FormCraft 365

Security & Zero-Backend Architecture Fact Sheet

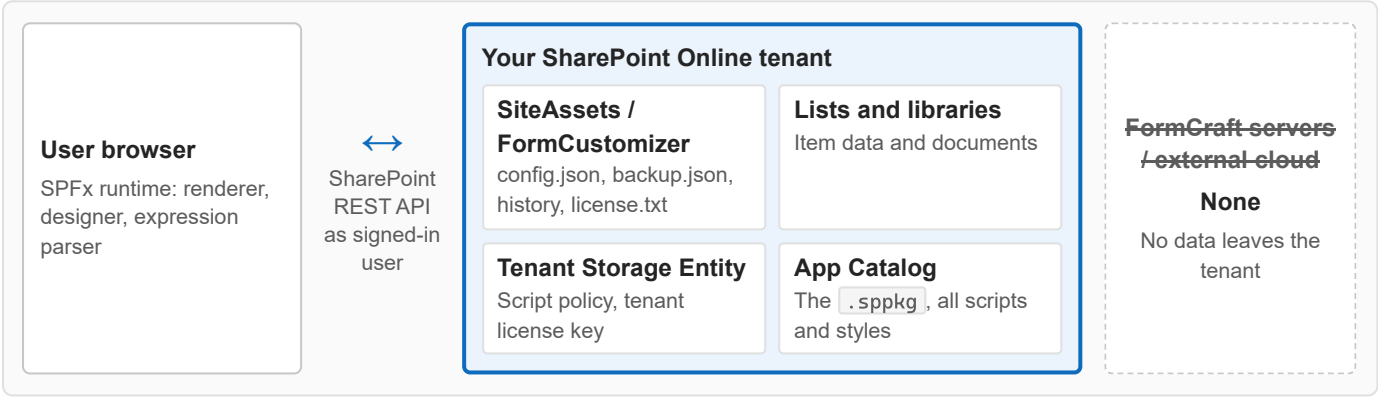
Technical summary for Microsoft 365 security and App Catalog review

formcraft365.com
hello@formcraft365.com
docs.formcraft365.com

Executive summary

- **100% client-side SharePoint Framework (SPFx) `.sppkg`.** Scripts and styles are bundled in the package (`includeClientSideAssets: true`) and served by SharePoint from your App Catalog. No external CDN.
- **No FormCraft backend servers and no third-party cloud storage.** Configuration, history and the license key are files and entries in your tenant. License verification makes no network call.
- **Runs in the user's browser as the signed-in user.** Every read and write goes through SharePoint with that user's Microsoft Entra ID identity and SharePoint permissions.

Architecture and data flow



Outbound calls: only `triggerFlow` actions that you configure send an HTTPS request, and only to Power Automate / Azure Logic Apps hosts (`*.logic.azure.com`, `*.powerplatform.com`, `*.api.powerplatform.com`).

Core security controls

Data and config residency + Storage Lock

Each list's configuration, automatic backup and last 10 history versions live in `SiteAssets/FormCustomizer/<list>/`. On the first save by a site owner, **Storage Lock** gives the folder unique permissions: site owners and the locking user keep Full Control, every other principal is reduced to Read. If locking fails, the original inheritance is restored.

Designer access control

By default only site owners (`ManageWeb`) can open the designer. Owners can extend access to one named SharePoint group. If the permission check fails, the user is treated as unauthorized. Changing folder permissions requires `ManagePermissions`.

Tenant script policy (fail closed)

Custom JavaScript (`onFormLoad`, `onBeforeSave`, named functions) is **disabled by default**. It runs only after an App Catalog administrator sets the Storage Entity `FormCraft365_ScriptsPolicy` to `allow`. A missing value, any other value or a read error keeps scripts off.

Safe expression evaluator (no `eval`)

Rules, formulas and button actions run through a custom parser with nesting capped at 64 levels. It does not use `eval` or `new Function` and has no access to `window`, the DOM or `fetch`. Expressions work when scripts are disabled and need no `unsafe-eval` in CSP.

Additional safeguards

AI Assistant privacy (Pro)

The assistant calls no AI service. It builds a prompt file for the organization's own chat, containing column names, types and settings, **never item data**. The pasted response is schema-checked, summarized before → after, and needs confirmation for script changes and large removals.

Input and concurrency safety

Item saves use ETag optimistic concurrency with a conflict dialog; configuration saves carry a revision. Post-save redirect URLs are validated to `http`, `https` or relative, with field values encoded. Hyperlinks with unsafe schemes such as `javascript:` render as plain text.

Offline licensing: "Forms Never Stop"

The license key's signature is verified in the browser. No external license service is called. Limits apply only in the designer. A missing, expired or unreadable key falls back to Community mode and never blocks users from opening forms or saving data.

IT / security review quick-check

Review question	FormCraft 365 behavior	Verification
Where are form data and config stored?	Item data stays in your SharePoint lists. Config is in `SiteAssets/FormCustomizer`.	Browse the folder in Site Assets; watch browser network traffic while saving a form.
Does the package call a vendor service?	**No.** There is no FormCraft backend, and licensing is verified offline.	Browser DevTools → Network while opening and saving a form.
Are external CDNs used for scripts or styles?	**No.** Assets are bundled (`includeClientSideAssets: true`) and served by SharePoint.	Inspect the package manifest; check script origins in DevTools.
Can end users modify form rules or scripts?	**No.** The designer requires `ManageWeb` or the designer group, and Storage Lock leaves others Read only.	Review permissions on `SiteAssets/FormCustomizer`; open a form as a site member.
Can designers run arbitrary JS without tenant admin approval?	**No.** Scripts are blocked unless `FormCraft365_ScriptsPolicy` is `allow`.	Read the Storage Entity in the tenant App Catalog; see Security in the designer.
Are item values ever sent to AI?	**No.** The prompt is exported manually and holds column metadata only.	Open the downloaded `form-ai-prompt.md` before sharing it.

Boundaries to plan for

- **Enabled scripts are not sandboxed.** They run in each form user's browser with that user's permissions.
- **The editor-lock password is not a security boundary.** Protection comes from the Storage Lock.
- **Configuration is readable by form users,** including any `triggerFlow` webhook URL. Flows must not trust client data.
- **Locked configuration is readable by the organization and guests by default.** Both can be switched off.

© 2026 FormCraft 365 · Security & Architecture Summary · Full documentation: docs.formcraft365.com/en/admin/permissions.html