need rather than a net-new purchase
- Logging and audit trails convert best: 75% of those who required them bought something new
- Agent identity has the widest gap, required by 51% but newly purchased by 13%; we expect it to convert as agents in production multiply

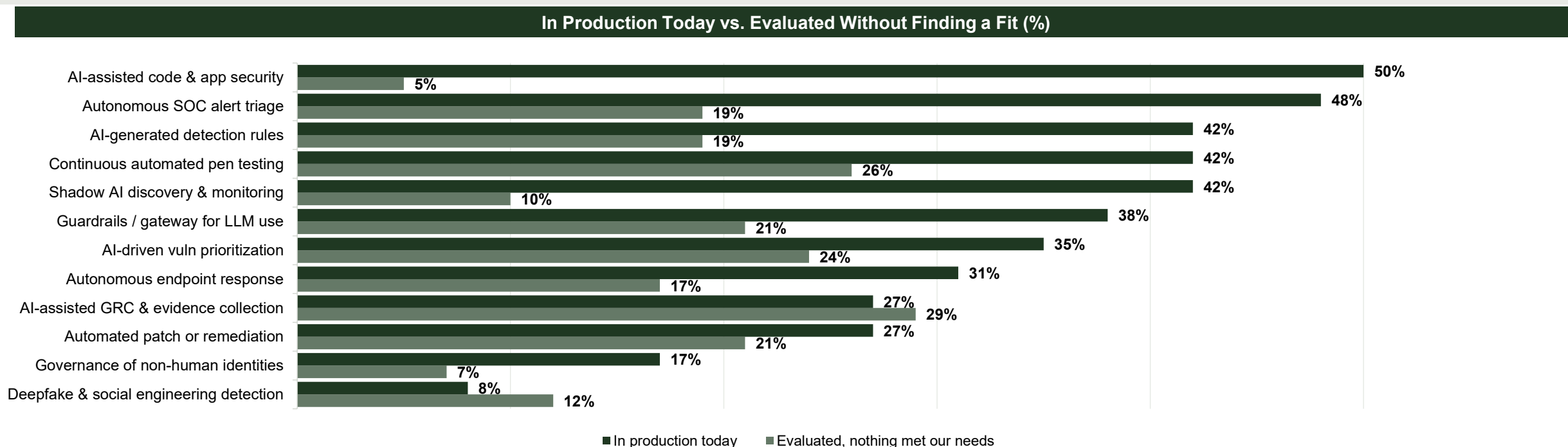
AI Threats and Which AI Tools Work

Buyers Vary Resolution Paths Depending on Threat



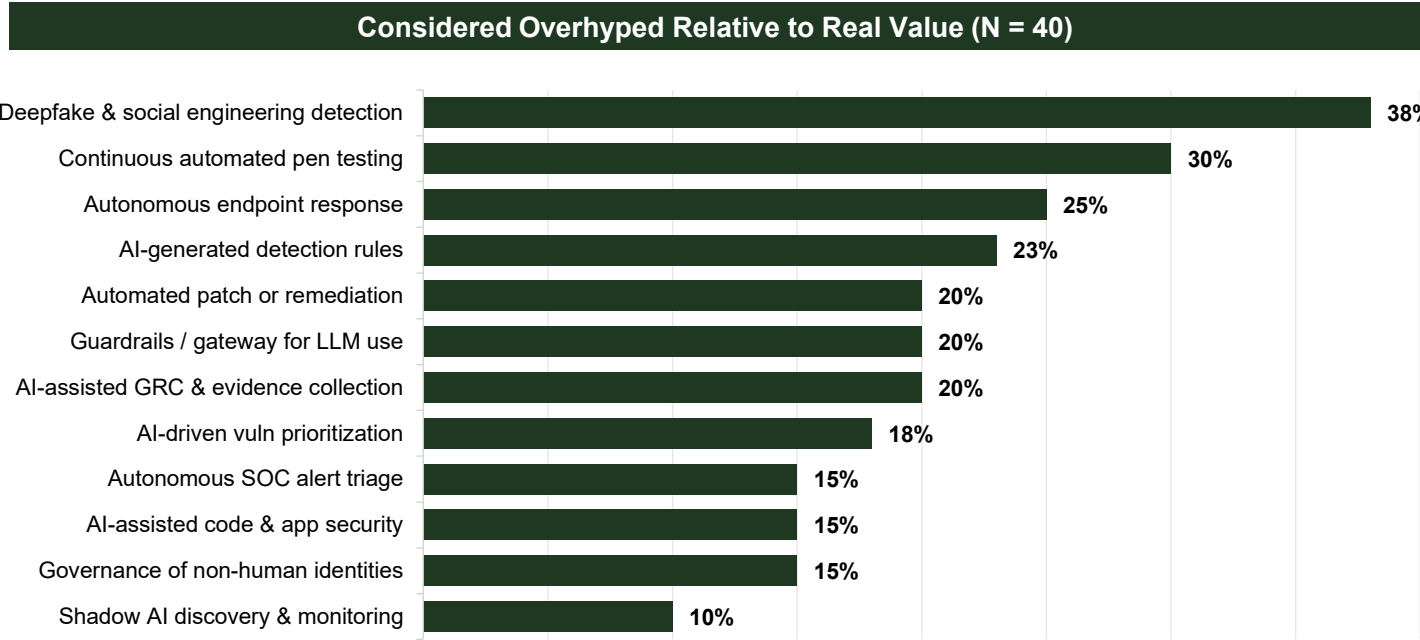
- **Enterprises are changing controls for the AI threats they expect, not the ones they see most often**
- AI-generated phishing is observed most but changes least, as existing email security absorbs it; deepfake impersonation and ransomware show the highest inaction
- AI-accelerated exploit development and agent permission abuse drove more control changes and vendor shopping, despite being observed less often

Deployed vs. Evaluated with No Fit

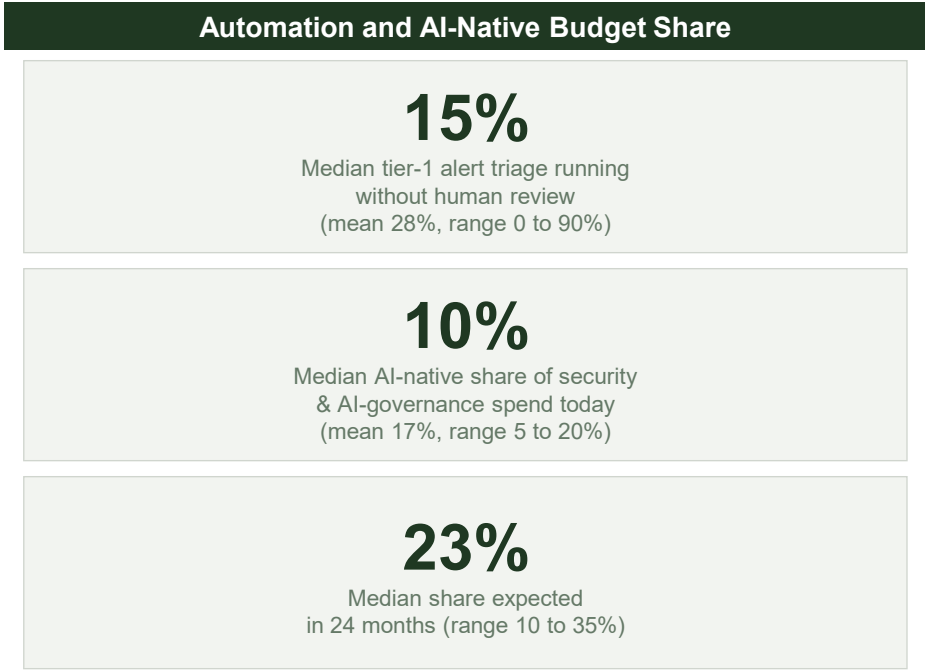


- **AI for code security is widely adopted, while AI for GRC and pen testing is most often tried and rejected**
- AI-assisted code security is the most deployed (50%) and least unserved (5%)
- AI-assisted GRC leads failed evaluations at 29% against 27% deployed; continuous pen testing (26%) and vulnerability prioritization (24%) follow

