

OpenAI



ChatGPT Work: Enterprise security

Execution boundaries, data protections,
and enterprise controls.

SECURITY WHITEPAPER

Executive summary

A framework for a controlled deployment

For enterprise security architects, privacy and GRC reviewers, workspace administrators, and account teams.

ChatGPT Work uses your organization's existing ChatGPT workspace and applicable business-data protections to help employees complete tasks using approved information and tools. This overview explains the execution boundaries, connected identities, data handling, administrator controls, and review considerations for a limited deployment.

- Work Cloud runs tasks on OpenAI-managed infrastructure; Work Local interacts with supported resources through the ChatGPT desktop app on the employee's device.
- The employee and device remain outside OpenAI systems and OpenAI Trust Zone 01. Verify device-management requirements separately from workspace membership.
- Cloud tasks do not automatically receive local files, browser sessions, passwords, device access, or the employee's private-network connectivity.
- Local execution does not mean that model inference or all task data remains on the device; intentionally supplied or authorized content can be processed by hosted services.
- Access depends on the actual workspace permissions, enabled capabilities, connected identity, application approvals, and applicable device controls.
- Business, Enterprise, Edu, and eligible Healthcare workspaces provide protections for covered service data; retention, administrator controls, and audit visibility vary by plan, information category, and configuration.

Execution architecture and trust boundaries

The surface used to start a task is not its execution environment. Supported web and mobile Work tasks run in the cloud. The desktop app can support cloud or local tasks when the relevant capabilities and permissions are available.

Work Cloud runs tasks in isolated, virtual-machine-backed execution environments on shared OpenAI-managed infrastructure. Access to task state is scoped to the relevant account and user, and an execution environment may be reused for subsequent authorized tasks.

A Work Cloud deployment crosses four distinct boundaries:

- **Customer or employer IT boundary:** The employee, their device, local files, applications, browser sessions, credentials, VPN, and private networks remain outside OpenAI systems and all three numbered trust zones. If the rollout requires employer-managed devices, verify that the device is enrolled and the required policies apply.
- **Trust Zone 01 — OpenAI-operated service access:** ChatGPT's service interface handles authenticated access and enforces applicable workspace identity, membership, and access policies.
- **Trust Zone 02 — hosted execution:** An isolated OpenAI-managed Work environment orchestrates the task, model interactions, authorized tools, and applicable hosted content.
- **Trust Zone 03 — external destinations:** Approved apps, hosted browsing, or separately governed network paths may reach permitted customer systems, third-party services, public websites, or required managed destinations.

An external request must follow an enabled and authorized path. Hosted execution does not inherit a return path into the employee's device simply because the task originated there.

If a person intentionally uploads a document, approves an application or browser interaction, or authorizes a connection, relevant content can become task context and reach hosted services. Assess the information actually supplied, not only where the original file resides.

Cloud and local execution

Security question	Work Cloud	Work Local
Where does execution interact with resources?	In an isolated OpenAI-managed environment.	Through supported capabilities of the desktop app on the employee's device.
Which surfaces can start a task?	Supported web, mobile, and desktop experiences.	A supported desktop experience.
Can it automatically read files on the employee's device?	No. Files or content must be intentionally provided through an authorized path.	Selected local resources can be used when the task, user, operating system, and applicable device controls permit access.
Does it inherit the employee's existing browser session?	No. Hosted browsing uses a separate session and does not inherit the employee's existing browser sign-ins.	An approved local browser or desktop-application path may use an existing signed-in session.
Can it reach internal company systems?	Only through an authorized connection or another explicitly supported access path; it does not inherit the device's VPN.	Only through a permitted device, browser, application, network, or connected-account path.
Does local execution keep all processing on the device?	Not applicable: execution is hosted.	No. Local execution refers to where tools run, not on-device model inference. Relevant task content can be sent to OpenAI-operated services for processing and storage.
How is execution access managed?	Review the Work Cloud permissions available in your workspace.	Review the Work Local permissions available in your workspace.

