

Security and enterprise readiness

What stands between our AI and enterprise revenue

\$0.0M of pipeline in security review

0 deals · median 0 days in review

☐ Agent access	How many agents run in production, and does each have its own identity? How long their tokens last, who can revoke them, and your last injection test result
☐ AI vendors	How many AI vendors touch customer data, and what triggers a re-review How much notice customers get before you add a model provider
☐ Ownership and claims	Who owns AI and security risk, and how often they report here Each claim you make to buyers (no training on customer data) and its proof
☐ Team AI tools	Which AI tools can read email, drives and CRM, and who approved them What an agent can send or delete without a person, and the approved-apps list
☐ Proof buyers can check	SOC 2 status with window dates, and your last pentest with the AI features in scope Trust center link, and the security answers a buyer's AI can find

The ask: name the one decision you need from the board.

Security and enterprise readiness

What stands between our AI and enterprise revenue

\$1.8M of pipeline in security review

5 deals · median 19 days in review

Agent access	4 production agents, each with its own identity · tokens expire in 1 hour Prompt injection success: 9% before fixes, 2% after
AI vendors	7 AI vendors, re-reviewed whenever they ship AI changes Customers get 30 days' notice before we add a model provider
Ownership and claims	CTO owns AI and security risk and reports here every quarter “No training on customer data” is in our contracts · test due November 15
Team AI tools	Inventory of AI tools that can read email, drives and CRM starts November 3 Approved-apps list due December 1
Proof buyers can check	SOC 2 Type 2 window open since October 1 · trust center public September pentest covered the AI features · security answers published

The ask: Approve the SOC 2 Type 2 audit and an AI red team test before the January enterprise launch.

APPENDIX

Evidence for every row

What a director, or a buyer's reviewer, can open and check

Row	Evidence a reviewer can check	Date	Owner
Agent access	Agent inventory with identities, scopes and token lifetimes; AI red team report with injection rates	Sep 2026	CTO
AI vendors	AI vendor list with the data each one touches; re-review triggers; subprocessor notice clause	Oct 2026	Operations
Ownership and claims	Owner named in board minutes; contract clause on training data; test plan for each claim	Nov 15	CTO
Team AI tools	Connected-apps report from Google Workspace or Microsoft Entra; approved-apps list	Starts Nov 3	IT lead
Proof buyers can check	SOC 2 Type 2 window letter; pentest letter with the AI features in scope; trust center link	Oct 1	CTO

Replace the gray examples with your own. Keep each link current: reviewers read the oldest date first.

One slide, five rows, four minutes

Fill it in

- Start with the money: pipeline in security review, deals and median days. Pull it from your CRM.
- One row per question a buyer's security team will ask. Two lines each, with numbers and dates.
- Mark each row honestly: black when it's in place with evidence, dashed when it's in progress with a date, an outline when it hasn't started (give a start date).
- End with one ask: the decision you need from the board.
- Put the evidence in the appendix, and refresh the dates every quarter.

Present it in four minutes

- Minute 1, the money: what's waiting on security review, and why.
- Minute 2, what changed since last quarter, row by row.
- Minute 3, the one risk you're carrying, and how you're handling it.
- Minute 4, the ask, and what it unblocks.
- Skip the heat maps, scan counts and acronyms. Directors want the business answer.

The guide, the data behind every row and a builder that draws this slide for you: ysecurity.io/blog/security-slide-board-deck

Made by YSecurity, the on-demand cybersecurity team. Free to use and adapt.