What Buyers Call Overhyped



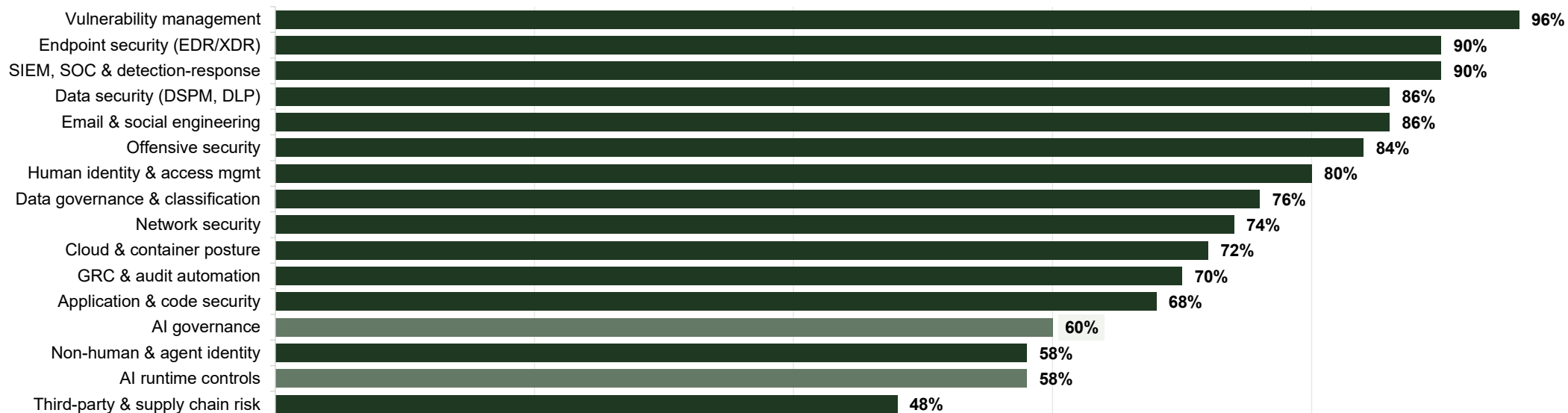
- Buyers see deepfake detection as the most overhyped AI security product, while categories that are at direct threat from AI are more appreciated



Which Categories Are Open to New Vendors

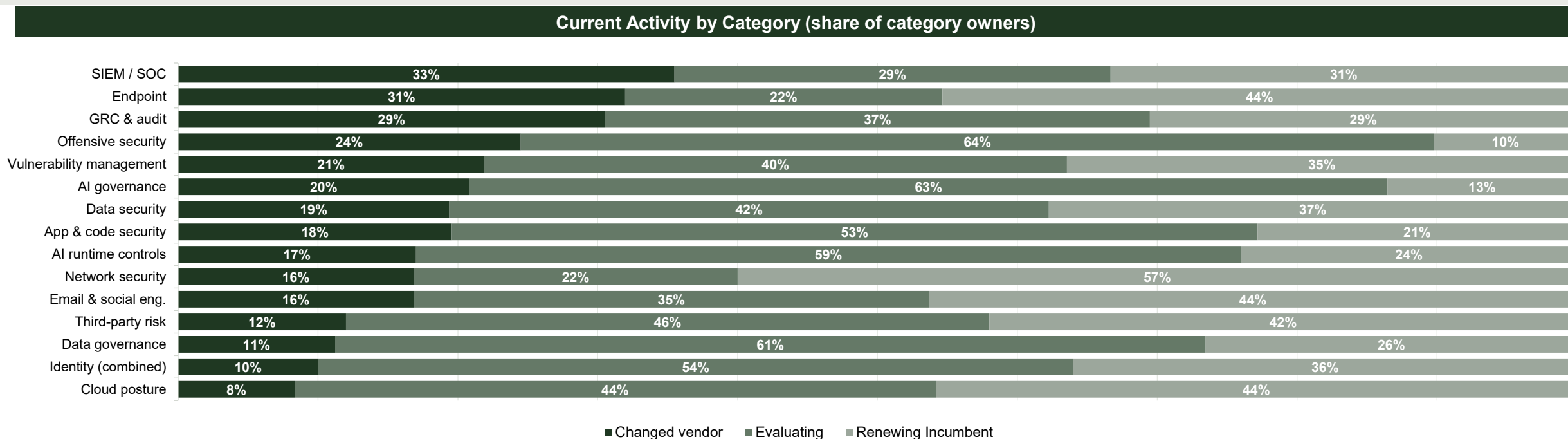
Where Security Leaders Hold the Budget

Areas Where the Respondent Holds Budget Responsibility (N = 50)



- **Security leaders hold budget for traditional security categories, but often not for AI-specific tools**
- Budget responsibility is near-universal in traditional categories: vulnerability management 96%, endpoint and SIEM/SOC 90% each
- It drops to 60% for AI governance and 58% for AI runtime controls and non-human identity, so in about four in ten AI-native deals the security leader cannot sign alone

