

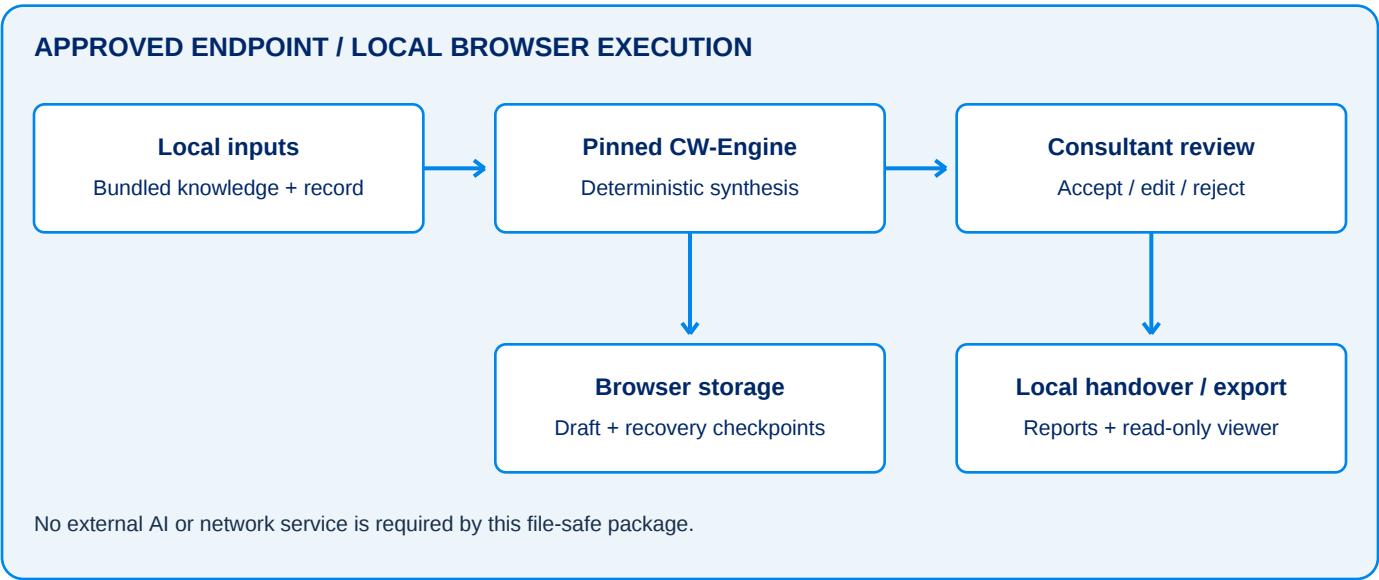
# Security architecture & deployment review

## Public edition | Offline NatSec Workbench | 28 September 2026

Understand how Cloud Waypoint supports local readiness work, keeps consultant decisions explicit and equips a security team to evaluate deployment in its approved environment.

### 01 / Designed for local readiness work

The offline Workbench brings bundled knowledge, CW-Engine synthesis, consultant review and handover into a browser-based workflow. The engagement record can remain within the approved boundary throughout that workflow. A receiving organization determines whether the software and its operating conditions are acceptable.



| Capability              | What the offline package provides                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Browser-based execution | Extract the blank NatSec package and open index.html locally. The intended endpoint is an approved Windows/Edge environment. No native installer, administrator rights, browser extension or local web server is required by this package. |
| Model-free operation    | CW-Engine produces deterministic readings and proposals from the bundled rules and record. Consultants review proposed decisions. An AI model is not required; the optional second reader is disabled in the model-free offline package.   |
| Local handover          | Generate reports, handover files and a read-only client viewer locally. AI handover instructions do not themselves upload records or activate an AI service.                                                                               |

