OPENAI ENGINEERING + ASSURANCE READOUT

# Inside the Codex Sandbox

Execution boundaries in the existing environment

A visual readout of how Codex configures, enforces, and runs commands, and how enterprise evidence must follow authority changes.

OFFICIAL OPENAI SOURCE / INDEPENDENT LUMINITY SYNTHESIS



Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.

Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026

OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

# The Codex Sandbox in One View

The harness resolves permissions, prepares the command, applies platform controls, and runs the process tree.

## DOCUMENTED EXECUTION PATH




### Filesystem Boundary

PROFILE

Workspace writes sit beside protected paths and broad reads allowed by the operating-system user.

### Network Boundary

STATE

Network can be off, direct, or filtered through an active proxy that applies domain rules.

The control ends where another process, server, or person consumes an output under different authority.

IN THIS READOUT

## Key Points

**01 Existing Environment**

Native developer tools remain available inside platform constraints.

**02 Effective Configuration**

Resolved rules, managed limits, runtime roots, and proxy state set the real boundary.

**03 Authority Handoffs**

Escalation, MCP launch, and later artifact use need separate evidence.

OpenAI documents the execution control. Luminity supplies the enterprise transition-evidence reading.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.

Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026

OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

# Commands in the Existing Environment

Codex keeps native tools available while platform controls limit what each command can reach.

01

## Design Choice




02

## Tradeoffs

### Broad Reads

LIMIT

Sensitive files readable by the OS user may remain visible.

### Network Off by Default

DEFAULT

The workspace profile blocks network access until a different boundary applies.

### Later Execution

HANDOFF

A modified package may run later through an editor or another tool.

**DEFENSE IN DEPTH**

The sandbox limits command access. Training and alignment help the model use that access as intended.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.

Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026

OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

# Sandboxed Command Execution

The harness turns configuration and command context into one constrained process launch.

01

## Execution Path




02

## Evidence at Each Transition

### Resolved Profile

CONFIG

Inherited rules, managed limits, and effective roots.

### Launch Inputs

CONTEXT

Command, arguments, working directory, environment, and requested permissions.

### Applied Controls

CONTROL

Generated platform policy plus actual proxy state.

### Observed Outcome

OUTCOME

Process result, descendants, approved exceptions, and artifacts.

03

## Evidence Boundary

- Candidate Records
- Configuration Dependent
- No Complete Automatic Package

**LUMINITY RULE**

Retain the effective boundary and observed result, not only the intended configuration.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.

Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026

OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

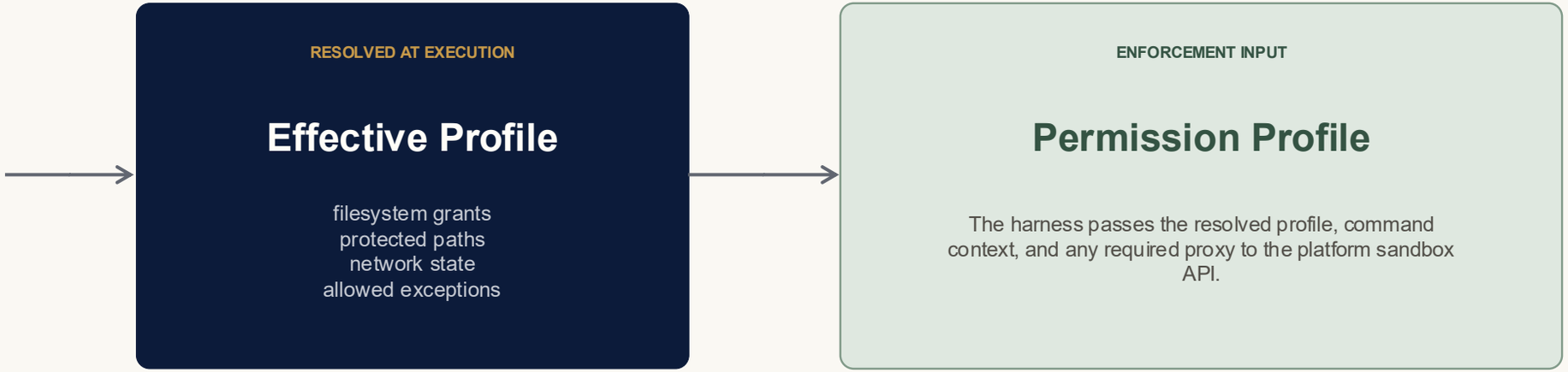
# The Effective Permission Profile

Authored settings, inherited profiles, managed requirements, and runtime roots resolve into the launch boundary.

