

## TECHNICAL SETUP

# AgentLens

What you register, the APIs it calls, and the permissions you grant

A read-only governance agent. One Entra app registration, five Microsoft APIs, admin consent once - and nothing is ever written back to your tenant.

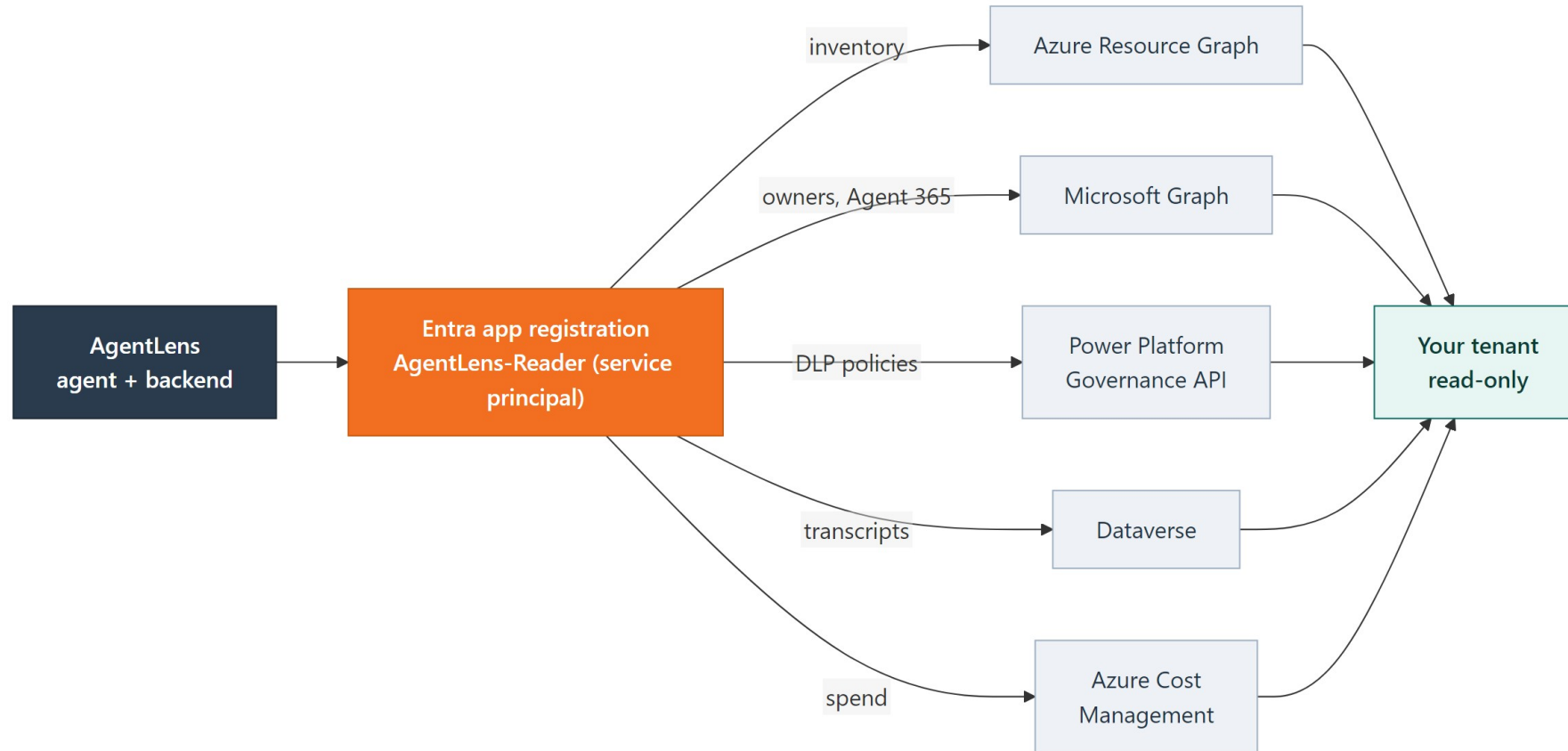


---

**Elliot Margot**

Microsoft MVP - M365 Copilot & Copilot Studio · [e-margot.ch](https://e-margot.ch)

# One registration, five read-only APIs



*AgentLens authenticates once as a single service principal, then fans out to five Microsoft APIs - each answering one question. Every call is read-only.*

## STEP 1 - REGISTER

# One Entra app registration

## AgentLens-Reader

The one you actually need - the data service principal.

**Confidential client** - daemon - no user sign-in

**Application (client) ID + tenant ID** - its identity

**Client secret or federated credential** - how it authenticates

**Grant admin consent** - once, tenant-wide

## AgentLens-WebApp

Optional - only if you host the UI.

### User sign-in (Entra SSO)

openid · profile · email

Redirect URI = your app URL

## Read-only by design

No write scopes anywhere - no Directory.ReadWrite, no environment changes. Admin consent is required once, tenant-wide, and it is auditable.