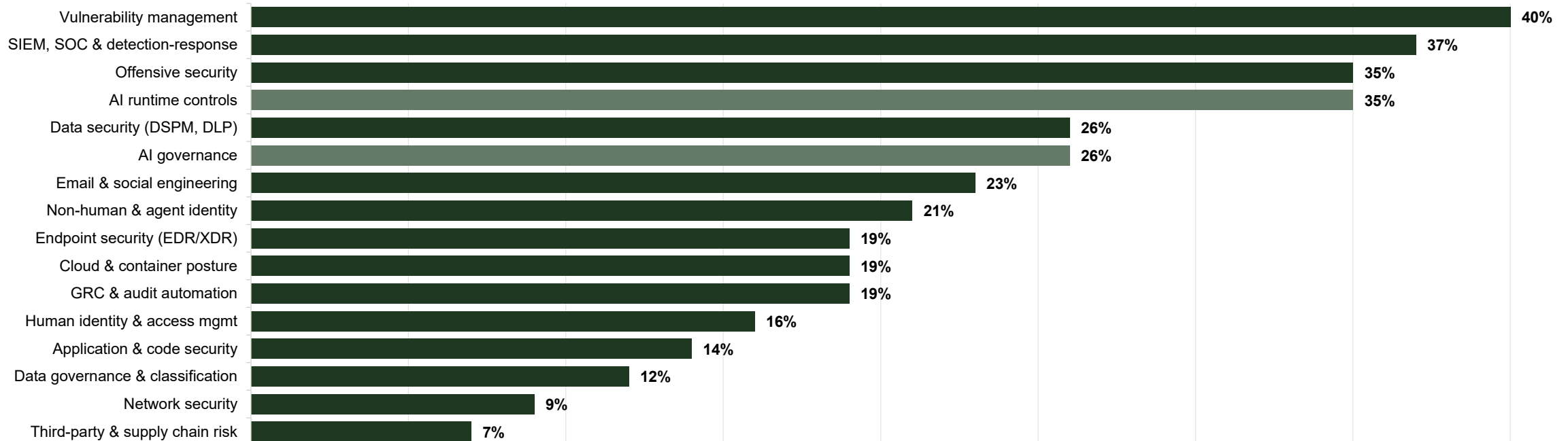
Buyer Appetite For Change by Category



- **Buyers are evaluating alternatives in most security categories**
- Offensive security and AI governance are the most open: 64% and 63% evaluating, only 10% and 13% renewing
- Network security is the most locked in: 57% renew the incumbent and only 22% are evaluating
- Switching has been highest in SIEM/SOC (33%), endpoint (31%) and GRC (29%)

Where AI-Native Vendors Are Actually in the Room

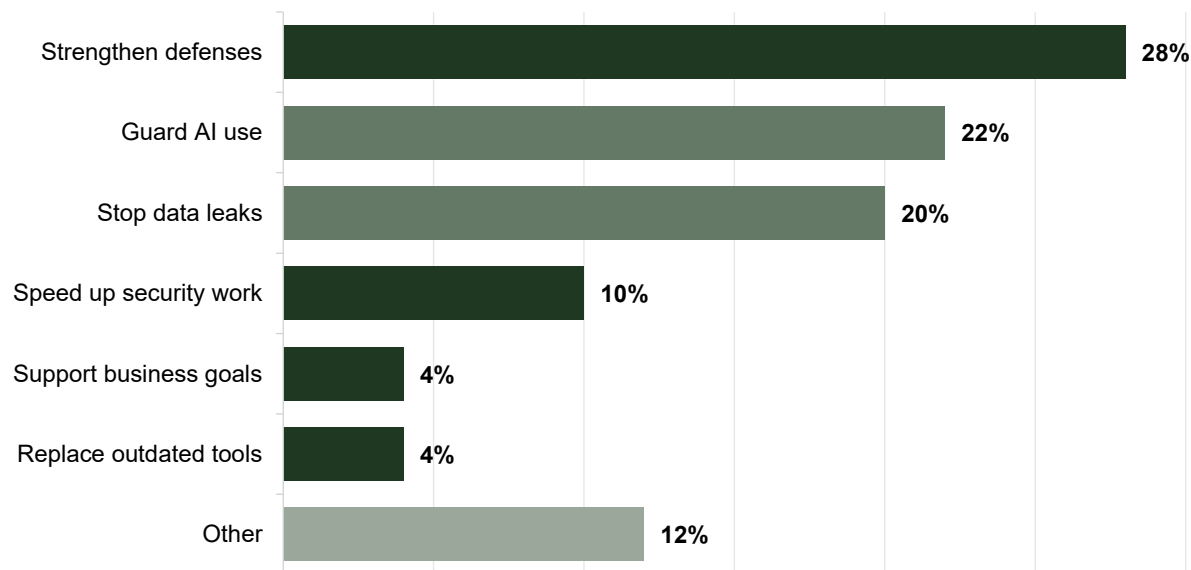
AI-Native Vendor in an Active Evaluation, POC or Shortlist (N = 43)



- **Buyers most often evaluate AI-native vendors to fix long-standing security operations problems**
- Vulnerability management leads at 40%, followed by SIEM/SOC at 37%, with offensive security and AI runtime controls at 35% each

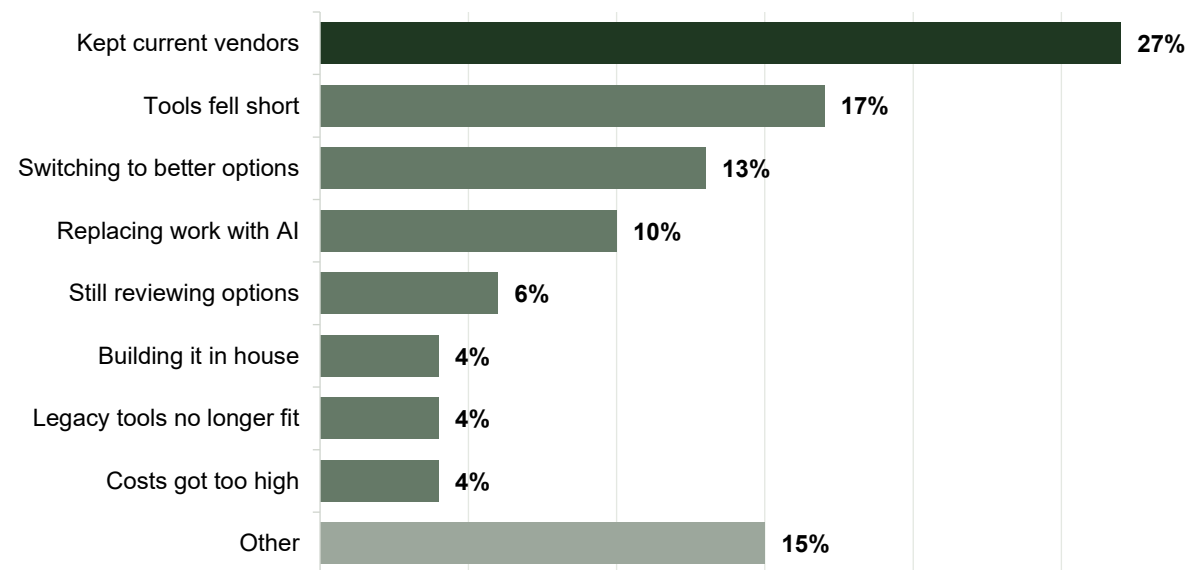
What Gets Bought, and What Gets Dropped

Trigger for Most Recent Purchase (N = 50)



- **Securing AI use is now a leading trigger for new security purchases**
- Strengthening defenses triggered 28% of recent purchases, but guarding AI use (22%) and stopping data leaks (20%) together account for roughly four in ten

Reason for Removal or Non-Renewal (N = 48)

