TransitionSuite · Security fact sheet

Whisper Consulting · Version 1.0 · November 2026

In one paragraph

TransitionSuite is an Excel workbook plus an Office add-in, a set of web screens that runs inside Excel. The add-in reads and writes only the workbook that is open. It has no server, no database and no user accounts, and it sends no data anywhere. Its files are hosted by the client, and it is deployed by the client's IT through the Microsoft 365 admin center. Access to the data is controlled by the permissions on the workbook in SharePoint or OneDrive, exactly as for any other Excel file.

How data flows



No data leaves the workbook. The panel loads its code from the two places shown, then works entirely inside Excel.

Key facts

Area	Fact
Permission requested	`ReadWriteDocument` : the open workbook only. No access to mail, calendars, other files, Microsoft Graph or the user's identity.
Where data is stored	Only in the workbook. A few add-in preferences (logo, office name, pack commentary and section choices, "not needed" interview flags, checklist ticks) are kept in the workbook's hidden add-in settings. They travel with the file and go nowhere else.
Network calls	Two at start-up: the add-in's own static files from the client's host, and Office.js from Microsoft's CDN, which Microsoft requires for add-ins. There are no other calls: no analytics, tracking, telemetry, cookies, third-party fonts or third-party libraries.
Server-side code	None. The host serves static files only.
Authentication	None in the add-in. Who can open and change the workbook is decided by SharePoint or OneDrive permissions and the client's normal Microsoft 365 sign-in, conditional access and MFA.
Hosting	On the client's own HTTPS host, so the client controls the code that runs, its version, and when it changes.
Deployment	Through the Microsoft 365 admin center (Integrated apps), to named users or groups. It can be removed centrally at any time.
Code	Plain JavaScript with no third-party packages. The source is held in Whisper Consulting's private repository and can be made available for review. The IBM Plex Sans font is bundled (SIL Open Font License).
Macros and VBA	None. The workbook is a plain .xlsx file.

Handling of content

- **No HTML from data.** Everything shown on screen that comes from the workbook is inserted as text, never interpreted as HTML. A workbook cell that contains script text is therefore displayed, not run.
- **Files created by the user.** The calendar file (.ics) and printed or PDF output are generated on the user's machine. They are saved only where the user chooses.
- **Email requests.** "Ask the lead by email" opens the user's own mail program with a draft message. The add-in doesn't send email.
- **Logo upload.** The logo image stays in the workbook's add-in settings. It is limited to 300 KB and to PNG, JPG or SVG.

Failure and resilience

- If the host can't be reached, the panel doesn't load. The workbook keeps working as normal, because every screen has a worksheet behind it.
- If Microsoft's Office.js can't be reached, the panel shows a message instead of the screens. No data is affected.
- Edits are written cell by cell, as if the user had typed them, so Excel's version history, AutoSave and co-authoring all apply as usual.
- Calculated cells are locked by sheet protection. The add-in never writes to them.

What the client controls

- Who gets the add-in: assignment in Integrated apps.
- Who can see and change the data: workbook permissions.
- Which version runs: the files on the client's host.
- Network policy: allow-list the host address and `appsforoffice.microsoft.com`.

The Connected level (Level 3, coming soon)

Everything above describes Levels 1 and 2, as delivered today. The Connected level (`DEPLOYMENT-LEVELS.md`) adds the following, and nothing else.

- **Microsoft Graph, limited to one site.**
- The add-in, the Teams tab and the web page sign people in with their own Microsoft 365 account.
- They read and write SharePoint **lists** on the programme's site only.
- Access is delegated, so a person never sees more than they already can, and IT names the one site (Sites.Selected).
- **Two named library exceptions, both Microsoft's own, bundled with TransitionSuite's files and never loaded from a CDN:**
- **MSAL** (`@azure/msal-browser`, MIT licence) for silent sign-in, which reuses the Office or Teams sign-in;
- the **Teams JavaScript library** (`@microsoft/teams-js`, MIT licence), needed for a Teams tab.

No other third-party code is used. - **Network calls go to Microsoft only:** - Office.js; - sign-in (`login.microsoftonline.com`); - Graph (`graph.microsoft.com`); - inside Teams, Microsoft's list of Teams domains (`res.cdn.office.net`). - **No client data on the web host.** The host serves code and demo data only. Programme data is read live from the client's SharePoint after sign-in and is never stored anywhere else.

For your review

- **Review of the code.** Clients can review the code, or have it reviewed independently, before hosting it.

- **Web host headers.** Clients may wish to set a Content-Security-Policy on their host. Whisper Consulting can supply recommended header values.