## STEP 2 - APIS & PERMISSIONS

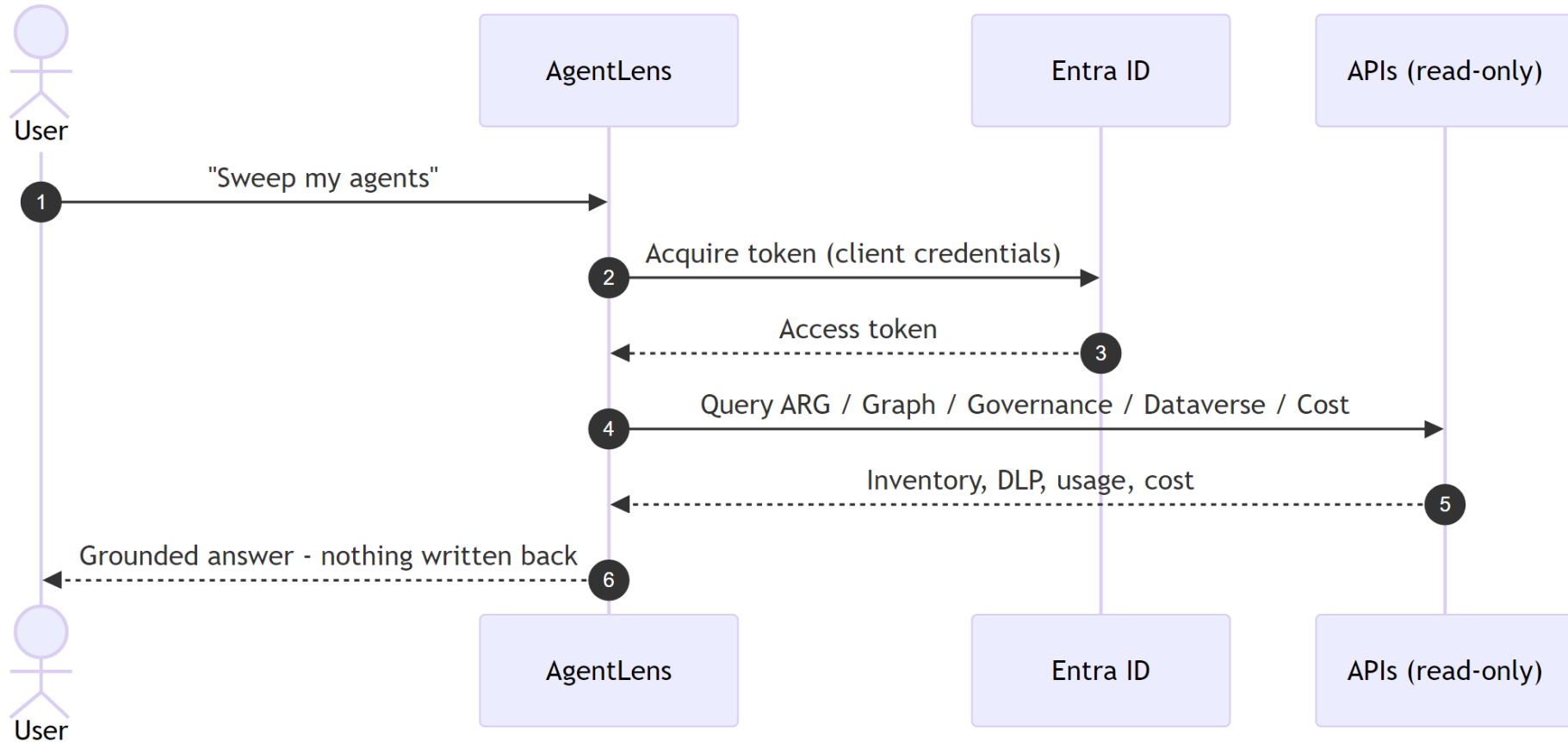
# Five APIs, the permission each one needs

| API / resource        | What it returns                           | Permission or role you grant                                                            | Consent |
|-----------------------|-------------------------------------------|-----------------------------------------------------------------------------------------|---------|
| Azure Resource Graph  | Agent inventory across all four stores    | Reader on the subscriptions + Power Platform Administrator (for PowerPlatformResources) | Admin   |
| Microsoft Graph       | Agent owners; Agent 365 packages          | User.Read.All (+ CopilotPackages.Read.All, optional)                                    | Admin   |
| PP Governance API     | DLP policies per environment              | Power Platform Administrator role                                                       | Admin   |
| Dataverse (per env)   | Conversation transcripts - aggregate only | Dynamics CRM user_impersonation / app user                                              | Admin   |
| Azure Cost Management | Real spend per store                      | Cost Management Reader (Azure RBAC on scope)                                            | RBAC    |

### One registration holds all of these

Every scope above is read-only. There is no write permission anywhere in the app - by design, for a governance tool.

# Acquire a token, read, answer - nothing written



*The service principal acquires a token via client credentials, calls the APIs read-only, aggregates in memory, and answers. No data is written back, and only aggregate counts leave the tenant.*

## GET INVOLVED

# Not open source yet - I'm looking for the right people

AgentLens is early. I'd rather build it with people who know this space than ship it alone. If any of these are you - or you know someone - let's talk.

### Agent 365

Microsoft's agent management & security layer - CopilotPackages, licensing, the A365 admin surface.

### Agent governance

DLP for agents, Default-environment lockdown, sharing controls - real-world posture, not theory.

### APIs

Azure Resource Graph, the Power Platform Governance API, Dataverse and Microsoft Graph - the plumbing underneath.

---

**Know this space, or know someone who does? Reach out.**

**Elliot Margot** · Microsoft MVP - M365 Copilot & Copilot Studio · [e-margot.ch](https://e-margot.ch)

*Thank you - questions welcome.*