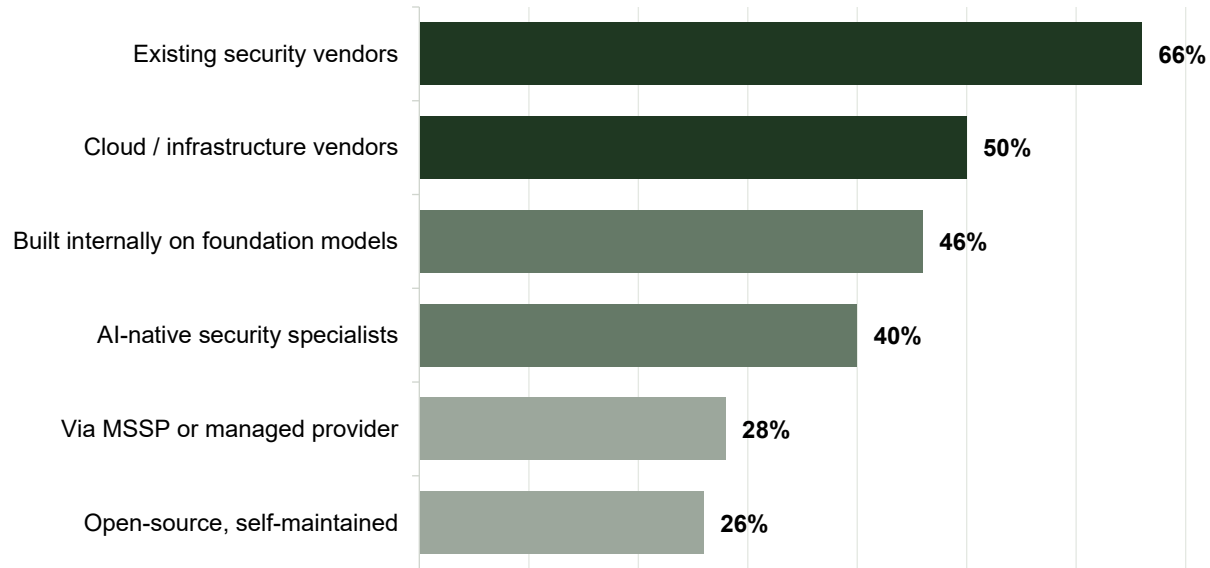


- **Enterprises rarely drop a security vendor unless it falls short or a clearly better option appears**
- 27% kept all current vendors; churn came from tools falling short (17%) or better options (13%), and 10% replaced work with AI

Who Captures AI Security Spend

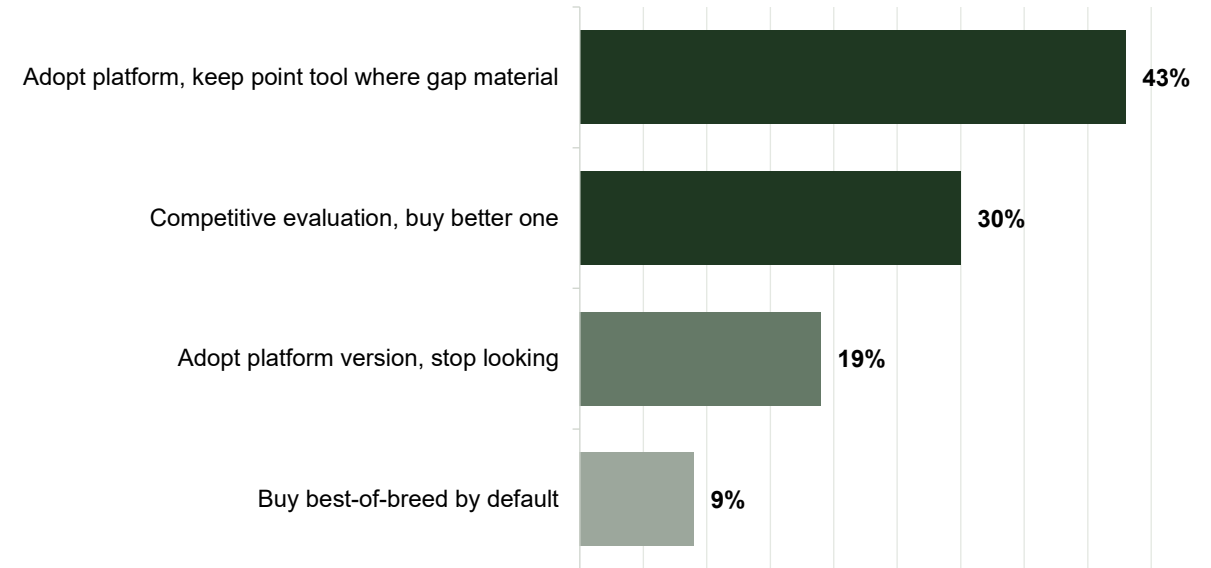
Incumbents Lead on Distribution, Not Preference

Where Deployed AI Capability Came From (N = 50)



- **Enterprises get AI security capabilities mostly from vendors they already use**
- Existing security vendors supply 66% of respondents and cloud or infrastructure vendors 50%; AI-native specialists rank fourth, behind internal builds on foundation models

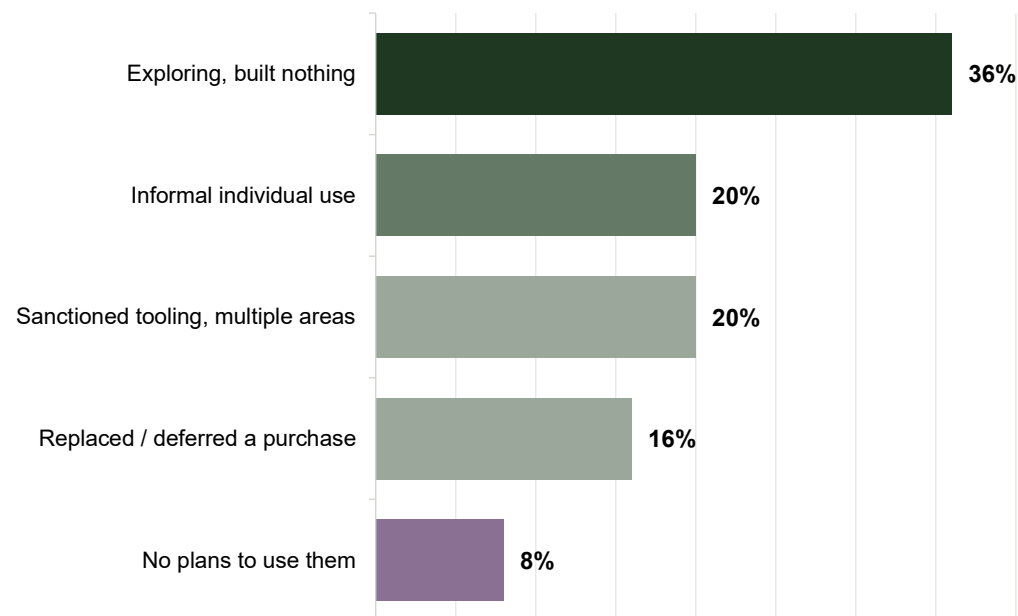
Response When a Platform Ships "Good Enough" (N = 47)



- **A new product only displaces a platform's built-in feature when it is materially better**
- Only 19% adopt a platform's adequate capability and stop looking; 81% keep a point tool, run a competitive evaluation or buy best-of-breed