Resource access boundaries

A cloud task can use information a person submits, an intentionally uploaded or attached file, permitted project or Library content, an authorized app connection, or an enabled website capability. It does not automatically inherit local files, desktop applications, open browser tabs, saved passwords, existing website sign-ins, corporate VPN access, or private networks.

A local task can interact with selected files, approved applications, permitted browser experiences, authorized connections, or other supported device capabilities. Enabling local Work alone does not grant administrator privileges, approve every application, expose every file, bypass operating-system safeguards, or authorize every account or external action.

Identity, apps, and external destinations

An app or plugin can retrieve information or act in another system only when the workspace permits the app and any required plugin, the connection is authorized, and the connected account's permissions allow the request. Enabling a plugin does not automatically enable its underlying app or authorize an account.

A personal connection uses the employee's source-system permissions. A shared or agent-owned connection uses its connected account's permissions, which may be broader. Limit account scopes, eligible users, and supported read/write actions or confirmation settings.

Review these access paths separately:

- **Hosted browser:** Uses a separate hosted session and does not inherit the employee's local browser profile, open tabs, saved passwords, or existing sign-ins. Where supported, users can sign in separately through a secure hosted sign-in flow. Availability depends on workspace permissions and rollout.
- **Local browser or approved desktop application:** May use an existing authenticated session or a separately signed-in desktop browser. Evaluate the account, website, application approval, operating-system permission, and available device policies. Browser Use site restrictions do not apply when Computer Use operates a browser as a desktop application; review application access and device controls separately.
- **Connected apps:** Reach permitted source-system data and actions through the authorized account and integration-specific controls.
- **Code or shell networking:** Follows its own network policy. Required managed destinations may remain reachable when general public internet access is disabled; a destination allowlist is not a shell-command allowlist. When available, changes to the cloud code and shell network setting take effect after the current run finishes and Work refreshes its execution environment.

Cloud browsing, web search, connected apps, local browsing, and shell networking are distinct capabilities. Restricting one does not automatically disable the others or authorize external disclosure.

Enterprise administration and deployment controls

Feature availability, permission labels, defaults, and enforcement can vary by plan, workspace rollout, role, desktop client, operating system, and integration. Verify the controls present in the actual deployment before relying on them.

- **Execution access:** Review the Work Cloud and Work Local permissions available in your workspace. For Work Local, verify effective access in the deployed desktop client with one explicitly allowed pilot account and one explicitly denied account, and record whether the applicable control affects Work Local, Codex Local, or both. Enable only the execution environments approved for each user or group.
- **Effective role access:** Verify each participant's permissions across all assigned roles and applicable workspace policies. If a user has multiple custom roles, disabling a permission in one role does not override access granted by another.
- **Product surfaces:** A Work Cloud permission can apply across supported web, mobile, and desktop experiences; it is not, by itself, a per-surface restriction.
- **Apps and actions:** Verify app and plugin availability, connected-account scopes, eligible users, source-system permissions, and supported action or confirmation controls.
- **Browser and networking:** Where supported, review cloud-browser access separately from Work access, web search, and code or shell networking. Do not assume hosted browsing inherits the employee's VPN, proxy, or organizational network policies. Distinguish administrator-enforced restrictions from user-managed website permissions.
- **Managed devices and Computer Use:** Work Local, browser access, and Computer Use are separate capability decisions. Computer Use requires an approved application and applicable operating-system permissions. Review supported device restrictions, persistent application approvals, and platform-specific behavior before enabling it.

A suggested model, starting setting, or user experience is not an enforced access restriction. Test both the permitted workflow and the intended denial with a representative nonadministrator account.

Data protection and lifecycle

Covered data from Business, Enterprise, Edu, and eligible Healthcare workspaces is encrypted in transit and at rest and is not used to train or improve OpenAI models by default. Confirm the applicable plan, service, information category, agreement, and configuration; these protections do not automatically extend to unmanaged device files, third-party systems, or exported records.