01

## Configuration Inputs

- Built-in or named profile
- Profile inheritance
- Layered config
- Managed requirements
- Runtime workspace roots




02

## Workspace Profile Defaults

### Workspace Writes — WRITE

Active workspace roots and system temp paths.

### Protected Paths — READ

Selected paths such as .git and .codex remain read-only.

### Broad Reads — LIMIT

Other OS-readable files can remain visible.

### Network Disabled — DEFAULT

The workspace profile blocks network by default.

**VERSION NOTE** Managed permission-profile allowlists require Codex 0.138.0 or later. Older clients ignore those fields.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.

Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026

OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

# The Network Boundary

Network availability and domain filtering depend on separate settings and actual proxy activation.

01

## Three Runtime States

| | | | |
|---|---|---|---|
| 01 | **Network Off** | Commands cannot access the network. | DOMAIN RULES IRRELEVANT |
| 02 | **Direct Network** | Network is enabled while the proxy is off. | DOMAIN RULES NOT ENFORCED |
| 03 | **Proxy Filtered** | Network is enabled and the proxy applies domain rules. | DOMAIN RULES ENFORCED |

02

## Proxy Enforcement Path




Platform controls block direct external connections while permitting the local proxy path.

**EVIDENCE QUESTION** What proves the proxy was active, received the traffic, and applied the intended policy for this command?

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.
Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026
OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

# Platform Enforcement

One harness API translates the permission profile into different operating-system controls.

01

## Operating-System Implementations

### macOS

SEATBELT

Seatbelt policies run through sandbox-exec. Codex builds SBPL from a base policy, the resolved profile, and runtime context. Proxy rules allow the configured local ports.

### Linux

BWRAP + SECCOMP

codex-linux-sandbox coordinates bubblewrap and seccomp. Bubblewrap creates the filesystem view. Seccomp adds restrictions before the command runs.

### Windows

MXC

Microsoft eXecution Container receives translated filesystem and network policy with broad reads, narrower writes, and concrete denied paths.

02

## Shared Contract




**PLATFORM LIMIT**

Linux and native Windows may expand deny globs before launch. New matching paths may not join that command's restrictions.



© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.

Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026

OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

# Escalation and the MCP Boundary

Command permissions can change through approval, while a stdio MCP server starts under a separate launch boundary.

01

## Shell Command Lane




The harness evaluates requested access according to active approval settings and organization policy.

02

## Stdio MCP Server Lane

**Configured Launch** — SEPARATE

The harness does not automatically apply the command sandbox to this launch.

→

**Explicit Wrapper** — OPTION

codex sandbox can apply a dedicated profile when the operator configures it and prepares dependencies.

→

**Separate Authority** — BOUNDARY

Executable, arguments, environment, files, network, and downstream tools require their own governance.

03

## Evidence Distinctions

| Requested Access | Approval Decision | Actual Launch Boundary | Downstream Authorization |
|---|---|---|---|

**AUTHORITY RULE**

Approval can change a command boundary. It does not establish the server's business authority or downstream permission.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.
Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026
OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