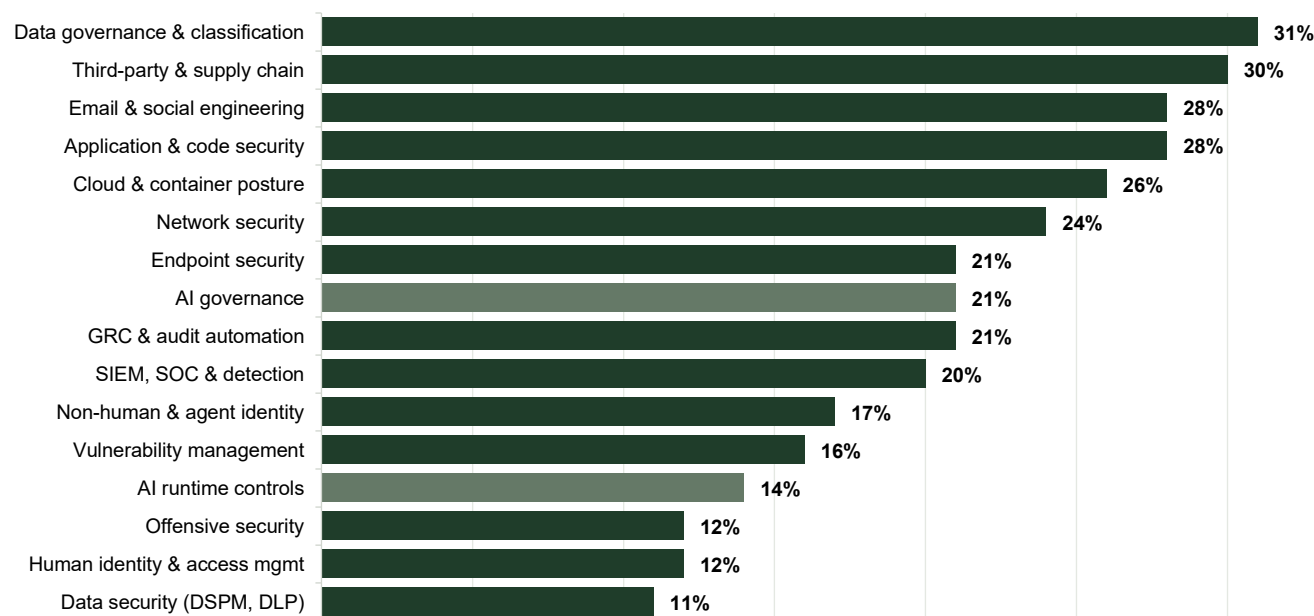
Foundation Models: Build Activity and Substitution Risk

Use of Foundation Models for Security Work (N = 50)



- Some enterprises are building security tooling on foundation models instead of buying it
- 20% have built sanctioned internal tooling, and 16% say it replaced or deferred a commercial purchase

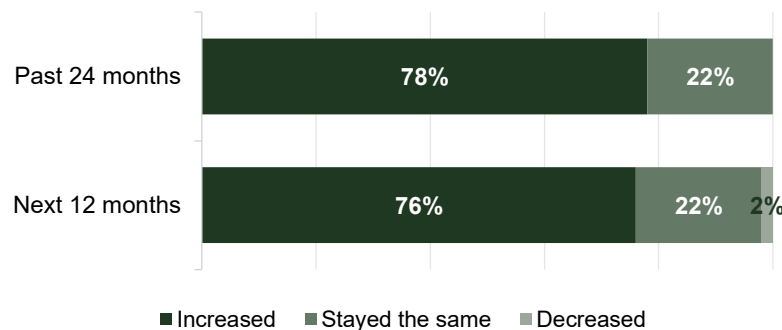
Share Saying a Foundation Model Could Handle It Alone



- Buyers don't expect foundation models to entirely replace security specialists in any category
- No category came close to a majority; buyers need a control plane around the model that no single model vendor can supply

Budgets Are Growing and the AI Share Is Compounding

Direction of Cybersecurity Budget (N = 50)



+15%

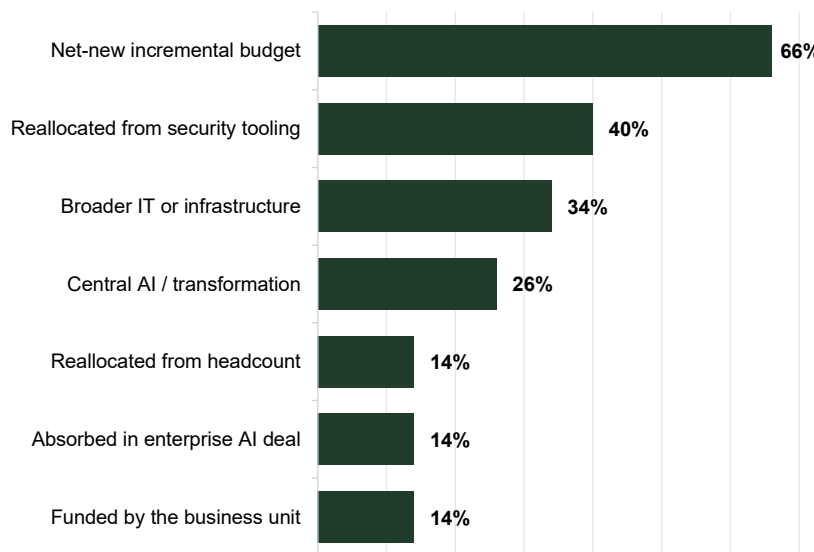
Median change,
past 24 months

+10%

Median expected,
next 12 months

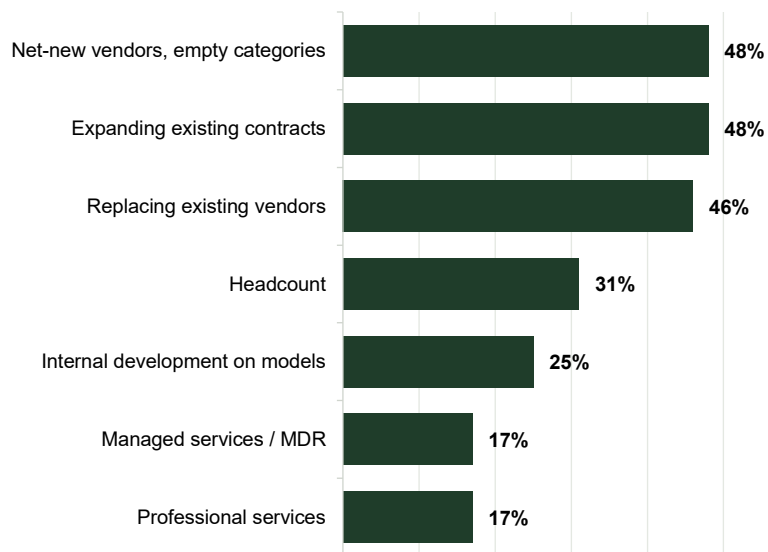
- Security budgets are growing, and no respondent reported a cut
- 78% grew budgets over the past 24 months (median +15%), and 76% expect further growth (median +10%)

How AI-Related Spend Is Funded (N = 50)



- AI security is mostly funded with new money rather than taken from existing security lines
- 66% secured net-new incremental budget; 40% also reallocated from existing security tooling

Where Incremental Dollars Go (N = 48)

