What the reach sheet touches

For your change ticket. The free tenant reach sheet runs in your tenant, under one read-only app registration that you create and you delete.

1. App registration

One new app registration in your own tenant. Suggested display name: `[agency]-reach-sheet-graph`.

2. Exact permission

- `Directory.Read.All` · Microsoft Graph · **application** permission · **admin consent** required. Read-only; it cannot change anything.
- Optional, off by default: `RoleEligibilitySchedule.Read.Directory`, only if you want PIM-eligible roles shown for the listed administrators.

Nothing else. No write permission, no `RoleManagement.*`, no `AuditLog.Read.All`, no Defender or mail permission.

3. What is read

- Directory role definitions and directory role assignments.
- Members of role-assignable groups that hold a directory role.
- Account name and enabled state of the user accounts that hold a privileged role, from a fixed, published list of Microsoft role templates.
- For each service principal that holds a privileged role: its id, app id, display name, type and enabled state, and its owners (owner object id, type and enabled state only).
- OAuth2 permission grants: delegated consents and tenant-wide consents.
- The display names of the applications those grants name.

No app role assignments are read, so service principals' application permissions are not shown. No other user account or service principal is listed; delegated consents held by other users appear only as one number.

4. What is never read

Mail, files, messages, sign-in logs, audit logs and devices. Application permissions of service principals. The whole directory, all users and all service principals are never enumerated. Nothing is written to the tenant.

5. Where results land

One HTML page and one JSON file, written to a folder the operator chooses on their own machine. Nothing is written to tenant storage. Nothing is transmitted to Cerydora.

6. How to revoke

Delete the app registration. One step; its client secret goes with it. Nothing else was installed.

7. Who at Cerydora can see results

No one. Cerydora never runs the tool, never receives its output and holds no access to your tenant.

The sheet is an inventory of effective permissions. It does not say who authorized any grant, and it is not an audit finding or sealed evidence. Questions: hello@cerydora.com.