Information category	Review the applicable lifecycle
Hosted conversations	Follow the workspace's applicable conversation-retention settings. Deleted chats are generally scheduled for permanent deletion within 30 days, subject to published security, legal, and de-identification exceptions.
Saved memories	Saved memories are managed separately from conversation history. Deleting a conversation does not necessarily delete an associated saved memory; review applicable workspace settings and deletion controls.
Hosted execution state and snapshots	Hosted execution state follows a separate lifecycle from conversations and saved files. Confirm applicable retention, deletion, and residency; deleting a conversation or file does not necessarily remove hosted execution state immediately.
Files saved to Library	Follow applicable Library and workspace retention rules. Deleting a conversation does not delete a separately saved Library file.
Project files	Remain associated with their project until removed or the project is deleted, subject to applicable deletion rules.
Eligible transient Enterprise uploads	Certain temporary uploads outside Library may expire after 48 hours when the relevant product and retention conditions apply; this is not a general rule for all files or local content.
Connected-app records	Original records follow the source system's policies. Copies saved to a hosted conversation, project, Library, or another location follow that location's rules.
Hosted browser data	The hosted browser keeps its browsing data, cookies, and website sessions separate from the employee's local browser.
Device and local-browser artifacts	Local files, outputs, browser sessions, downloads, application records, and device backups follow the relevant endpoint, browser, or source-system behavior. Confirm separately which selected task content reaches hosted services.
Eligible compliance records	Supported Compliance Logs Platform records are available for 30 days; exported copies follow the receiving system's retention policy.

Keys, residency, and deletion

Enterprise Key Management is available for eligible Enterprise and Edu workspaces and supported data categories. Confirm which Work data and configurations are covered; do not assume customer-managed keys apply to connected systems or every execution artifact.

Deleting a chat, removing a saved file, clearing hosted or local browser data, disconnecting an app, and deleting an exported record are separate actions. Hosted-snapshot cleanup can occur separately from file deletion. Data residency, inference residency, deletion commitments, and regional availability depend on the applicable agreement and supported configuration.

Audit and compliance visibility

Eligible Enterprise and Edu workspaces may have access to supported Work prompts, responses, connected-app activity, or other documented compliance events. Available records differ by execution mode, event type, product surface, integration, plan, workspace enablement, and configuration. Access to an event also requires the appropriate Compliance API authorization scope.

Work conversations can be associated with the employee who initiated them. Actions performed through a personal connection use that employee's connected account; actions performed through a shared or agent-owned connection use the connected account and may appear under that account in the external system. Available compliance and source-system records vary by integration and do not necessarily provide a complete action-by-action record or identify who approved each action.

Review the available Work, administrator, connected-system, and endpoint records for the relevant execution mode. Do not assume those records capture every browser action, approval, file operation, or external change.

Shared security responsibilities

OpenAI operates the hosted service and execution environment and provides applicable documented enterprise privacy protections, product controls, and supported compliance capabilities.

The customer manages employee identity, workspace membership, role assignments, approved devices, source-system permissions, connected accounts, endpoint policy, permitted data, human approvals, monitoring, and the decision to authorize a deployment.

Validate a limited deployment

1. Choose one useful task, approved information, a small user group, and an accountable owner.
2. Confirm whether the task needs Work Cloud, Work Local, browser access, Computer Use, an app or plugin, or a connected account.
3. Verify effective permissions and enable only the access required; review consequential actions and persistent approvals.
4. Confirm applicable retention, deletion, residency, connected-account identity, and available audit records.
5. Test both an approved task and an action that should be blocked using a nonadministrator account.
6. Record how to revoke access, disconnect accounts, and stop the pilot before expanding.

For example, compare an approved vendor advisory with an authorized inventory extract, or review approved local files on a managed device. Have a person review the result before expanding access.

Published documentation

- [ChatGPT Work overview](#)
- [ChatGPT Work and Codex](#)
- [Role-based access control](#)
- [Cloud browser](#)
- [Managed configuration](#)
- [Enterprise privacy](#)
- [Chat and file retention policies](#)
- [OpenAI Compliance Platform](#)