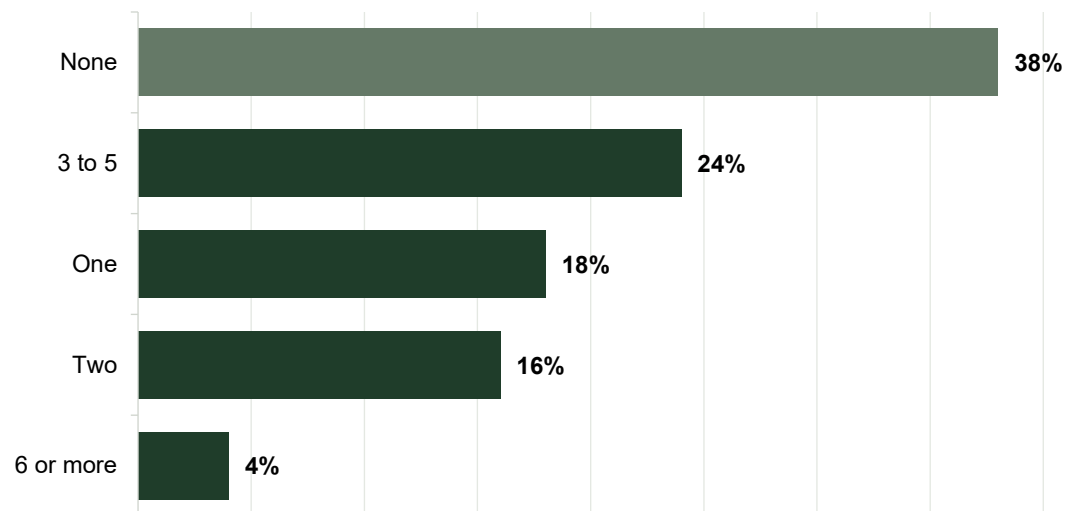


- New security dollars are flowing to categories with no incumbent vendor
- 48% direct incremental dollars to net-new vendors in empty categories, as many as expand existing contracts

How Startups Win and Lose Deals

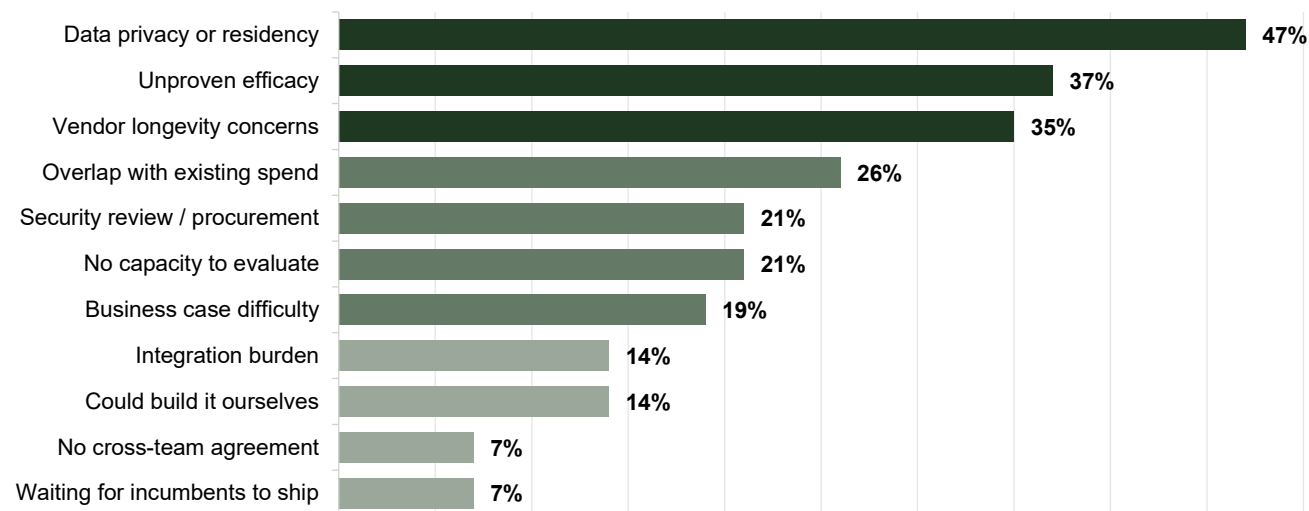
What Actually Kills a Deal

Early-Stage Vendors Signed in 24 Months (N = 45)



- **Enterprises regularly buy from early-stage security vendors despite incumbents' reach**
- 62% have signed at least one early-stage vendor in the past 24 months

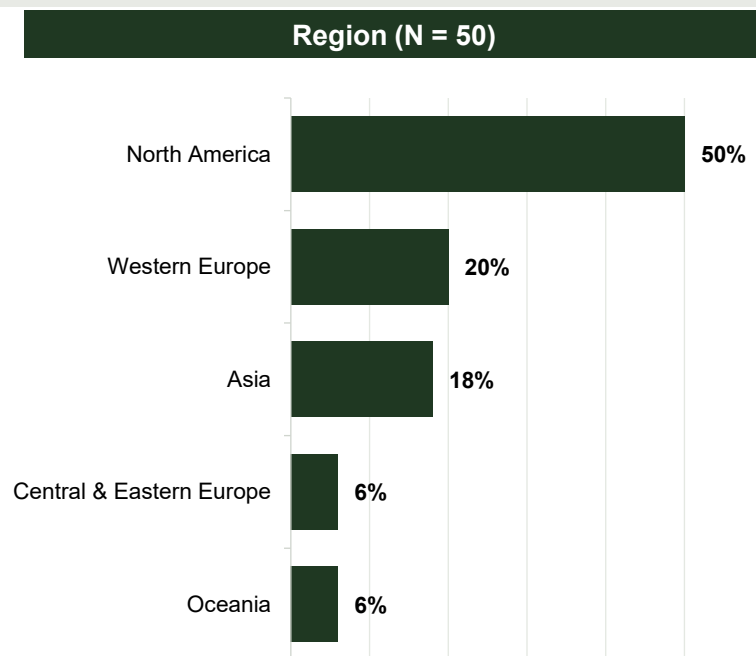
What Has Blocked or Killed a Purchase (N = 43)



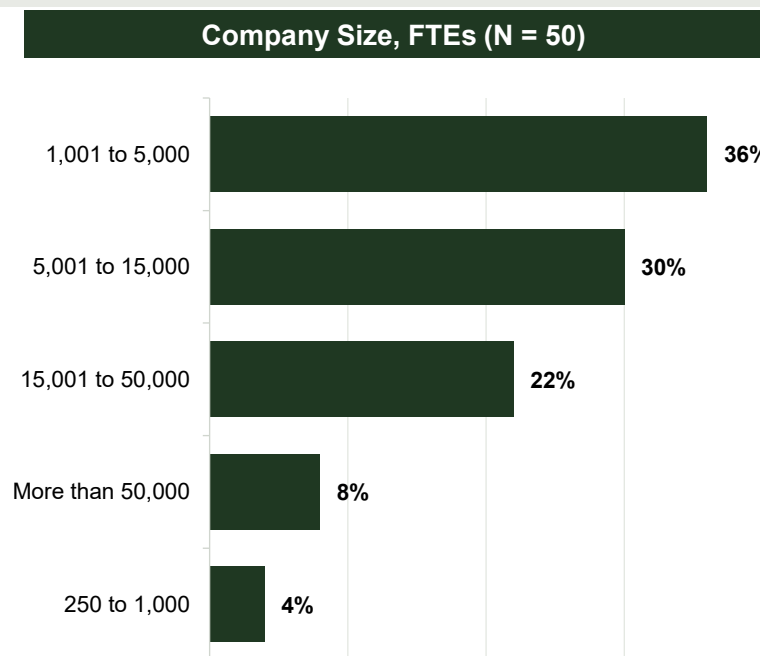
- **Startup deals mostly die on data residency and unproven efficacy, not loyalty to incumbents**
- Data privacy and residency kills the most deals (47%), an architecture choice made at founding
- Only 7% killed a deal to wait for an incumbent, and 7% over cross-team disagreement