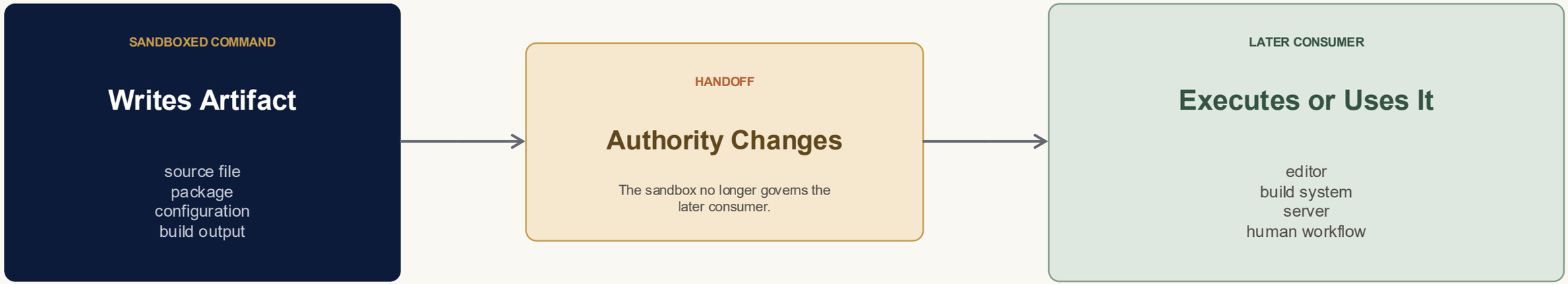
OpenAI Select Partner

# When an Artifact Leaves the Boundary

A file written under one command boundary may later be consumed under a different identity and permission set.

01

## Downstream Handoff




02

## Evidence That Must Travel

**Producer** — ORIGIN

Command, effective profile, approvals, and observed outcome.

**Artifact** — OBJECT

Version, hash, path, and review state.

**Consumer** — AUTHORITY

Identity, permissions, environment, and network state.

**Effect** — RESULT

Later execution or business outcome and its retained record.

SOURCE BOUNDARY

OpenAI supplies the later package-execution example. The authority-handoff evidence model is Luminity synthesis.

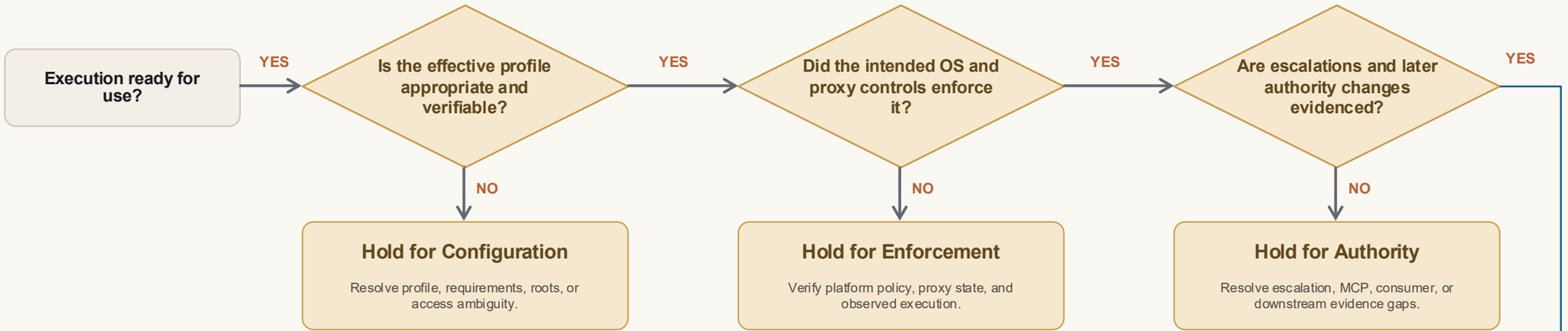
Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.
Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026
OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner

# Enterprise Assurance Boundary

The sandbox supplies an execution control. The enterprise validates authority, enforcement, transitions, and evidence.




## LUMINITY EVIDENCE CHECK

### Effective Authority — AUTH

Profile, requirements, approval policy, roots, and exception.

### Enforcement — CONTROL

Platform policy, proxy state, outcome, and descendants.

### Handoffs — TRANSITION

Escalation, MCP launch, artifact, consumer, and later effect.

### Retained Record — EVIDENCE

Correlated workflow, proxy, hook, and enterprise evidence.

**ARCHITECTURE RULE**

A sandbox constrains one execution boundary. Enterprise assurance connects authority and evidence across every boundary.

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

© 2026 Luminity Digital, Inc. All rights reserved in the original analysis, selection, arrangement, visual design, and commentary.

Source: https://openai.com/index/inside-the-codex-sandbox/ · verified Nov 18, 2026

OpenAI and related marks are trademarks of OpenAI, L.L.C. Independent analysis of public information. Not sponsored or endorsed by OpenAI.

OpenAI Select Partner