## 02 / Data handling and deployment responsibilities

| Area                  | Application behavior                                                                                                                                                    | Organization's review                                                                                                                     |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Records and recovery  | Local drafts and recovery checkpoints use browser storage. Explicit record/session exports provide a portable recovery path.                                            | Validate persistence under the actual browser policy. Browser profiles and local-file storage behave differently across environments.     |
| Storage protection    | Browser records and exported files are plaintext at the application level.                                                                                              | Apply endpoint encryption, access, backup, retention and approved-media controls appropriate to the data.                                 |
| Network behavior      | The file-safe workflow needs no external network connection. Its content security policy restricts connections; local scripts and styles execute in the browser.        | Review inline script execution, external links and exported HTML. Browser policy does not replace endpoint security or transfer approval. |
| Handover scope        | Client turnover omits working-session and reader-history material. Practice exports have a different scope.                                                             | Check the selected export and handling requirements before sharing. Browser records and downloaded files are separate copies.             |
| Separate environments | IL5 and IL6 records can be worked independently on their approved devices.                                                                                              | This is not a cross-domain transfer mechanism. Any movement of information requires the organization's approved process.                  |
| Optional AI           | A separately configured second reader can stage suggestions for consultant review in permitted environments. It is excluded from the model-free package described here. | Approve any model-enabled configuration separately. No AI installation or record submission is implied by these materials.                |

## 03 / What a security reviewer should establish

**Identify the package and endpoint.** Record the exact software version, package digest, browser build, endpoint policies and intended data scope. Obtain the matching software bill of materials (SBOM), provenance and validation records for the submitted package.

**Exercise the complete workflow.** Use approved test data for launch, import validation, consultant decisions, report generation, save/restore, failure recovery and cleanup. Observe network behavior throughout, not just at startup.

**Record the receiving authority's decision.** Retain results, exceptions and approved operating conditions. A successful functional test is evidence for that decision, not an authorization.

## 04 / Provenance and evidence you can request

Cloud Waypoint was developed from DoD cloud-readiness practice under Chuck Greene’s product and method direction. Development has included Anthropic Claude Code and OpenAI Codex. AI-assisted development is part of the provenance; it is not independent assurance. Development AI services are not runtime dependencies of the offline package.

| Review material                               | Purpose                                                                                                                                                      |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical architecture and package provenance | Explains the delivered components, compiled CW-Engine snapshot and data paths for the exact package under review.                                            |
| Package hashes and component inventory        | Lets a reviewer match retained evidence to the delivered bytes. Hashes establish identity, not trust or approval.                                            |
| Software bill of materials                    | Identifies components within its stated scope. Confirm that it covers the submitted offline package; a file inventory alone is not an SBOM.                  |
| Validation receipts                           | Describe the actual test environment, software version, observations and limitations. Historical test results do not automatically apply to a newer package. |
| Endpoint review procedure                     | Supports local testing of browser policies, imports, persistence, exports, network behavior and cleanup on the intended device.                              |

## 05 / Validation scope and assurance limits

Engineering checks for the reviewed model-free build included recovery/workflow checks and an isolated offline Mac/Chromium startup with no observed HTTP(S) requests or page errors. Those observations are limited to the tested conditions; they are not a current Windows/Edge hardened-endpoint validation or a full security audit.

Historical Windows/Edge evidence is retained separately. The reviewed evidence does not establish that the current package was validated on a STIG-hardened government-furnished endpoint. Deployment compatibility must be established against the receiving organization’s actual endpoint and policy.

This overview does not claim DISA certification, device accreditation, IL6 approval or system authorization. Cloud Waypoint supports readiness and evidence organization; named individuals with the applicable authority retain approval and authorization decisions.

## 06 / Start a deployment review

Request the detailed security review and package-specific evidence through your Cloud Waypoint engagement contact. Exact release identifiers, private source locations and retained technical receipts are supplied through the agreed review channel.

Scope: the blank, model-free NatSec offline Workbench. Hosted sites, older endpoint kits and optional model-enabled configurations require their own scope review. This public overview is not a substitute for the submitted package’s release evidence.