Who We Surveyed

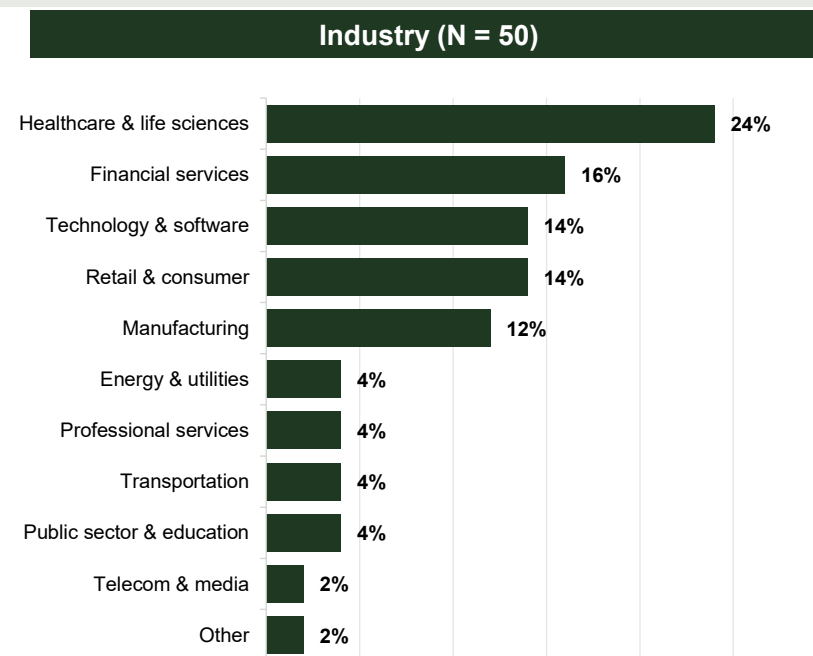
Sample Composition



- North America is the largest region, with Western Europe and Asia making up most of the rest
- North America 50%, Western Europe 20%, Asia 18%

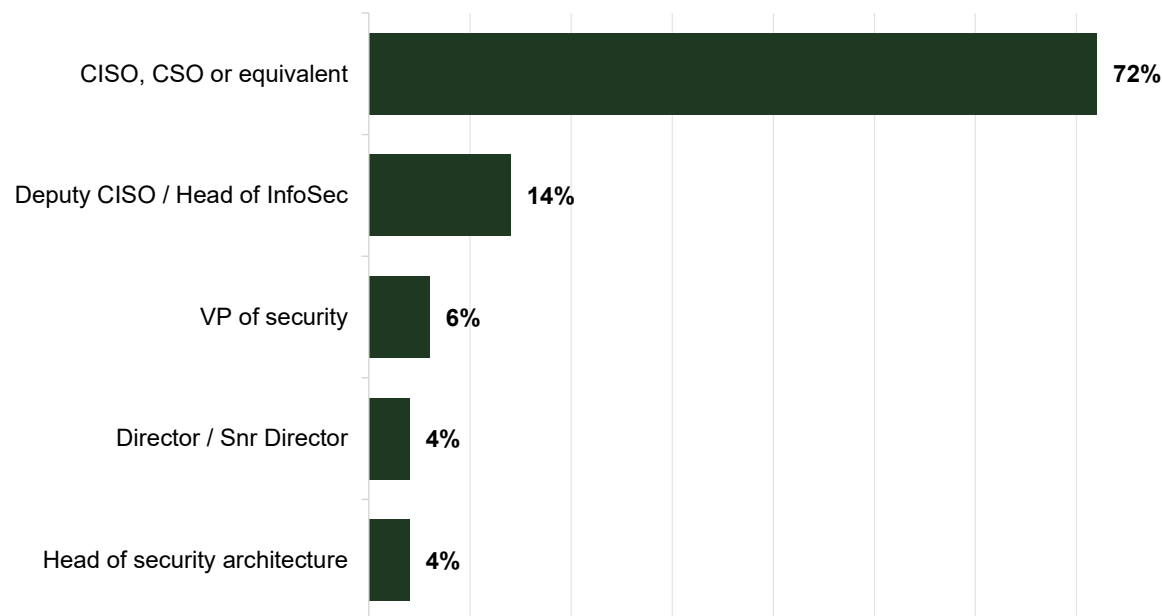


- Respondents lead security at mid-to-large enterprises across a broad mix of industries
- Two-thirds work at organizations of 1,001–15,000 employees
- Healthcare & life sciences is the largest sector at 24%



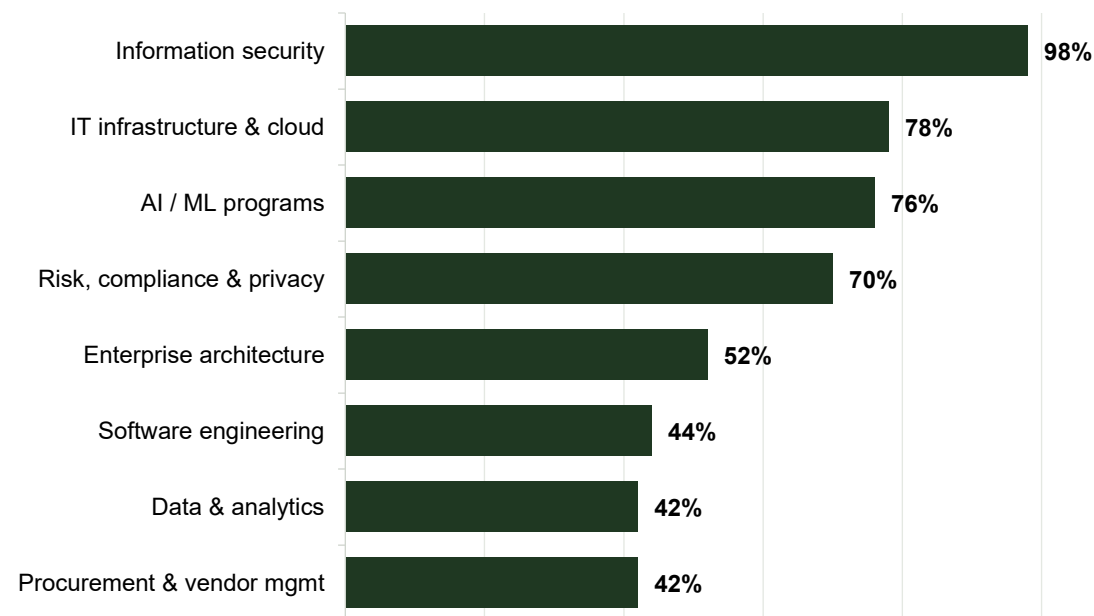
Role and Remit

Current Role (N = 50)



