Rolling out to the team

A sequence that has fewer surprises than doing it all at once.

1. One machine, yours

Install, sign in, govern one tool, watch the request appear in Activity. Everything else depends on this working, so prove it once, slowly.

2. A friendly pilot, three to five people

Pick developers who will tell you when something is odd. Nothing pinned, no restrictions — they should be able to disconnect a tool and tell you why they had to.

Watch for a week. What you are looking for: tools that will not stay governed, MCP servers you did not expect, and requests failing for reasons that turn out to be a missing provider key.

3. Set policy before you widen

Use what the pilot showed you. Approve the MCP servers that turned out to be legitimate. Decide about prompt capture and **tell people the answer**.

4. Roll out

Send the installer, or push it through your MDM. If you are using managed configuration, start with **start at login** and **automatic governing** pinned, and leave the restrictions off until your policy has stopped changing.

5. Close the direct path

Once most machines are governed, apply the egress blocklist. Do this last: applying it first means the tools break before the alternative exists.

Two things to say out loud

Subscription mode does not change who pays — developers keep their own plans. And **say whether prompt capture is on**. Both rumours spread quickly and both are corrosive if they are wrong.

Revision #5
Created 2026-08-02 10:19:57 UTC by Sentilai Docs
Updated 2026-08-02 16:29:07 UTC by Sentilai Docs