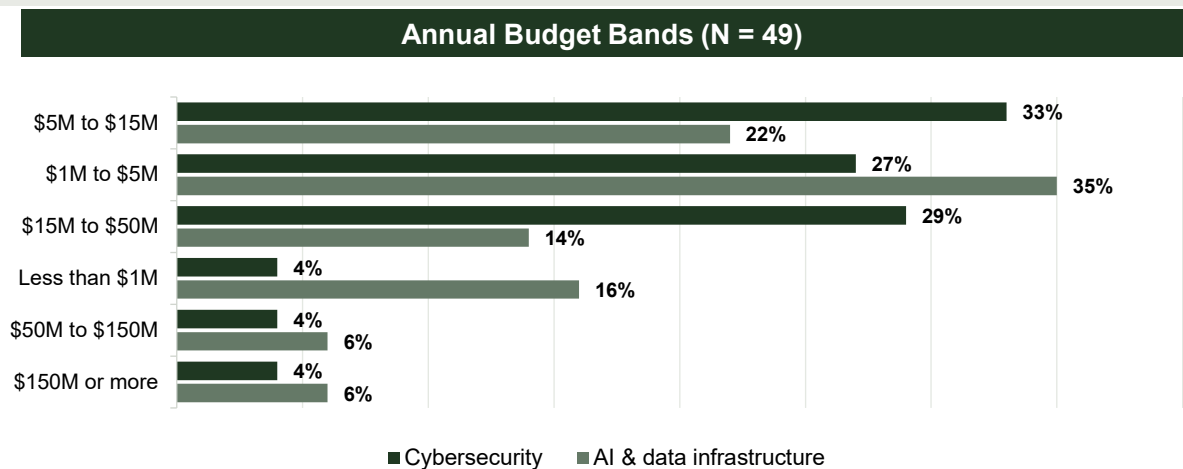
- Respondents are the senior executives who own security decisions
- 72% are CISO, CSO or equivalent, and 98% are directly responsible for information security

Also Responsible For (N = 50)

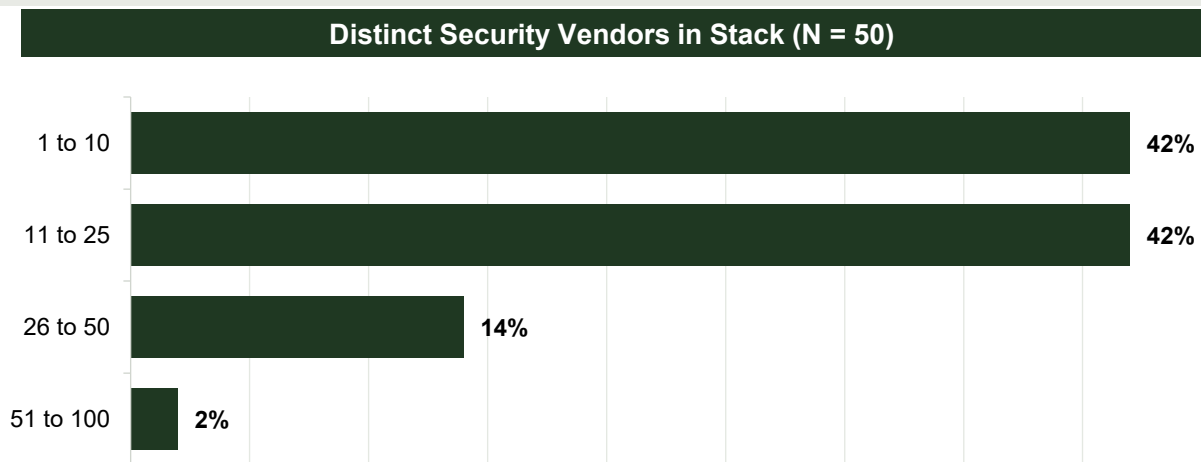


- Most security leaders also run IT infrastructure and AI programs, not just security
- 78% also own IT infrastructure and 76% own AI / ML programs

Budgets, Stack Size and Team Scale



- **Enterprises spend more on cybersecurity than on the AI and data infrastructure it protects**
- Weighted-average cybersecurity budget is \$5–15M, against \$1–5M for AI and data infrastructure



- Security teams run compact vendor stacks with little spare capacity for new tools
- 84% run 25 or fewer security vendors; a median of 18 security FTEs run a median of three tools in active pilot

18

Median security FTEs
(mean 115; range of 9 to 50)

3

Median tools in active POC
(mean 6; range of 2 to 5)

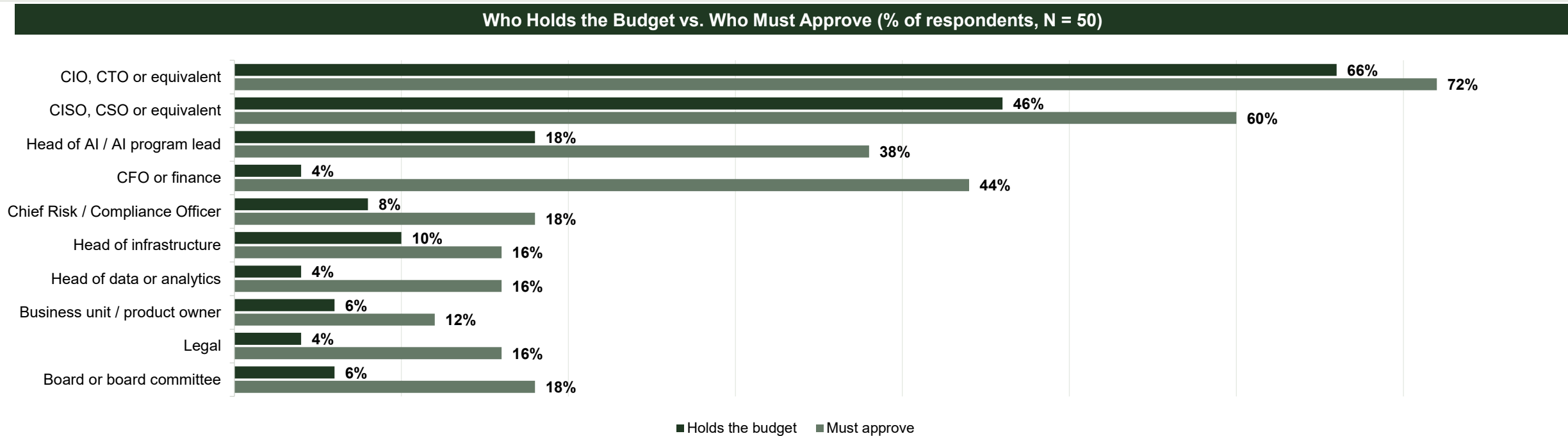
84%

Run 25 or fewer
security vendors

\$5 to 15M

Weighted-average
cybersecurity budget

The CISO Is Not the Only Signature



- **AI security purchases need sign-off from several executives beyond the CISO**
- CIO / CTO and CISO hold most budgets; the Head of AI holds budget in 18% of organizations but must approve in 38%
- Finance approves far more often than it owns budget: CFO sign-off in 44% of cases, budget ownership in 4%
- Approvals routinely span four to five roles, yet cross-team disagreement has killed only 7% of deals